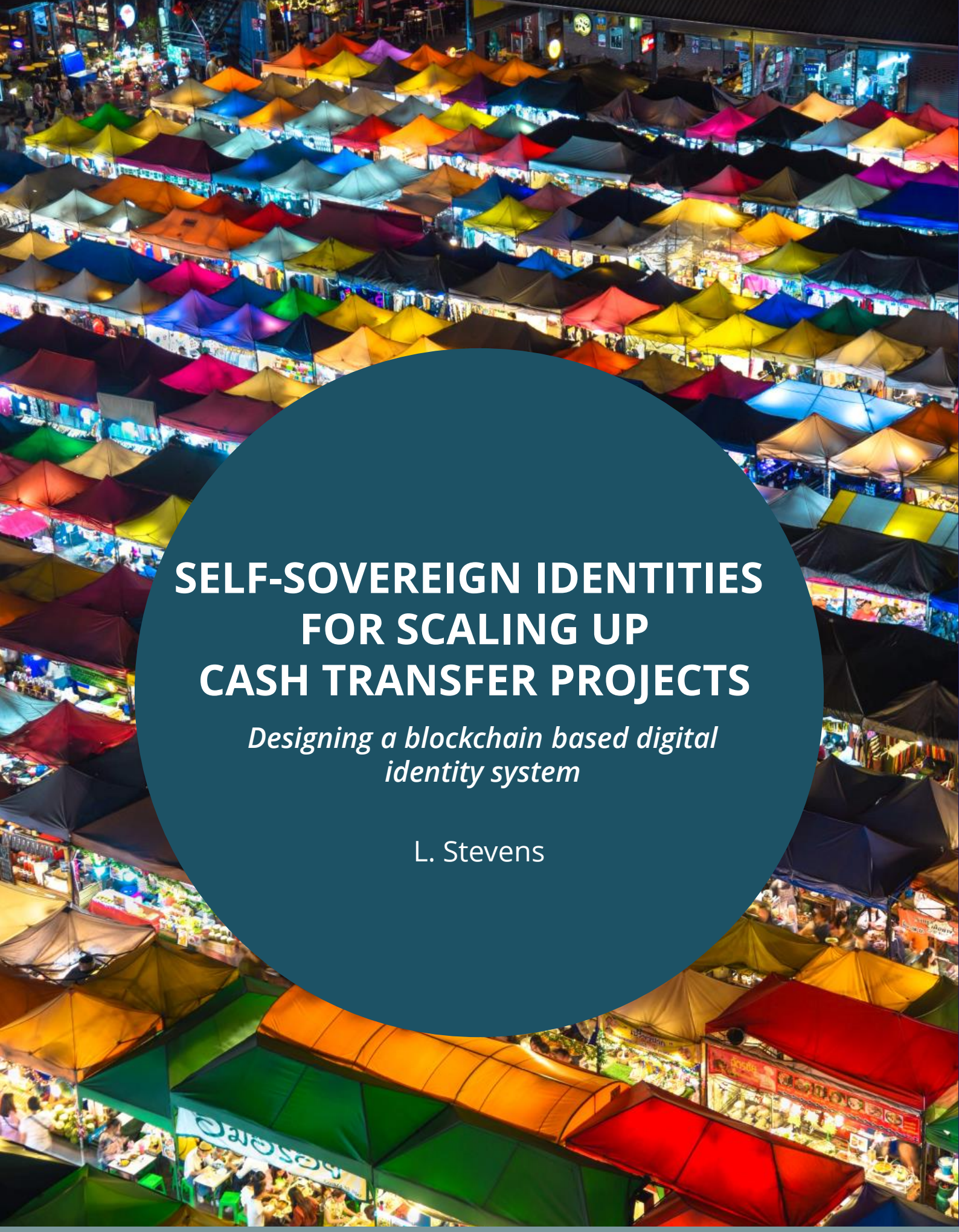


# SELF-SOVEREIGN IDENTITIES FOR SCALING UP CASH TRANSFER PROJECTS

*Designing a blockchain based digital identity system*

L. Stevens

TU Delft

510

AN INITIATIVE OF THE NETHERLANDS RED CROSS

# Self-Sovereign Identities for Scaling Up Cash Transfer Projects

Designing a blockchain based digital identity system

by

**L. Stevens**

in partial fulfillment of the requirements for the degree of

**Master of Science**
in Complex Systems Engineering & Management

at the Delft University of Technology,
to be defended publicly on Monday, 20 August 2018 at 14:00 PM.

| | | |
|---|---|---|
| Chair: | Prof. Dr. B.A. (Bartel) Van de Walle | TU Delft, Policy Analysis |
| First Supervisor: | Drs. J. (Jolien) Ubacht | TU Delft, ICT |
| Second Supervisor: | Dr. M.E. (Martijn) Warnier | TU Delft, Systems Engineering |
| External Supervisor: | Dr. S. (Stefania) Giodini | 510 |
| External Supervisor: | M. (Maarten) van der Veen | 510 |



TU Delft Delft University of Technology

# Preface

*"A creative man is motivated by the desire to achieve, not by the desire to beat others."* - Ayn Rand

On the same day that I handed in the first version of this thesis, I also turned the last page of a book that blew my mind, *Atlas Shrugged* from Ayn Rand. Where the former was an outcome of a process motivated by doing good and improving the lives of those in need, the latter prescribed that my own happiness should be the highest moral purpose of life. Are they contradictory? No, maybe, I am not sure yet. One thing dawned on me, in this project they were complementary. By aiming for my own contentment, the pleasure of achieving personal goals such as understanding blockchain technology and improving systems engineering skills, this final product has become richer and holds much more societal value than it would have had otherwise. It would be an illusion to think that I could have established this on my own, I may have tried at first. Yet, no amount of Trello cards, to-do lists or planning could have prepared me for this journey. It were the people, not the tools, that kept me on my feet.

From the TU Delft, I would first and foremost like to thank Jolien Ubacht. I believe she might have invented the concept of being a "listening ear", whilst asking the right questions at the right time. Our weekly conversations were about everything under the sun. Her critical assessments of my work and a life-lesson here and there were of incredible value. I would also like to thank Martijn Warnier, who had a sixth sense for knowing when to boost my confidence and challenged me to really understand the technical aspects of this research. Bartel Van de Walle, the chair of my committee, I want to thank for his input from his vast experience within the field of humanitarian assistance. His critical remarks on the human and organizational side, balanced out this research.

From the NLRC and 510 I would like to thank the entire team, being part of it opened up my world-view. Working with so many volunteers, graduate students and staff that are consciously choosing to innovate in a sector where the primary benefactors are people in need, is a very refreshing experience. In particular, I want to thank my supervisors Stefania Giodini and Maarten van der Veen. I am grateful for letting me be part of this project, supporting me with your time and knowledge was vital to the process. Your vision and operational skills will surely make 510 a well-known institute. Also, I would like to thank the experts and cash delegates that were interviewed to validate my findings and share insights.

Finally, I would like to thank all my friends, fellow students and family. The last few months I have been living under a rock, I am sure some might have liked the quietness but it feels good to be back! Myrna, Kees and Tamara, thank you for the support only family can give, it was unconditional. Amée, thank you for opening my eyes to so many things in the world I had been previously blind for, it was definitely one of the reasons for choosing this topic. Thanks for spell checking, hearing me out, bringing me food (lots of it) and being very patient, I know it was hard sometimes. For what its worth, at least you can now tell your new colleagues your not dating a student but an unemployed engineer.

*L. Stevens*
*The Hague, August 2018*

# Extended Summary

Humanitarian organizations are continuously balancing between the number of vulnerable people in the world and the available resources to assist them. In light of this struggle, many have ventured towards more efficient and effective means of providing aid. Ever since the Indian Ocean Tsunami in 2004, one of the preferred instruments became Cash Transfer Programming (CTP). It was estimated that in 2004 cash transfers only represented 1% of humanitarian aid, this figure rose to 6% by the end of 2015 [15] and to 15% by the end of 2017 [2]. It is expected to rise even more [13, 15, 143]. A CTP can be defined as:

> "..programs that provide noncontributory cash grants to selected beneficiaries to satisfy minimum consumption needs" [62, p. 18]

CTPs can have multiple goals, of interest for this research are the projects that have a protective purpose. They protect those affected by disasters to assure that people continue to live on a basic level of well-being and do not endure permanent losses [62]. Protective CTPs are most-often used in a humanitarian context via the hand out of unconditional cash, because this is easier and faster to implement than conditional CTPs during the first weeks/months after a disaster has struck. CTPs are only beneficial to set up if there is a functioning local market, otherwise distributed cash cannot be spend and in-kind aid is preferable.

Under the right circumstances, using CTPs instead of in-kind aid is already an improvement in itself. Yet, CTPs are not impeccable and scaling up will magnify some of the current imperfections and create new shortcomings. To implement a CTP the following steps are needed [31, 90] of which two are of concern for this research: *targeting* and *registration & identification*. Several weaknesses are expected to arise in these two steps:

- Collaboration and Interoperability; although humanitarian governance exists, there is not a lot of collaboration on CTPs, which leads to sub-optimal outcomes [16]. People are registered by various organizations repeatedly. Even if there is willingness, the means for collaboration and interoperability remain limited.
- Identity; identification and registration is hampered by the lack of proof-of-identity. The The World Bank Group 2017 estimates that 1.1 billion people have no official means to prove their identity, the majority living in Africa and Asia.
- Centralization; most identity management systems are centralized, they have a single point of failure and do not easily grow [52].
- Privacy and data-protection; humanitarian organizations will have to protect more data and guard the privacy of the most vulnerable, while not many of the humanitarian information management systems incorporate privacy-by-design [65]

CTPs are popularized and therefore increased in frequency and scale by humanitarian organizations. This means the challenges above will be enlarged and new challenges will arise. This calls for solutions and one potential solution to allow for scaling up and to leapfrog inefficiencies of centralized and non-digital identity management, is to create digital identity systems. More specific, to develop self-sovereign identity systems enabled by blockchain technology. Self-sovereignty is the concept of entities owning and controlling their own digital identity [12]. Blockchains are digitally distributed ledgers, which are almost immutable, append-only and are borderless. All data on a blockchain is digitized which eliminates the need for paper and manual documentation [46]. This information is stored in a block of data which is cryptographically sealed, chronologically stored with a permanent time-stamp and thus provides a trace of data transactions [46]. Each node in the network holds a copy, hence the distributed ledger, of the data which is automatically updated when everyone in the network agrees on an updated version of the ledger [46]. As with CTPs, blockchains have several drawbacks and different

architectural options, of which the public versus private and permissioned versus permissionless are the primary examples.

Blockchain can partly replace trust by encoding it in the system which can enhance collaboration and interoperability. Blockchain enables self-sovereign identities, which means that identities would not have a single use and can be maintained and controlled by the identity owners themselves. Blockchain has a distributed architecture, thus it allows for organic growth. Lastly, blockchains cryptographic protocols could enable an identity system at scale while still protecting privacy as long as no private data is stored on the blockchain.

Blockchain is a nascent technology and it has to be integrated within a multi-stakeholder environment where interests differ and physical distress is continuously present. The problem is that we know both the issues and potential solutions, but we do not know how such a system might look and what kind of choices need to be made. The challenge is as much a complex technical as social problem. This leads to the main research question:

> *Which design choices need to be made to develop a blockchain based system that allows registration, identification and targeting in protective Cash Transfer Programs to scale up?*

This research is conducted in collaboration with the Netherlands Red Cross and 510, their in-house data-science team. To answer the main research question a Design Science Research (DSR) strategy was used. Integrated in this strategy is a Technical, Institutional and Process (TIP) approach which is suited for dealing with complex socio-technical problems. Its roots are in systems engineering and entails that the final form of a system is much more the result of implementation and users interacting with it, than it is a one-on-one copy of the system on paper. One could design a specific process for implementation but this is left out of scope. The flexibility needed in such a process design is already integrated in this conceptual system design that is the end result of this research. The final deliverable is a set of advised design decisions with their implications and limitations. Methods that have been used throughout this research are literature reviews, semi-structured interviews, desk studies, participatory research, requirements engineering, comparative analysis, modelling, model validation and expert validation. In the following paragraphs the phases of the research are discussed.

### System Analysis

The design integrates three sets of design principles related to self-sovereign identity [9], privacy-by-design [34] and humanitarian information management principles [115]. Phases and functions in the design are based around the digital identity life-cycle [145]. Blockchain is analyzed from a layered architecture perspective, distinguishing the data structure, consensus protocol, network layer and application layer [100]. Expected preferences of several stakeholders were taken into account: national and local authorities, humanitarian organizations, the affected community and local merchants. These were perceived to hold significant power, have a very high interest in the solution or both.

### Program of Requirements

This scope has lead to the design of a program of requirements, which is the foundation on which the final deliverable is build. This program of requirements is ambiguous to the use of blockchain, i.e. it could also be used to guide developments of a centralized or federated identity system. It consists of over forty requirements, the rationale to include them, a priority and if they state something about a function the system must perform or a quality the system must have.

### System Design

The program of requirements was used to map four similar existing digital identity systems: Blockstack, Sovrin, the NLRC system and uPort. Comparing these alternatives resulted in a wider perspective on the possible techniques and concepts that could be used. Looking at the differences and similarities, ten design decisions were made. An abstract overview of this first version of design decisions can be seen in figure 1:

This first version satisfies almost all requirements except for four. Two have to do with the type of identifier used in the system, which puts more emphasis on validated credentials than it does on

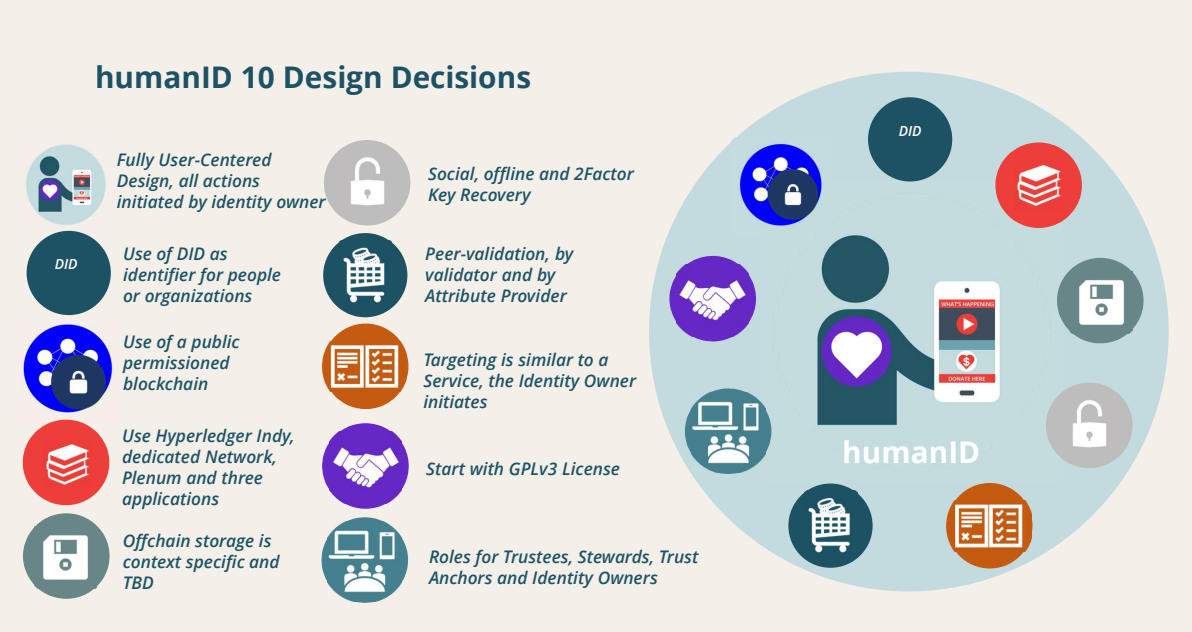



Figure 1: First version of Design Decisions

how many identities one has. An identity owner has multiple identities in the system, for each digital relationship one. In each relationship it matters what is vouched for by other attribute providers rather than how many accounts one has, but this does leave room for fraud. This is a problem that has so far not been in solved in any digital identity system. The other two have to do with the decision for a public permissioned chain which lets everyone register, but creates a barrier for organizations to join and perform certain roles. This barrier could also be perceived as a buy-in, resulting in more commitment from these organizations.

### System Demonstration and Validation

To understand how this design would translate into an actual system, a walk-through using Business Process Models & Notation (BPMN) followed. This was complemented with a Unified Modelling Language (UML) Class diagram, which demonstrated how this system could be programmed. A byproduct of this demonstration was the realization that some design decisions could be improved upon. The demonstration had a twofold purpose, it also allowed for model validation. The design decisions were also assessed by five experts, for which an interview protocol was set-up. In general the system was assessed positively yet some suggestions for improvement were made. This lead to the second version of the design decisions, which is presented in figures 6.16 and 6.17. In *italics* the improvements with regards to the first version are highlighted. Significant changes were deciding to leave out peer-validation and using some of the centrality provided by a permissioned chain to create a more sustainable way of retrieving access to accounts. Also two new cryptographical concepts, hierarchical deterministic key pairs and multi-signature signing are added to the design.

### Conclusions

To conclude, this research has gone through an entire design science research cycle. It produced several artifacts along the way, of which the second version of the design decisions is the most complete. The main scientific contribution can be found in the design of a system based on three sets of principles, which combines the fairly ideological concept of self-sovereignty with the practical measures to improve collaboration and better protect privacy of data subjects. This has lead to a set of design decisions that not only have a functional purpose, that of executing CTPs, but can grow into a foundational purpose, to create a continuous value proposition. One could argue blockchain is not truly necessary for this, but at the least this proposition brings organizations together to talk about a shared and interoperable system. This set of design decisions should be used by the humanitarian sector as a concept version, a 40% draft which needs to be finalized by all participants through a well-crafted process management approach.

This concept version invites organizations to join the cause, demonstrates a rigorous research process and is flexible enough to take in the wheeling and dealing of an implementation process. What a well-crafted process management approach would look like is something that needs to be further researched as it was left out of scope for this research. In further research humanitarian governance should be taken into account, the limited formal powers and mandate of humanitarian organizations before disasters strike and how the design principles are represented during changes of the design. A more specific part of this process design could be the financial feasibility of a global humanitarian identity system, who will pay for what and what business models are preferred. This is a sensitive subject as many people relate blockchain to the ominous world of cryptocurrencies, where vast amounts of money is speculated on. A strategic design research assignment could also include field-research into user preferences and demands, out of scope in the current research. Lastly, sooner or later a self-sovereign system should be largely governed and used by communities themselves. Some researchers already hint towards the application of Ostrom's theories on self-governance [41], it would be interesting to find out if lessons from her research apply on managing self-sovereign identities.

## humanID

| # | DECISIONS | IMPLICATIONS | LIMITATIONS |
|---|---|---|---|
| 1 | Use blockchain technology | • Use strong asymmetric encryption<br>• Enables self-sovereign identity<br>• Accommodates growth<br>• Encode trust in the system | • Uncertainty due to nascent technology<br>• *Multiple blockchains with the same use-case are inefficient* |
| 2 | Use a public permissioned blockchain | • Open to all to register<br>• Creates a buy-in for stakeholders<br>• More scalable than permissionless<br>• A trust-framework is needed outside the system | • Not open to all to validate, identify and provide services<br>• Could create a barrier for adoptability<br>• *Technically complicates the first registration for participants*<br>• Not a pure self-sovereign identity<br>• *Less transparency and more chances for fraud* |
| 3 | Use DIDs and a fully User-Centered Design | • All contact is initiated by the identity owner<br>• Identity owner controls all private data<br>• Identity owners can have multiple identities based on the digital relationship because they are pairwise pseudonymous<br>• Attribute providers become the center of gravity<br>• A Decentralized Public Key Infrastructure is used<br>• Multiple validation for one credential is possible<br>• DIDs may be used for other systems<br>• *Hierarchical Deterministic Key Pairs enable multi-show unlinkability*<br>• *Fraud detecting algorithms should be used to counter corruption with multiple identities using self-attested attributes only* | • Hundreds of DIDs are needed which should be maintained<br>• *DIDs are not human-readable a solution is necessary to maintain them*<br>• *Fraud is more likely if there are limited attribute providers or few validated credentials* |
| 4 | Use Hyperledger Indy, HumanID, Plenum and four applications | • A blockchain designed for only one use-case<br>• Different consensus mechanism can be plugged in<br>• An Identity Owner Application to register and maintain an identity<br>• An Identity Application to approve registrations and provide credentials<br>• A Service Application to provide services only accessible by humanitarian organizations<br>• An Admin Application for Trustees and Stewards to appoint other roles and direct nodes | • *Time is needed to set up a dedicated humanID network with a minimum a mount of nodes to grant security*<br>• *Identity Wallet not directly necessary as DIDs only stem from humanID and not from other blockchains* |
| 5 | Use the GPLv3 License | • Does allow for commercial use as long as it is opened up which creates a business model as proposed by Hyperledger Indy and Sovrin | • *It does not fully comply with the humanitarian principles* |

Figure 2: Second version of Design Decisions #1 to #5 (in italics are presented improvements suggested during validation)

**humanID**

| # | DECISIONS | IMPLICATIONS | LIMITATIONS |
|---|---|---|---|
| 6 | Use Hyperledger roles and matching interfaces | • Roles for Trustees, Stewards, Trust Anchors (Identity, Attribute and Service Providers), Identity Owners, *Custodian*<br>• Interfaces for Identity Owners: Feedback, User, *Custodian*, *Validator*<br>• Interfaces for Trust Anchors: Registration, Validation and Services<br>• Interfaces for Stewards and Trustees: Admin interfaces<br>• Feedback via FAQ, Chatbots and face-to-face | • A community engagement approach is necessary<br>• UX/UI must allow for illiteracy, the visual impaired, other disabilities and various languages<br>• Before implementation there must be enough Stewards and Validator nodes to grant secure and fair consensus<br>• *Uncertain how the custodian role is integrated in the system*<br>• *Custodian might endanger their own privacy* |
| 7 | Offchain storage is to be determined by context | • Options are local devices, paper-based, smartcards, secure cloud storage, *Highly Secure Modules*<br>• Private keys are stored on the device or paper based<br>• Identity attributes could be stored on a device or *on paper via QR codes*<br>• Agents back-up data | • Single points of failure arise if chosen for specific options<br>• There will always be attacks to retrieve private data |
| 8 | Social and off-line key recovery, two-factor authentication and *centralized account protection* | • An option based on social recovery<br>• An option based on offline back-up<br>• Two-factor authentication as *a permanent way to access an account*<br>• *Multi-signature signing to block an account and create a new account*<br>• *Hierarchical Deterministic Key Pairs to block an account* | • Social recovery depends on others ability to access their accounts<br>• Paper based solutions can get lost too<br>• *People often forget to make back-ups*<br>• *Multi-signature signing and Hierarchical Deterministic Key Pairs introduce some centrality with agents* |
| 9 | Targeting is seen as a service not as a separate activity | • Service provider role reserved for humanitarian organizations in functional purpose phase<br>• *Service providers can retrieve a map to see registration coverage without revealing any private information or specific location*<br>• *Inclusion algorithm is send to the identity owner, only an inclusion result is send back*<br>• *Service providers must keep a list of organizations they trust to validate credentials*<br>• Inclusion scores can only be stored temporarily<br>• Trustees and Stewards must open up the role of service provider to create a foundational system | • *Device of identity owner must be able to process inclusion algorithm*<br>• *Visualizations of geotags are available to service providers, if the system becomes foundational this connection must be reviewed*<br>• *Trust lists must be kept up to date* |
| 10 | Validation by attribute provider and by appointed validator | • *No peer validation as it is difficult to value and opens up private information*<br>• Validation by Attribute Providers<br>• Validation by appointed Validators for predefined periods only by using key rotation | • *The Validator role has to have a public facing credential opening up the identity of an individual for a specific time frame*<br>• *There is no method of assuring there are enough Validators and Attribute providers, which have a central role* |

Figure 3: Second version of Design Decisions #6 to #10 (in italics are presented improvements suggested during validation)

# Contents

# List of Figures

# List of Tables

# List of Acronyms

| | |
|---|---|
| **AP** | Attribute Provider |
| **BPMN** | Business Process Model and Notation |
| **CCT** | Conditional Cash Transfers |
| **CTP** | Cash Transfer Program |
| **dAPPS** | Decentralized Applications |
| **DDO** | DID Description Object |
| **DII** | Demographically Identifiable Information |
| **DLT** | Distributed Ledger Technology |
| **DNS** | Domain Name System |
| **dPOS** | Delegated Proof of Stake |
| **DID** | Decentralized Identifier |
| **DPKI** | Decentralized Public Key Infrastructure |
| **DSR** | Design Science Research |
| **GDPR** | General Data Protection Regulation |
| **HIMP** | Humanitarian Information Management Principles |
| **ID** | identity or identity documents |
| **IDEF** | Icam DEFinition for function modeling |
| **IDP** | Internally Displaced Persons |
| **IdP** | Identity Provider |
| **IHL** | International Humanitarian Law |
| **IO** | Identity Owner |
| **IP** | Internet Protocol |
| **IPFS** | Inter Planetary File System |
| **IS** | Information Systems |
| **NGO** | Non Governmental Organization |
| **P2P** | Peer-to-Peer |
| **PbD** | Privacy-by-Design |
| **PII** | Personally Identifiable Information |
| **PKI** | Public Key Infrastructure |
| **PoS** | Proof-of-Stake |
| **PoW** | Proof-of-Work |
| **SaaS** | Software-as-a-Service |
| **SDK** | Software Development Kit |
| **SP** | Service Provider |
| **SSI** | Self-Sovereign Identity |
| **TA** | Trust Anchor |
| **TSP** | Trust Service Provider |
| **UCT** | Unconditional Cash Transfers |
| **UML** | Unified Modelling Language |
| **URI** | Uniform Resource Identifier |
| **UUID** | Universally Unique Identifier |
| **ZKP** | Zero-Knowledge Proof |
| **zk-SNARKS** | Zero-Knowledge Succinct Non-interactive Argument of Knowledge |

# 1

# Introduction

*"I'd like to see it become impossible to be comfortably off and do nothing for the world's poor"* - Peter Singer

The frequency of climate related disasters, geophysical catastrophes, armed conflicts and man-made environmental emergencies is increasing [49]. The effects are often mutually reinforcing, severe, immediate and initiate a ripple effect [125]. In 2010, approximately 500 million people lived in an uncertain and destructive environment [70]. This was before the Syrian conflict and Ebola crisis struck. In the Global Humanitarian Overview 2017, published by UN OCHA[1], an estimated 128.6 million people were in humanitarian need for which $22.2 billion is required for relief. Almost a 10-fold increase of what was needed in 1992 when the appeal for funding humanitarian needs was started [149, p.5]. All the while, the necessary resources to overcome or prevent the devastating outcomes of these disasters, remain limited. Therefore, NGOs, governments and humanitarian organizations are in search of more efficient and effective methods for intervention [29].

## 1.1. Cash Transfer Programming

One intervention that is used increasingly is Cash Transfer Programs (CTP) by humanitarian organizations and governments, as an alternative or in parallel to in-kind aid (supply of materials and food) [65]. A CTP can be defined as:

> "..programs that provide noncontributory cash grants to selected beneficiaries to satisfy minimum consumption needs" [62, p. 18]

According to Lee [104] the benefits of CTPs can be found in the significant reduction of overhead costs, monitoring of financial activity, restoration of dignity by giving beneficiaries power over their choices, timeliness of providing aid, stimulating the local market and positively effecting health. Yet, there are also risks. Such as local inflation, the use of cash for temptation goods (e.g. cigarettes, alcohol, etc.), aid diversion, segregation within the population, adverse effects on gender equality and corruption and security issues with distribution of cash [104]. CTPs have been thoroughly researched and evaluated, which has provided rich evidence for their effectiveness in humanitarian assistance and international development [10, 15, 62, 74].

CTPs can have multiple roles as is shown in figure 1.1. First, the focus on protective CTPs is chosen because they have more urgency as they are often carried out in post-disaster environments and in low-income countries where governments have less capacity and capabilities to assist their citizens themselves. The other forms of CTP assistance are mostly carried out by more stable governments. Mind you, in protective CTPs it is also the government that should fulfill this role but is sometimes unable to do so.

The focus on protective CTPs comes with the focus on the humanitarian context which can be defined as:

[1] United Nations Office for the Coordination of Humanitarian Affairs


Figure 1.1: Various roles of a Cash Transfer Program based on Garcia and Moore [62]

> "[..] intended to save lives, alleviate suffering and maintain human dignity during and after man-made crises and disasters associated with natural hazards, as well as to prevent and strengthen preparedness for when such situations occur." [49, p. 81]

Humanitarian assistance is based on the principles of humanitarianism: "the impartial, neutral and independent provision of relief to victims of conflict and natural disasters" [17, p. 382]. A more generous definition is that humanitarianism is any activity that aims to alleviate suffering, cease preventable harm, save lives and improve welfare of the most vulnerable [17]. Humanitarian assistance as a whole is a global undertaking and comprises of intergovernmental organizations, religious organizations, NGOs and the International Committee of the Red Cross (ICRC), where the latter has a special status in humanitarian law [77]. As such, the execution of CTPs concerns many stakeholders and is subject to a form of humanitarian transnational governance. This type of governance is special as humanitarian organizations are often outside the sovereignty of a single state [77]. Thus, humanitarianism is governed by the humanitarian organizations themselves and not by formal powers, leaving room for politics and diverging interests [77].

### 1.1.1. Characteristics of a Cash Transfer Program

There is not one specific way to set up CTPs but there is one very important criterion that has to be met before a CTP is set: is there a local functioning market or a chance of one being there in sufficient time? If not, than cash is useless and in-kind aid would be of better assistance. If yes, than a CTP of some type might be of help. Four types of CTP exist [75, p. 4]:

1. Unconditional Cash Transfers (UCT), where the beneficiary is free to do with the cash as she pleases
2. Conditional Cash Transfers (CCT), where the beneficiary has to comply with pre-specified spending requirements for the cash she receives
3. Vouchers, a paper/card/token which can be traded for a set of goods
4. Cash-for-Work, where payment is provided in either cash or vouchers

Which type is used highly depends on the context. In a humanitarian context the preference goes out to unconditional transfers in the first phases of the response. Because they are easier and faster to implement which is necessary in disaster situations. Within each type, one can distinguish six design components: Design Objectives, Monitoring & Evaluation, Transfer Amounts, Targeting & Registration Method, Time Frames and Transfer Mechanism [24, 75]. *Design objectives* can be a practical objective (e.g. humanitarian aid) and/or a research objective (e.g. effect study). *Monitoring & Evaluation* is about the approach to check whether the design objectives have been achieved. The use of interviews, focus groups, physical examinations and market assessments is common. *Transfer amounts*, depend on the local context (e.g. price for rice, hourly wages), the available funding, and the *time frames*. Single donations are possible, but in some cases monthly donations for a limited period of time are

preferred. *Targeting & registration* is about identifying the beneficiaries and subsequently registering their identities, upon which it can be checked whether a beneficiary is eligible for the program. Self-selection, community-based selection, vulnerability assessments and geographical targeting all occur and are sometimes used to complement each other. Lastly, the *transfer mechanism* is about how the money is transferred to the beneficiary. Examples are direct cash, mobile money, vouchers or bank accounts.

### 1.1.2. Popularization of Cash Transfer Programs

The humanitarian sector is starting to see CTP as the go-to-option for humanitarian assistance in case the necessary criteria are met. It was estimated that in 2004 cash transfers only represented 1% of humanitarian aid, this figure rose to 6% by the end of 2015 [15] and to 15% by the end of 2017 [2]. The World Bank confirms the trend starting from the Indian Ocean Tsunami in 2004 and expects cash transfers to become increasingly popular [143]. As a result of the popularization the challenges CTPs face are magnified and new challenges arise, the following are identified:

- **Collaboration and Interoperability**: Although humanitarian governance exists, there is not a lot of collaboration on CTPs, which leads to sub-optimal outcomes [16]. Even if there is willingness, the means for collaboration and interoperability remain limited
- **Identity**: Identification and targeting is hampered by the lack of proof-of-identity. The The World Bank Group [146] estimates that 1.1 billion people have no official means to prove their identity, with the majority living in Africa and Asia. Although CTPs can be more efficient and faster than in-kind assistance, a slow process of manually targeting and registering affected people remains a problem.
- Centralization; most identity management systems are centralized, they have a single point of failure and do not easily accommodate growth [52]
- **Privacy and data-protection**: Humanitarian organizations will have to protect more data and guard the privacy of the most vulnerable, while not many of the humanitarian information management systems incorporate privacy-by-design [65]
- **Adaptability to context**: The design, and imminently the success, of a CTP depends significantly on political, economic, social, technical and administrative constraints [10] implying a local solution is always needed so generalizations at scale are difficult to make
- **Responsive markets**: According to Brooy [30] scaling CTPs could increase the chance of local inflation

One could say that organizations acting in the humanitarian context where they conduct CTPs have a clear need to resolve the issues above. It is not likely that all of them can be tackled at once, but some can. In the following paragraph a solution is put forward.

## 1.2. Blockchain Technology as a Potential Solution

As in many sectors, solutions with regard to data protection and interoperability are increasingly sought after in new technologies and of late, in blockchain technologies (BT). The Digital Humanitarian Network, the United Nations, the Netherlands Red Cross, the GSMA (a representative organization for the mobile operator industry) in cooperation with UK AID and the Institute of Development Studies link blockchain to CTPs and describe the following potential use cases: protected data sharing & digital registries, (self-sovereign) identities, supply chains, donor financing, CTPs, aid transparency and smart-aid contracts [3, 69, 88, 98, 151].

What is blockchain exactly and why is it put forward? Blockchain is a *digital distributed ledger*, which is *almost immutable* and is *borderless*. All data on a blockchain is digitized which eliminates the need for paper and manual documentation [46]. This information is stored in a block of data which is cryptographically sealed, chronologically stored with a permanent time-stamp and thus providing a trace of data transactions [46]. Each node in the network holds a copy, hence the term 'distributed ledger', of the data which is automatically updated when everyone in the network agrees on an updated version of the ledger [46]. In some blockchains anybody can join the network, making the ledger

borderless by only requiring the software and hardware to become part of it. In this thesis the terms 'blockchain' and 'ledger' will be used interchangeably.

For CTPs, blockchain is best understood when introducing two types of software architecture: centralized architectures and distributed architectures. An architecture is centralized if in the network one node can be turned off, which brings down the entire system. A centralized system requires less coordination costs, less dependency on networks and less security issues. A distributed system offers higher computing powers, higher reliability and the ability to grow naturally [52]. With regard to CTPs this means that if technical solutions are proposed, they speed up manual processes and decentralized architectures could accommodate growth more naturally though at the cost of increased coordination. However, this is where blockchain thrives since it deals with coordination and security by "manufacturing trust through clever code" [40, p.5]. In reality blockchains are not trustless as they require some form of trust [81], but what this implies is that there is no need for a trusted third party - it leaves out the middle-man. For CTPs this indicates that collaboration within the humanitarian sector might improve as blockchain could offer a trustworthy and interoperable tool.

Blockchains are also called Distributed Ledger Technologies (DLTs) and the characteristics described above differ by the specific DLT form that is used [107]. A regular distinction is that of public versus private and permissioned versus permissionless [158]. In figure 1.2 an overview is given of open and closed blockchain types [81, p.20]. There are two open and two closed blockchain architectures.

- **Public permissionless**: The "purest form" of blockchain where everything is transparent and anyone could change the state of the ledger
- **Public permissioned**: Anyone can see the blockchain but not everyone can change the state of the ledger
- **Consortium ledgers**: A restricted set of participants across organizations have full access and can change the state of the ledger
- **Private permissioned**: A restricted set of participants within one organization have full access to the ledger. Only the network operator can change the state of the ledger

These different types imply design decisions influence how issues such as speed, privacy, growth and security with scaling up CTPs are dealt with [41]. These design choices presumably portray the interests of stakeholders, indicating that decisions on which interests should be included need to be made [117]. Ølnes et al. introduce the term 'governance of blockchains', which dictates what values should be reflected in designing a blockchain system and how to cope with changes.

| Blockchain types | | Read | Write | Commit | Example |
|---|---|---|---|---|---|
| Open | *Public permissionless* | Open to anyone | Anyone | Anyone* | Bitcoin, Ethereum |
| Open | *Public permissioned* | Open to anyone | Authorised participants | All or subset of authorised participants | Sovrin |
| Closed | *Consortium* | Restricted to an authorised set of participants | Authorised participants | All or subset of authorised participants | Multiple banks operating a shared ledger |
| Closed | *Private permissioned ('enterprise')* | Fully private or restricted to a limited set of authorised nodes | Network operator only | Network operator only | Internal bank ledger shared between parent company and subsidiaries |

Figure 1.2: DLT Architectures from Hileman and Rauchs [81]

As with CTPs, blockchain faces challenges. *First*, the design of a blockchain is said to be contesting with the power of existing institutions. Blockchain could be seen as an institutional technology of

governance, aiming for decentralization [41]. Due to the near-immutability of the ledger and the codification of trust, the middle-man or the third-party has to change its role and act accordingly [38]. For the humanitarian sector this implies that some form of humanitarian governance becomes obsolete, as it is encoded in the technology. The humanitarian sector would need to alter their responsibilities, adapt to the new environment and maybe even let go of some of its tasks. *Second*, with the design options at hand choices have to be made that weigh wants of privacy versus transparency and security versus speed [52]. These choices reflect certain values and perspectives, e.g. they have an ethical dimension. In a diverse set of stakeholders in the humanitarian sectors these values and perspectives might differ, or change altogether. Fast-forwarding to the implementation of a blockchain, this could result in institutions with formal or informal power to block promising solutions. *Lastly*, legal challenges should not be taken lightly or be overlooked as the current juridical system needs many amendments for blockchain to fully take off [164]. Especially, when blockchain is seen in the shape of an institutional technology of governance, and competes with firms, markets, networks and other governance structures [41].

## 1.3. Demarcating the Solution Space

As of yet, the integration of blockchain is minimal in any sector and although there are many potential use-cases in a CTP, due to the complexity of humanitarian assistance and blockchain, and time-restraints of this research project, this thesis' focus is on one component of a CTP. In figure 1.3 an overview is provided of a CTP system.

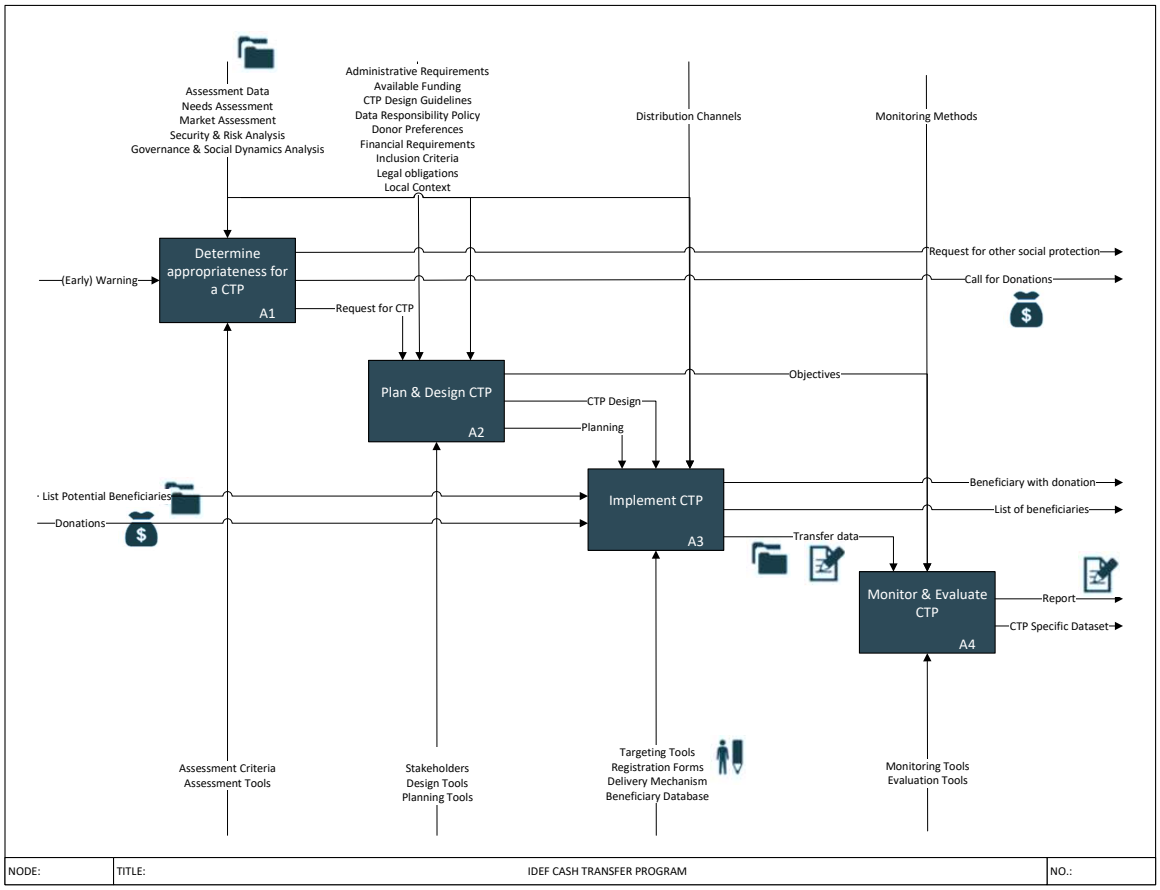



Figure 1.3: IDEF System Diagram of a CTP based on CaLP [31], Harvey and Bailey [75], HelpAge International [76], International Red Cross and Red Crescent Movement [90], NRC [112]

The system is visualized using the IDEF0 standard, which is often used to describe a set of interrelated activities. Each activity is shown in an activity box, which can later be decomposed in sub-

activities. Each activity is subject to four arrows. From left to right, input flows in and gets transformed by the activity to output. From the top, control mechanisms are shown and each box is supported by a set of resources. The input for this diagram was taken from guidelines for CTPs in a humanitarian context from the Humanitarian Practice Network [75], HelpAge International [76] and the Norwegian Refugee Council [112]. Also the tool-kits of the ICRC[2] and the Cash Learning Partnership[3] (CalP) were consulted. In this diagram four application areas that can be supported by blockchain are denoted. While not being exclusive, these four options present the main application areas and are briefly described below:

 Using blockchain as a digital (donor-to-beneficiary) payment mechanism

 Using blockchain to create shared data ledgers, enabling secure and trusted data sharing among stakeholders in an untrustworthy environment

 Using blockchain to track transfers of assets, provide feedback to donors and evaluate projects

 Using blockchain for digital identity management, providing identities for beneficiaries, targeting beneficiaries by using their digital identification

This research further zooms in on the activity "Implement CTP" from figure 1.3 and further detailed in figure 1.4. "Implement CTP" consists of five sub-activities. First, the CTP design is translated into an operational program. Second, potential beneficiaries are targeted based on inclusion criteria and this plan of approach. Third (optional), in case a humanitarian organization does not provide all of the services themselves, a service provider is contracted. This can be a local bank, remittance company, mobile phone operator, humanitarian information management software and the like, they are necessary to move the money from the origin country into the pockets of beneficiaries. This means they have to be somehow included into the system as they will likely express the need for some personal information of the beneficiaries. Fourth is the identification and registration of beneficiaries, which should result into a list of eligible and validated identities. Lastly, there is the disbursement and encashment of money.

More specific, this research focuses on the activities targeting (activity A3.2.) and identification & registration (activity A3.4.) of beneficiaries in figure 1.4. There are four reasons for this demarcation. *First*, the assumption is that blockchains enabling payments are already popularized by the financial sector and actively researched. *Second*, to track expenses, provide feedback to donors and make payments one first has to establish the identity of the beneficiary. *Third*, using blockchains solely for data storage is unfeasible since blockchains are rather inefficient as just a database [123]. However, if the data stored on a database needs to be near-immutable and requires a certain degree of shared trust then blockchain could be a good fit. *Fourth*, targeting and registration requires a lot of humanitarian governance if done by multiple organizations. An architecture that offers blockchain based targeting and registration can be shared and used by multiple organizations, thus compete with the current governance structure that blocks collaboration.

[2] http://rcmcash.org/
[3] http://www.cashlearning.org/toolkits/cash-toolbox

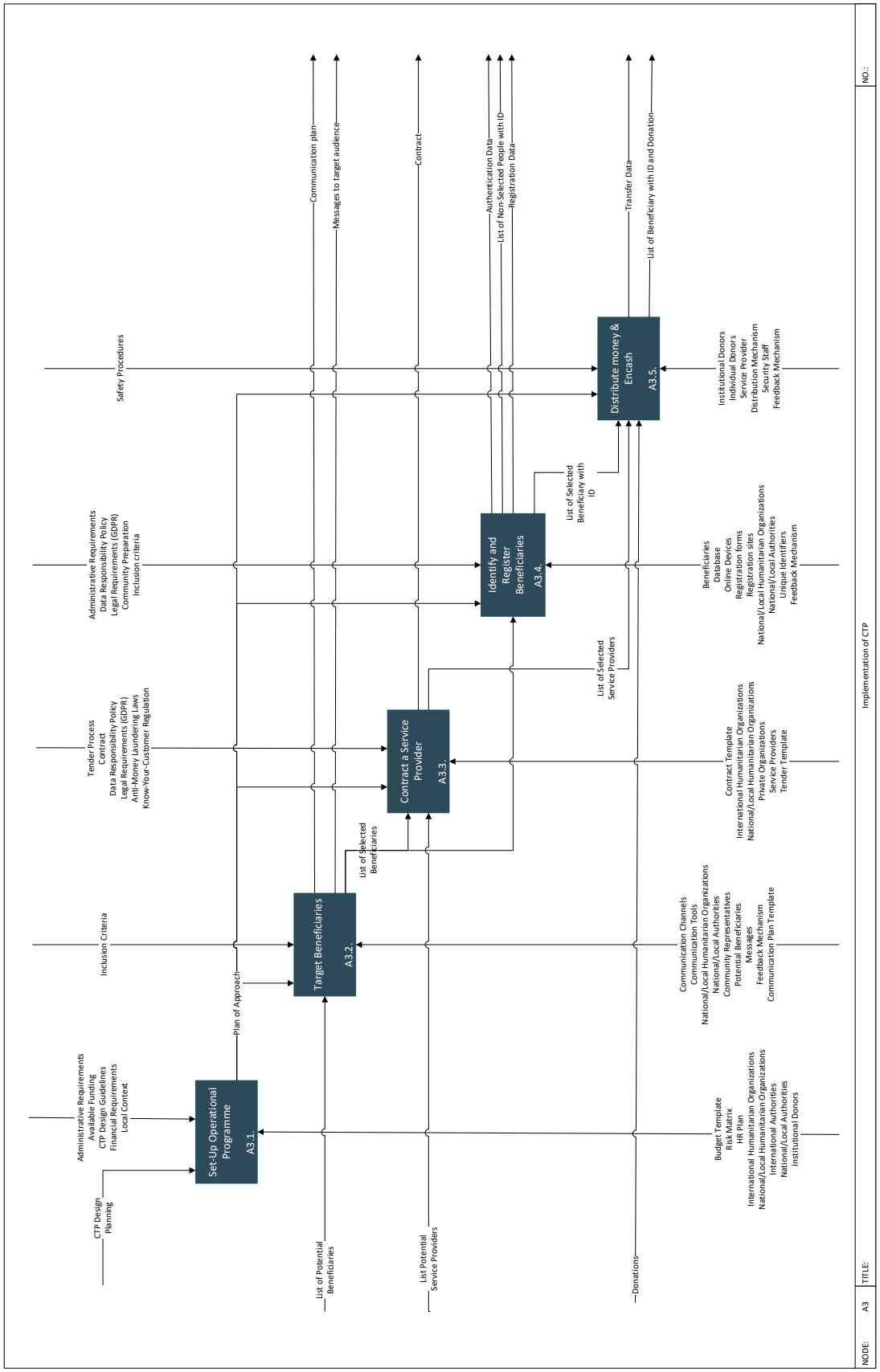



Figure 1.4: IDEF System Diagram of CTP implementation based on CaLP [31], Harvey and Bailey [75], HelpAge International [76], International Red Cross and Red Crescent Movement [90], NRC [112]

## 1.4. Problem Definition

To summarize the previous section, the focus of this research is on registration, identification and targeting of protective CTPs which development help to overcome existing and future scale-up challenges. Blockchain could specifically assist in providing a safe and secure way of sharing data, which increases the efficiency of identification and targeting in CTPs. Due to its decentralized structure blockchain can grow more naturally as CTPs grow and blockchain offers a method for trust and control in an environment where collaboration is lacking.

Blockchain might not be the only solution for the challenges faced by scaling up CTPs. Yet, this thesis focuses on blockchain since up to now it remained unclear how the potential benefits can actually be transformed into a working solution and subsequent implementation. The problem can be defined as follows:

> CTPs and humanitarian assistance serve the most vulnerable people, which are already very difficult to identify. Scaling up CTPs will enlarge this problem which is faced throughout the sector. A blockchain based identity system could help standardize registration, securely store and retrieve information, grow naturally with the number of CTPs and smoothen collaboration. It is unclear how the design of such a system should look like.

This is a socio-technical problem because it involves the technicalities of the system in an environment with limited mobile or internet connectivity in affected areas, time consuming procedures, limited interoperability between organizations due to missing tools and the nascence of blockchain technology. While also involving the social challenges of humanitarian collaboration, cultural systems in affected communities and user behavior related to technical systems. Incorrect technical targeting might even make the most vulnerable worse off, as other people can buy more of the limited available products on the market and their purchasing power is further decreased [96]. These problems require both a sound technical and institutional solution, as a process design. A process design deals with participation of stakeholders, creating support and changing a conceptual design into a final working system. A new system integrating blockchain thus requires a socio-technical system design, which acknowledges the fact that systems are a product of human behavior and technicalities.

## 1.5. Reading Guide

This research proceeds in six chapters. In chapter 2 the research design is presented which includes the objective, main research question and scientific relevance. Chapter 3 depicts the first phase of research and describes the outcome of a literature review on CTPs, a technical, institutional and stakeholder analysis on the environment in which CTPs take place. Based on these outcomes, chapter 4 discusses a program of requirements that lays the foundation for a system design. Chapter 5 compares four similar systems to draw concepts and ideas from, upon which a set of design decisions are laid out. The workings of these design decisions are demonstrated in chapter 6, which also includes the validation of the design. After validation a second version of the design decisions is presented. Chapter 7 evaluates this research and answers the main research question.

# 2

# Research Design

*"The best game plan in the world never blocked or tackled anybody"*
- Vince Lombardi

To conduct this research a game plan or, in academic terms, a research design, is needed. This chapter describes the objective of this research in paragraph 2.1. Based on the problem definition and the objective, a research strategy was chosen and is put forward in paragraph 2.2. The research strategy sets up the main research question, which is supported by various sub-questions. Each question is answered by using various methods which are also described in paragraph 2.3. A description of the research deliverable is given in paragraph 2.4. In paragraph 2.5 the societal relevance of this research is described and in paragraph 2.6 the academic relevance is put forward.

## 2.1. Research Objective

The goal of this research is to:

> Help enable the humanitarian sector collaborate on scaling up the use of cash transfer projects by integrating a blockchain based solution.

More specific, this research is conducted in the name of the humanitarian sector, and the *Netherlands Red Cross (NLRC) and 510*. The NLRC and 510 are part of the International Federation of Red Cross and Red Crescent Societies (IFRC) and have provided their network, facilities and time to supervise part of this research. This global humanitarian organization has the goal to improve the lives of vulnerable people by activating the power of mankind [89]. They live up to the Fundamental Principles of Humanity, Neutrality, Impartiality, Independence, Voluntary Service, Unity and Universality. 510 is an inhouse data science team of the NLRC with the goal to: "Shape the future of humanitarian aid by converting data into understanding, and put it in the hands of humanitarian relief workers, decision makers and people affected, so that they can better prepare for and cope with disasters and crises"[1]. 510 has dedicated a project towards exploring the future of CTPs, including the use of blockchain. Their aim is to improve CTPs with reference to safety, costs, scalability, inclusiveness and timeliness [3]. This project is conducted with several development partners and other studies in this project are focused on international affairs, the acceptability of digital identities and the cooperation between governments and humanitarian organizations on CTPs. The synergies and insights from our research will provide 510, the NLRC, IFRC and humanitarian sector with in-depth knowledge on the use of blockchain and scaling up targeting, identification and registration for CTPs.

## 2.2. Research Strategy

For this research a Design Science Research (DSR) strategy and a systems engineering approach are used. The strategy lays out the phases of this research, while the systems engineering defines the

[1] https://www.510.global/video/

mindset. This attitude entails that the final form of a system is the result of implementation and users interacting with the system. This confines a design to embed flexibility and incorporate a process perspective when making trade-offs in the design.

DSR is the practice of combining behavioral science with design science [80]. Behavioral science aims for the truth and considers the development of theories on human behavior, for example in relation to technology [80]. Design science aims for utility, by building and creating artifacts [79], for which it relies on existing kernel theories to create innovative artifacts [47, 106]. Hence, DSR provides two outcomes: an artifact and a scientific contribution. The artifact for this research is a set of design decisions which the humanitarian sector can use to develop a working first version of a blockchain based system.

DSR is a good fit with the research objective and problem definition of this paper for several reasons. *First*, the research implies a design of sorts, as both CTPs and blockchains are subject to design decisions. DSR comes up with a practical design in the form of an artifact. *Second*, DSR is often used in Information Systems (IS) [93]. An IS is a system which collects, processes and distributes data. This implies that the system that will be designed is an IS. *Thirdly*, DSR is known to be applied to wicked problems. These are problems in socio-technical systems for which there is no ready made solution and requirements are still unknown [35]. These problems need the right cognitive abilities derived from design science and the right social abilities derived from behavioral science. It also allows for flexibility, which is needed when not all requirements are known upfront [79]. The question if and how to apply blockchain solutions to CTPs is also a wicked problem. *Fourthly*, DSR is also a good match because of the collaboration between the NLRC, 510 and its development partners. This enables participatory research into a design process.

As with every research strategy, there are some drawbacks to DSR. Developing disruptive innovations can be quite difficult if one only relies on existing scientific theories [79]. Next, a researcher using DSR has to balance the importance of two outcomes: an artifact and a scientific contribution. This could lead to shortcomings or a delay in the study. There are also dangers with the two underlying sciences. Design science could struggle with cultivating a competent knowledge base, which could lead to well-designed artifacts that are impractical for the users [80]. Behavioral science could be flawed when there is an overemphasis on contextual theory and fails to detect technological competences, this could culminate into theories focusing on inadequate technologies [80]. These risks will always exist in some form, so mitigation is done by pro-active retrieval of feedback and validation of the design. Throughout this research semi-structured interviews with relevant stakeholders will be conducted to validate intermediate results and later a model validation and expert validation are done to test the validity of the artifact.

## 2.3. Research Question and Methods

DSR requires a main research question focusing on the creation of a design. Synthesizing this with the problem definition and research objective leads to the following main research question:

> *Which design choices need to be made to develop a blockchain based system that allows registration, identification and targeting in protective Cash Transfer Programs to scale up?*

This research question suits the Complex Systems Engineering & Management (CoSEM) program since its focus is on designing socio-technical systems. In particular given that the track Information & Communication within this program pinpoints the development of information systems within a social context.

To answer this question a set of steps shall be followed. This research uses steps described by Johannesson and Perjons [93] and can be seen in figure 2.1.

Each step represents a sub-question in the research design. One adaptation to the original steps of Johannesson and Perjons has been made. Step 1 was originally named ”explicate problem” and has an output in the form of an ”explicated problem”. In this research design the first step is named ”describe system” and the output is a ”system analysis”. DSR described by Johannesson and Perjons, states that explicating the problem is ”about investigating and analyzing a practical problem. The problem needs to be precisely formulated and justified by showing that it is significant for some practice.” [93, p.75].

This has already been done in chapter 1. It was changed to more adequately describe the systems engineering perspective that is taken.

The first sub-question is:

*1. What is the current socio-technical system of targeting, identification and registration in Cash Transfer Projects in a humanitarian context?*

*1.1. What is the current technical composition of the system and how might that change due to blockchain?*

*1.2. In what institutional environment does targeting, identification and registration take place?*

*1.3. Which important stakeholders are involved in targeting, identification and registration?*

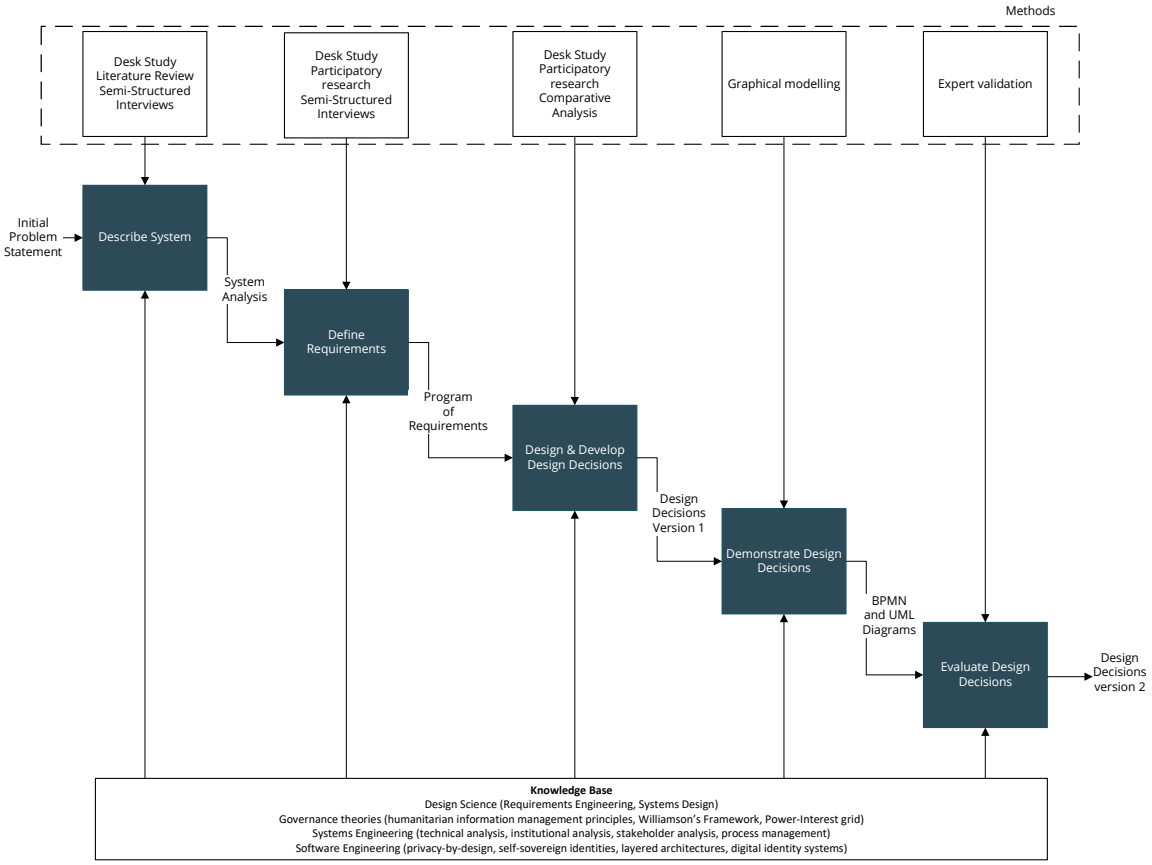



Figure 2.1: Flowdiagram adapted from Johannesson and Perjons [93]

The answer to this sub-question takes the form of a system analysis of the current systems and technologies available. This analysis consists of four different parts. First, the results of the literature review specifically for registration, identification and targeting are discussed. Second, an overview of the current technical system is given and what might change due to the introduction of a blockchain based system. Third, a sketch of the institutional environment is provided to enhance insights into what norms, rules, regulations and organizational structures exist. Fourth, a stakeholder overview in order to understand their preferences and how they will be involved in the system is given. Based on these four chapters, the scope for the program of requirements will be given.

The necessary data is derived from semi-structured interviews with cash delegates from the IFRC and other humanitarian organizations, and by conducting desk research. Semi-structured interviews can easily lead to abstract and off-topic answers, therefore an interview procedure is introduced before the start of each interview. Bycatch from the literature review, 26 reports and other gray literature

are consulted and complemented with information from the Cash Learning Partnership [2], the IFRC and Reliefweb[3]. To prevent an information overflow, which could result in confusion, a selection of the documents has been made in advance of the analysis.

The system analysis is used to set a boundary for what is seen as input for requirements engineering. Which leads to the second sub-question:

*2. What are the requirements that must be satisfied in a design?*

Based on the system analysis a set of requirements is established which can be used to evaluate and design a new system. Requirements are elicited, analyzed, categorized and prioritized. To understand what kind of requirements are necessary, this sub-question also describes in more detail the types of artifacts that will be used. The main research question already explains that some design choices have to be made and the objective points to creating a helpful tool for actually building a system. In DSR, an artifact can be one or a combination of the following: constructs, models, methods and instantiations [19]. In the upcoming paragraph decisions are presented on the type of artifact(s) which are further detailed as part of answering this sub-question.

Eliciting requirements is often a time consuming process and troublesome when stakeholders are difficult to reach. This is mitigated, by collaborating with the NLRC, 510, blockchain developers, cash delegates and other researchers in this project. A final program of requirements launches the next phase, in which the following sub-question is answered:

*3. Which design decisions have to be made?*

*3.1. What alternatives are available for the design decisions?*

*3.2. Which alternatives best satisfy the program of requirements?*

*3.3. Do the proposed design decisions match with the program of requirements?*

In 3.1. four similar systems shall be compared that were structurally chosen. In 3.2 an assessment of the alternatives is made and a selection is done on what to integrate into the design. The design is made and in 3.3. it is checked whether the requirements are sufficiently met. These questions are answered by conducting a comparative analysis and mapping the results against the program of requirements. The design is set up as a set of design decisions, which is also mapped against the program of requirements.

Once the system is designed, it has to be demonstrated. This is to prove the feasibility of the artifact and leads to the fourth sub-question:

*4. How can the design decisions be used in the an illustrative Cash Transfer Project?*

Unfortunately, due to time constraints it will be impossible to conduct a real-life pilot or witness a pilot as part of the participatory research. Therefore an illustrative and purely fictional case study is used, where Alice is living in an affected area and wants to register a digital identity in order to receive cash-based assistance from the Red Cross. Using process models a walk-through of the activities is given to demonstrate the workings of the system and by doing so, the design is self-validated. The last sub-question considers a wider validation of the design decisions.

*5. What is the value of the design decisions in a humanitarian context?*

Together with a set of technical and humanitarian experts the system design is validated and their feedback is used to improve the system design. To clarify, expert validation can be very informative yet also very subjective. It requires a clear format and is hard to generalize. A preferable option would be to make an instantiation of the system and test it in the field, this is not possible due to time-constraints but is recommended for future research.

[2] http://www.cashlearning.org/resources/library
[3] https://reliefweb.int/

## 2.4. Research Deliverable

This research produces the following deliverables:

1. A program of requirements to be used for distributed, federated or centralized system
2. A set of Business Process Model and Notation (BPMN) diagrams, which portrays the dynamic processes of the design decisions
3. A Unified Modelling Language (UML) Class diagram, which portrays the static architecture on which the business processes are build
4. A set of design decisions, which portray the trade-offs between requirements that have been made

The artifacts are represented in models, which can be used to support the construction of an instantiation of the system [93]. The program of requirements consists of several statements about what qualities the system must have or what functions the system must perform. Each requirement is escorted by a rationale statement, priority, unique identifier and source. The BPMN diagrams specify dynamic business processes. It has a standardized notation and has direct face-value for people that are not known with this type of modelling or with the processes. The UML Class diagram is an object-oriented modelling language which depicts the static state of a system. It is often used for the modelling of information systems and compatible with software intensive designs [147]. UML Class is a standardized language which allows for widespread interpretation and has an adequate annotation for public, private and protected data that is suited to demonstrate the use of personal identifiable information. UML Class provides the blueprint for a technical design, BPMN provides the blueprint for stakeholders. The design decisions are a prescriptive set of statements, with its implications and limitations. They are based on important choices between requirements on the architecture, roles, interfaces and governance of the system. The design decisions are the main representation of a system design in this research.

## 2.5. Societal Relevance

The societal relevance of this research is found in creating a global digital identity system for the sake of helping people in need. It are exactly these people that can benefit most from inclusion in a cash-based program and it is their need for aid that legitimizes the development of a system design. If the system is designed to also assist people in acquiring other types of assistance, potentially non-humanitarian, its societal relevance increases. This research also holds societal value in that it is partly conducted at the NLRC and 510, for whom it could give enhanced insights into developing their own system.

## 2.6. Scientific Relevance

Based on the literature review documented in appendix A and the results that are presented in the next chapter, the main knowledge gap is derived:

> What we know is that targeting, registration and identification is time-intensive, expensive, complex and access dependent. We know there is a lack of accessible and trustworthy information. We know there are several ways to target and it starts with a geographical boundary. We know that targeting introduces corruption, fraud and uncertainty. What we do not know is how to improve it using technology and in specific blockchain technology.

This research fills this gap as it presents four artifacts that help understand how it can be improved and help the humanitarian sector collaborate on scaling up the use of CTPs.

# 3

# System Analysis

*"Complexity is your enemy, any fool can make something complicated. It is hard to keep things simple."* - Richard Branson

This chapter answers the first sub-question of this research: *1. What is the current socio-technical system of targeting, identification and registration in Cash Transfer Projects in a humanitarian context?*. To answer this question a combination of desk research, a literature review and semi-structured interviews with cash delegates from the humanitarian sector were used. An overview of the interview protocol, list of questions and interviewees is presented in appendix B. The answer to sub-question one takes the form of a system analysis using a *technical*, *institutional* and *stakeholder* analysis.

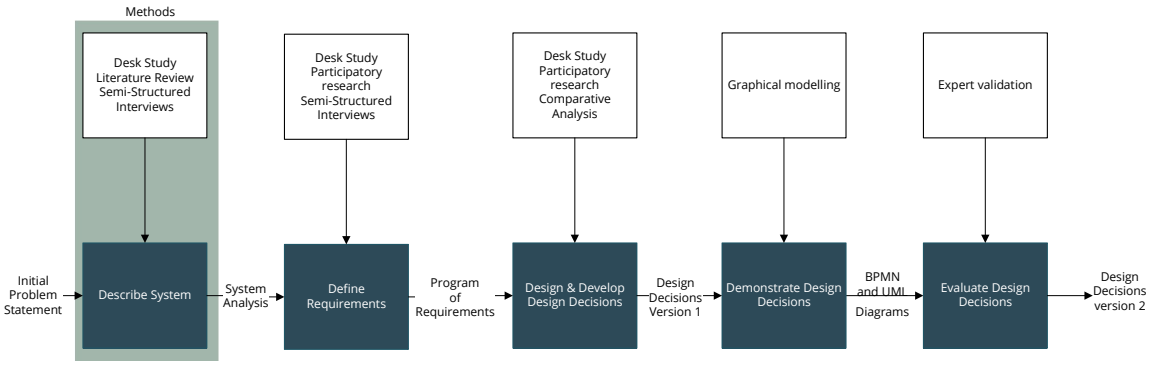



Figure 3.1: Methods for System Analysis

This chapter starts with explaining the use of a system analysis in paragraph 3.1. Then the results of an academic literature review on targeting, identification and registration in protective CTPs is presented in paragraph 3.2. Subsequently, a technical analysis which embodies the current state of identity information management systems in the humanitarian sector is shown in paragraph 3.3. In paragraph 3.4 the institutional analysis is provided and in paragraph 3.5 the interdependent network of stakeholders in this system is discussed. A sub-conclusion is given in paragraph 3.6.

## 3.1. Introduction to System Analysis

A system analysis is a systems engineering tool to get an integral view of the system-of-interest. Since information systems are never just about the technical side, but also about user behavior, rules and regulation it is of importance to get an understanding of these various aspects. The content in chapter 1 confirms this as a variety of technical and institutional barriers in CTPs but also in blockchain technology are to expected. Hence, looking at the technical and institutional side of the system and complementing this with the stakeholders involved, ensures a solid foundation for a later integral system design.

One approach is to take the scope of a Technical, Institutional and Process (TIP) analysis. The technical analysis focuses on the current technical systems in place. Since the scope of this research

is on registration, identification and targeting, these systems are to be (digital) identity management systems. The institutional analysis aims to give an overview of the formal and informal regulations that apply when conducting CTPs and running identity management systems. The stakeholder analysis provides an overview of all the actors that are involved in the humanitarian ecosystem, identity management ecosystem and blockchain ecosystem. Additional to the TIP approach, this system analysis incorporates an academic literature review. The review presents fifteen case studies on CTP and explains in detail what targeting, registration and identification consist of. This gives a more profound understanding of the CTP system.

## 3.2. Literature Review

Targeting, identification and registration within the CTPs in a humanitarian context has been part of scientific research, foremost in evaluative case studies. To have a better understanding of the academic literature on this topic a literature review was conducted. The full results can be found in appendix A.

There were several criteria for including studies into this review. First, as the research into CTPs has significantly increased as of 2004 (after the tsunami in the Indian Ocean), this was used a lower boundary for publication dates. Second, only articles written in English were selected. Third, articles were scanned on the use of CTP as one of their main interventions in order to extract challenges directly related to CTPs and not to other interventions. Fourth, the CTPs had to be used in a protective humanitarian context. Applying these criteria to 30.000 search results from SCOPUS, SUMMON and ScienceDirect led to 3 academic journals. Through backward snowballing in the academic journals and grey literature that was found, applying the same criteria, a final result of 15 studies were included. This is a small number of results and limits the generalization of the review. The selection of studies is presented in table 3.1.

Table 3.1: Overview of included articles in literature review

| Authors | Year | Study design | CTP Type(s) | CTP Size | Targeting & Registration |
|---|---|---|---|---|---|
| Aker [5] | (2017) | Case Study, Eastern DRC, emergency response | UCT<br>Voucher | 474 households | Community Based Selection |
| Ali and Gelsdorf [6] | (2012) | Case Study, Somalia, lessons learned | UCT<br>Voucher<br>Cash-for-Work | 1.700.000 beneficiaries | Categorical Selection, Community Based Selection |
| Bailey and Walsh [14] | (2007) | Case Study, DRC, non-acute emergency response | CCT | 40 households | Lottery, Self-selection |
| Bedran-Martins and Lemos [20] | (2017) | Case Study, Brasil, emergency response | CCT | 221 households | Categorical selection |
| Brooy [30] | (2007) | Quantitative & Qualitative economic review, emergency response, effect on local economy | n/a | n/a | n/a |
| Davies and Davey[42] | (2007) | Case study, Malawi, emergency response, effect on economy | UCT | 10.000 households | n/a |
| Doocy et al. [51] | (2016) | Case Study, Syria, exploration for expansion | UCT<br>Vouchers | 34 households | Categorical Selection |
| Fenn et al. [60] | (2015) | Case Study, Niger, emergency response, effect on nutrition | UCT | 412 households | Categorical selection, Vulnerability Assessment |
| Jelle et al.* [92] | (2017) | Case Study, Somalia, emergency response, effect on malnutrition | UCT | n/a | Vulnerability Assessment |
| Kebede [96] | (2006) | Case Study, Ehtiopia, emergency response, comparison with food aid | UCT<br>Cash-for-Work | 128.260 beneficiaries | Categorical Selection, Categorical Selection |
| Kelaher and Dollery [97] | (2008) | Case Study, Indonesia, comparison with food aid | UCT<br>CCT<br>Vouchers<br>Cash-for-Work | 15122 beneficiaries | Cateogrical Selection |
| Langendorf et al. [102] | (2014) | Case Study, Niger, emergency response, effect on food security | UCT | 5.395 beneficiaries | Categorical Selection |
| Lee [104] | (2012) | Case Study, Somalia, emergency response, review CTP | UCT | 13.830 households | n/a |
| Mattinen and Ogden [108] | (2006) | Case Study, Somalia, emergency response, review CTP | Cash-for-Work | 4029 households | Categorical Selection, Community Based Selection, Vulnerability Assessment |
| Pega et al.** [125] | (2015) | Systematic Review | UCT | Study 1: 1200 households<br>Study 2: 5395 beneficiaries | Categorical Selection |

* Future Study Protocol
** Systematic study including [5] and [102]

In table 3.1 it shows that among the selected studies 13 are country-specific case studies; Brazil, Democratic Republic of Congo (2x), Ethiopia, Indonesia, Malawi, Niger (2x), Somalia (4x) and Syria. It shows that there is some global coverage on protective CTPs. Also, as many CTPs are context specific, four studies from Somalia might distort the general picture. There was also one study that did research on CTP as an emergency response and its effect on local inflation and one study conducting a systematic review.

The studies varied significantly in size of the CTP program. The largest study describes a CTP benefiting 1.700.000 beneficiaries in Somalia and the smallest covers 34 households in Syria. Again, this

emphasizes the local context of CTPs. Hence comparing these programs is difficult. In eleven studies unconditional cash was used, in three studies conditional cash was used, in four studies vouchers were used and in four studies cash-for-work was provided as a CTP type. Most of the studies prefer working with unconditional cash, yet other types of CTP are also practiced. Unfortunately, in none of the studies a clear step-by-step approach could be distilled into how targeting and registration took place in the field. Because of this and the context specificity of these programs, the literature was used for eliciting challenges with targeting and registration, which were subsequently generalized on a very abstract level. This step is seen in the tables in appendix A. From here on, the generalizations that could be made from the literature are used to further discuss targeting and registration.

Each CTP starts with a geographical selection of the affected area. Then a set of inclusion criteria is set up and the choice is made to select households, individuals, communities or living clusters (more than one family). These criteria can be distinguished as [127]:

- Context specific, e.g. lost their homes or crop/livestock
- Social Welfare, e.g. individuals are chronically ill, households are child headed, households that have no income
- Specific vulnerable groups, e.g. internally displaced persons (IDP), refugees or specific livelihood groups

In the majority of studies the focus was first on a community and then on households or individuals within that community. In nine studies categorical selection took place. There was a mixed use of criteria, such as malnourished children [6], income [20], poverty [60, 96] and livestock [108]. In four studies community-based targeting was used [5, 6, 96, 108]. This method lets humanitarian organizations team up with local communities and use local knowledge to determine who should receive the aid. Three studies specifically focused on vulnerable groups and in one study self-selection was used, followed up by a lottery to determine who was included. When focusing on vulnerability assessments often local communities are also involved in setting up the criteria, the difference with community based selection is that the final selection is made by the humanitarian organization.

Ali and Gelsdorf mention that targeting the poorest is time-intensive, expensive, complex and dependent on accessibility [6]. This was confirmed in the studies done by Davies and Davey, Jelle et al., Mattinen and Ogden and Pega et al.. Another general note is the dependence on data quality for precise targeting in an unstable environment [30]. Community based targeting may provide a solution here due to incorporating local knowledge, but can also be socially divisive as communities have their own internal bias and thus lead to exclusion of vulnerable people [97]. Kebede finds that targeting errors might make the most vulnerable even worse off. Since beneficiaries receiving cash can now buy goods and services, it becomes even harder for the most vulnerable to acquire their minimal necessities. Targeting errors might also occur due to geographical targeting, when within the affected area certain locations are chosen over others due to inaccessibility and limited resources [14]. Davies and Davey note that categorical selection is often difficult as people hold multiple (seasonal) jobs, multiple partners, have seasonal spending and move from locations. A last remark is that targeting for CTPs is different than targeting for in-kind aid. Hence, staff needs to be retrained [97].

Looking at other design components interdependencies appear. First, if the design objective is to measure the effect of CTPs on a dependent variable such as health or equality, one needs not only be able to target the beneficiary but also to register personal information. This requires coordination between *local communities* as they can assist in validating identities, *(local) governments* as they are issuers of ID's, land titles and birth certificates, *beneficiaries* as the supplier of information, *humanitarian organizations and volunteers* as the registrars of this information and many others. Coordination is not only vital for research purposes but in general to the success of CTPs [6, 51]. Second, in the majority of studies physical cash was used as a transfer mechanism. This comes at a security risk, as some areas are inaccessible. So if cash is the preferred method these areas might be overlooked and not targeted and registered. In one study mobile cash was used, so beneficiaries at time of targeting have to possess a mobile phone and could potentially be reached via this mobile number for more information and further registration. This is of course context dependent. Third, monitoring & evaluation is highly dependent on the traceability of beneficiaries. For a valid and comparable evaluation, baseline information gathered during targeting is essential. Fourth, the time frame and frequency of a CTP

determines the duration of safekeeping and storing personally identifiable information (PII). Finally, there are many complementary programs (non-CTP and CTP) in affected areas [30]. This can increase uncertainty for targeting and for registered beneficiaries to what aid they are entitled to. It also results in more costs, as all programs are targeting people, while protecting PII [6].

## 3.3. Technical Analysis

The literature review has described the known challenges of targeting and registration. Yet, there is clarity needed on what registration, identification and targeting involves from a technical perspective. In order to design a technical artifact the current functional and non-functional characteristics of the systems and technologies need to be understood, as a new artifact will (likely) incrementally replace the existing ones. This section therefor aims to answer sub-question 1.1.: *What is the current technical composition of the system and how might that change due to blockchain?*

### 3.3.1. Identities and Identity Systems

Targeting and registration is intertwined with the concept of identification. Atick et al. states the following about identification in programs like CTPs:

> ”When mechanisms for identification are weak, individuals may experience difficulty proving their eligibility for social protection assistance. Without a common identity, coordination among different development programs on the identification of potential beneficiaries becomes more difficult and costly. Invariably, multiple databases result, with beneficiaries’ identities not necessarily linked across them. These programs become vulnerable to misuse and sizeable leakages.” [11, p.3].

Hence, understanding the concept of identity and identification, serves as a necessary start to design a system that aims to deal with the challenges found in the literature review and described by Atick et al. [11].

*Identity* is a social construct and has not been captured by a single definition. It is dynamic, as it depends on the environment and reason for which it is used [140]. It is the aggregate of personal and psychological features, physiological appearances, our environment and more [152].

Identity and reputation are interwoven, where knowing someone establishes trust in a given community. The use of identity as a proxy for trust becomes more crucial, when people commence in relationships without knowing their counterpart from a given community. Systems which assist in building trust proxies are based on the use of passports, identity documents, a password or PIN code, all grouped under the term ID token. ID tokens are then used for confirming a person’s identity.

In many societies mankind is familiarized with this concept by the institutionalization of identification by governments, in which identity attributes (e.g. biometrics, birth certificates, land-titles) are registered and issued as a legal identity. These legal identities are often a very strong trust proxy and can be used to identify yourself at government departments, banks, telecommunication operators, insurance companies and the like [63, 140].

A system that identifies and registers people is called an *identity system* and is a mix of databases, IT infrastructure, processes and procedures to establish identities [145]. An *identity management system* is ”a combination of technical and business systems, policies, and processes that is used to enable, govern, and synchronize the collection, utilization, and safeguarding of identity information.” [134, p.532]. The main purpose of an identity management system is to have a credible and scalable process of appointing and empowering identity attributes to an individual [134].

When investing in these systems USAID distinguishes between functional and foundational purposes (see figure 3.2). A system with a functional purpose provides identities for a specific function, they may be linked to other ID systems, where a system with a foundational purpose provides identity as a public good [152]. In areas where for some reason foundational systems are not working, functional systems might perform that role [152]. Also a functional system might grow to become or fulfil parts of a foundational system. The second distinction is between instrumental an infrastructural systems. Instrumental systems are often limited to a single project, hence they have a functional purpose. Infrastructural systems are either functional or foundational and built for the long run.

Developing countries often lack a robust identity system, coming short in supplying their citizens with official documents and ultimately leading to an ”identity gap” [140]. It is in these countries that

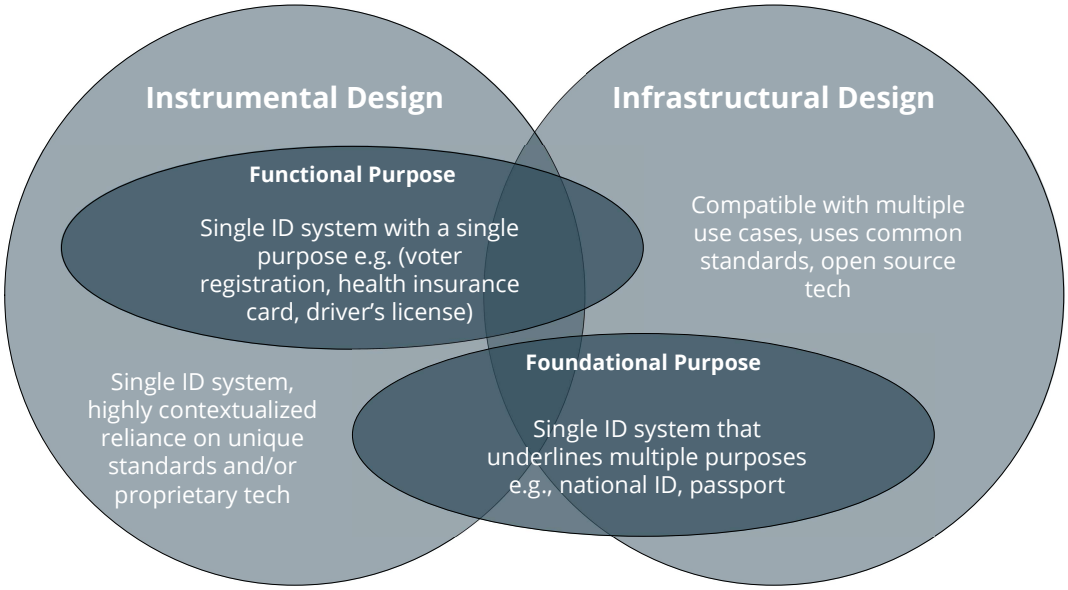



Figure 3.2: Characteristics of ID Management Systems from USAID [152]

many protective CTPs are initiated. The issue of the identity gap is long-lasting since in developed countries identity systems have evolved over time and needed to mature, while in developing countries the need is urgent and in emergency situations very urgent. So to close the identity gap, countries and humanitarian organizations are attempting to exploit digital technologies and build entirely new systems which includes biometric identification, smart cards, mobile IDs and online signatures [145]. These digital technologies pave the way for the usage of digital identities and digital identity systems.

### 3.3.2. Digital Identities and Digital Identity Systems

A digital identity is "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and is used for electronic transactions" [144, p.11]. A digital identity system is defined as "the systems and processes that manage the life-cycle of individual digital identities" [144, p.11]. Digital identification could leapfrog the inefficiencies from paper-based identification systems in developing countries, yet issues with data protection, privacy and design choices have to be dealt with [145].

The World Bank Group [145] states there are four steps in a digital identity system as can be seen in figure 3.3. Arjen Crince, a former information manager with a CTP in Nigeria (see appendix B.3) emphasizes that this last step "digital ID use and updating" will prove to be a true challenge in a humanitarian context. The life-cycle starts with the registration of the *identity owner* (end-user in the figure) by the *identity provider*. Registration consists of enrolment and validation. In enrolment key identity attributes (passports or birth certificates, biometric data and even social profiles) are recorded, which ones have implications for the trustworthiness of the identity and its interoperability with other identity systems [145]. It answers the question "Who are you?". Validation is the check of the given attributes by the identity owner with existing data coming from an *attribute provider* (e.g. biometric databases, national identity systems, humanitarian organizations). After validation a digital identity is created, which answers the question "Are you who you say you are?". In the next phase the credential is issued. Subsequently, the phase in which the identity and credential are used takes place. Authentication is about the identity owner demonstrating his or her control over the digital ID, by using the credentials to receive access to a service provided by a *service provider*. Different *authentication providers* can support this process, for example cloud services or suppliers of smart card readers. Updating digital identities, i.e. for newly acquired land or college degrees is then again done by the identity provider. In some systems authentication is incorporated into the activities of a service provider.

The architecture of such a digital identity system can have different forms. Nyst et al. [113] distin-

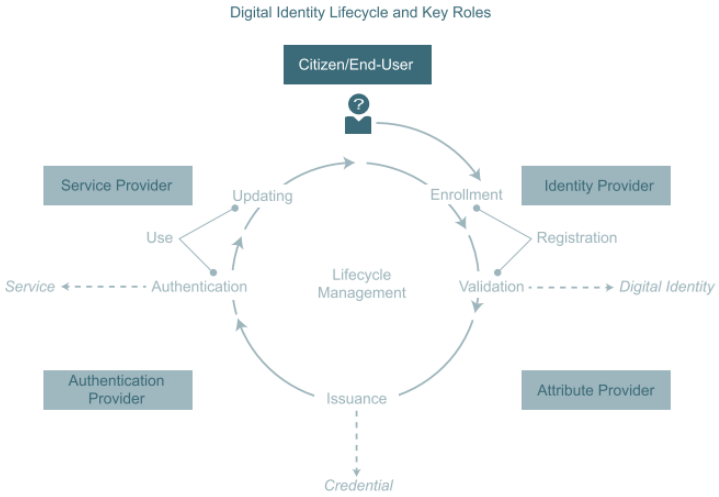



Figure 3.3: Digital Identity Lifecycle and Key Roles from The World Bank Group [145]

Table 3.2: Overview of Digital Identity Systems Architectures Nyst et al. 2016

| Architectural Model | Examples | Architectural characteristics | Positioning | Key privacy threats |
|---|---|---|---|---|
| Monolithic Identity Provider | Facebook, Google | Identity provider does Identification and Authentication; Market Dominance | Highly centralized, less privacy enhancing | Data breach<br>Individual surveillance<br>Mass surveillance<br>Passing of personal information to unvetted parties<br>Personal information made public |
| Federated Identity Provider | GSMA Mobile Connect, Open ID Connect, PayPal, Amazon | Identity provider does Identification and Authentication; Many Identity providers in the market | Slightly centralized or decentralized, less privacy enhancing | Data breach<br>Individual surveillance<br>Mass surveillance<br>Passing of personal information to unvetted parties |
| State issued e-identity cards | Estonia eID, Nigeria eID and the like | Government is identity provider; role of middle-ware | Centralized, more privacy enhancing | Identity theft<br>Data breach<br>Mass surveillance<br>Poor operational security<br>Poor operational processes |
| Brokered identity providers | UK verify, US GOV Connect | Government accredits multiple identity providers; Role of Hub to protect privacy | Slightly centralized or decentralized, more privacy enhancing | Identity theft<br>Data breach<br>Individual surveillance<br>Mass surveillance<br>Passing of personal information to unvetted parties |
| Brokered credential service provider | Canada Credential Broker Service | Credential service provider does authentication; Identification and authorization by service provider | Slightly decentralized, more privacy enhancing | Mass surveillance |
| Personal identity provider model | MyDex, Meeco, Microsoft u-Prove | Personal data store / user agent controls authentication that provides access to attributes that are then shared with service provider | Highly decentralized, more privacy enhancing | Identity theft<br>Individual surveillance |
| No identity provider model | Bitcoin, various blockchain identity start-ups | No identification takes place; Authentication and authorization are publicly available | Highly decentralized, more privacy enhancing | Identity theft<br>Individual surveillance<br>Mass surveillance |

guish between seven architectural models, where identification, authentication and authorization are executed in different configurations, an overview is provided in table 3.2. The overview shows the differences with respect to centralization versus decentralization, while also presenting the key privacy threats for each model. A group of private and non-profit organizations coordinates the standardization of such architectures, with the intention to increase interoperability and develop open identity solutions [144].

As of now most digital identity systems are based on a rather centralized or federated model [55, 134, 162]. For clarification, in these models a single entity controls the system, where the issued identities themselves can be used beyond this single entity but this is not always the case. An example, in affected areas humanitarian organizations register people digitally and hand out smart cards that are sometimes limited to the use for a single project but can also have multiple purposes for different projects according to one anonymous interviewee (appendix B.3). There are also other burdens when it comes down to digital identity systems such as not using minimal viable data sets or ignoring mandatory informed consent of the individual. Other issues are incomplete anonymization of data before sharing or opening up the data set leading to linkable identifiers and storing data unnecessarily or for too long [140].

### 3.3.3. Standards for Digital Identity Systems

The National Institute of Standards and Technology (NIST) has published an extensive set of digital identity guidelines, which serves as a handbook for organizations developing digital identity systems [67]. As stated, guidelines and standards are necessary for the interoperability and scalability of systems. The document details requirements to assist organizations in avoiding [67, p.17]:

1. Identity proofing errors
   (a) The impact of providing a service to the wrong subject
   (b) The impact of excessive identity proofing, or collecting too much personal information
2. Authentication errors
3. Federation errors

For each of these errors the NIST proposes an assurance level and a decision framework to assert which assurance level is needed. For the sake of clarity, there are three Identity Assurance Levels, three Authenticator Assurance Levels and three Federation Assurance Levels. Depending on the outcome of the decision framework, provided by the NIST, a level is chosen and the accompanying guidelines should then be asserted in designing a digital identity system. Other assurance frameworks can be found in the ISO/IEC[1] 29115, the FIDO UAF[2] and the eIDAS[3] from the European Union.

A report by the World Bank Group on "Technical Standards for Digital Identity" provides an overview of technical standards for interoperability [145]. In short, the report describes six categories of standards [145, p.9]:

1. Biometrics Image Standard; which differs for face images (PNG, JPEG, JPEG2000) and fingerprint images (PNG, JPEG, WSQ)
2. Biometrics Data Interchange Format; ISO standards per type of biometric
3. Card/Smart Card; different standards for cards with a chip (contact and contactless) and cards without a chip
4. Digital Signatures; depending on the use of the signature
5. 2D bar code; for example PDF417 or QR
6. Federation Protocols; SAML, Open ID Connect or OAuth are frequently used

There are also database system standards such as the ISO/IEC 18014 and cryptography standards such as SSH, PGP and SHA-256 that could be conformed with [100]. ISO is also working on some blockchain standards in ISO/TC 307, but these are not published yet. Which standards are applicable depends on the specifics of the system design. Using these standards is not compulsory, but it can enhance the scalability and interoperability of the system.

Kim Cameron, of Microsoft, described a set of seven laws for digital identity management [32, p.6-11]:

1. *User control and consent*: "technical identity systems must only reveal information identifying a user with the user's consent"
2. *Minimal Disclosure for a Constrained Use*: "the solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution"
3. *Justifiable Parties*: "digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship"

[1] International Organization for Standardization
[2] Fast IDentity Online Universal Authentication Framework
[3] electronic IDentification, Authentication and trust Services

4. *Directed Identity*: "a universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles"

5. *Pluralism of Operators and Technologies*: "A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers"

6. *Human Integration*: "the universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks"

7. *Consistent Experience Across Contexts*: "the unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies"

Even though these laws exist and can be applied, it is difficult to imagine that there will be a perfect system that is pareto-optimal and offers inclusivity for all [113], however this does not imply that a digital identity system should not aim to address these 'legal' principles.

### 3.3.4. Cash Transfer Projects and Digital Identity Systems

Humanitarian organizations are dependent on identity management for targeting, identification and registration in CTPs to optimize their services and establish whether a beneficiary is an eligible recipient of a CTP. However, as seen in the literature review many CTPs are designed with a specific objective in a local context. As such their identification systems have a functional purpose. Some of these systems are not even digitized. Aneel Ahmed from Concern Worldwide in Pakistan, mentions that their government does not have a digital identity system where they can subtract potential beneficiary lists from so Concern Worldwide does not use any form of digital identity but works with excel sheets (appendix B.3). Other organizations and countries are further ahead. An anonymous interviewee, explains they use a digital cash platform system which is integrated with a nationwide humanitarian information management system (appendix B.3). When asked if there is collaboration between organizations to share beneficiary data in a safe way, she states this is not the case. This was a reoccurring theme in the interviews, whether it was based on trust, differing assurance levels of each other's processes or diverging data responsibility policies, there was little interoperability between digital identity systems in the humanitarian sector. Ko and Verity [98] confirm this finding as they state that information silos between multiple humanitarian actors pose key barriers to effective information management, hence interoperable digital identity systems remain scarce. Van De Walle and Comes [153] demonstrate this by comparing the theory and the reality of the "Principles for Humanitarian Information Management" from UN OCHA for the cases of large scale emergency response in Syria and the Philippines. They mention there was no information sharing agreement which led to international NGOs protecting their data. The same study also presents the tension between standardization in information management and the dynamic context of emergency response, which in some cases demands flexibility. The study showed that different formats will be used to fill up the unintentional gaps, which later leads to hardships when merging datasets or the unwillingness to collaborate or share data [153]. Ergo, a technical design should allow for some flexibility and has to deal with coordination issues in the local context as well as governance of the identity system as a whole.

Some information management systems are developed specifically for the humanitarian sector. These systems offer a variety of services and other notable examples can be found in organizations using REDROSE[4], LMMS from World Vision[5], SCOPE from the World Food Programme[6], BIMS from the UNHCR[7], Commcare from Dimagi[8] and PIRS from the International Organisation for Migration (IOM)[9].

Besides organizations providing full identity management systems, there are also applications that serve only for the registration of data. Rebecca Visschedijk of the Netherlands Red Cross, mentions

[4] https://www.redrosecps.com/
[5] https://www.wvi.org/disaster-management/last-mile-mobile-solution-lmms
[6] http://documents.wfp.org/stellent/groups/public/documents/communications/wfp272586.pdf
[7] http://www.unhcr.org/protection/basic/550c304c9/biometric-identity-management-system.html
[8] https://www.dimagi.com/commcare/
[9] http://cb4ibm.iom.int/ibm/index.php/2012-06-13-02-09-37/pirs-the-personal-identification-\
and-registration-system

that for a CTP in Nigeria they used KoBo[10], to build up registration forms (see appendix B.3). KoBo is a service provided by UN OCHA with a 1 month set up time, it is free to use and build on the Open Data Kit (ODK) framework. Another example is, iFormBuilder[11], this is a Software-as-a-Service (SaaS), which allows for using third-party applications but at a significant higher cost ($15k) compared to KoBo. A last example is that of CommCare[12], this humanitarian information management system was developed specially for aid workers in remote areas with limited infrastructure. It also uses the ODK framework and has a case management function, where different projects can be run alongside with beneficiaries assigned to each project.

The systems described above are used for registration, identification and targeting (more limited though), yet there is more to it. Systems like these gather data which "facilitate various institutional process improvements, such as data-driven decision making, increased efficiency, or greater transparency and accountability. These process improvements, in turn, enable the system to contribute to functional goals" [152, p.19].

Paula Gil Baizan, with over 14 years of experience with CTPs at various humanitarian organizations, mentioned in an interview that although all these digital identity systems for the humanitarian sector exist, there is one aspect consistently overlooked (see appendix B.3). She states that new systems are developed and humanitarian services are optimized, but they also reinforce the monopolistic position of humanitarian organizations in targeting, validation and updating of digital identities. Wolfond states that "neither authentication nor identity registration are a source of competitive advantage for anyone – in fact, lack of consistency is a source of risk business and a frustration for customers"[162, p.37]. This might be the case for the private sector, but based on Gil Baizan's statement this is a cornerstone of the humanitarian sector and might prevent the development of a radical innovative system. On the contrary, one could also plea for a less radical innovation as the technologies used in such innovations are often nascent and once understanding improves could prove to be harmful, especially when the people involved are extremely vulnerable.

### 3.3.5. Blockchain and Digital Identity Systems

The challenges digital identity systems face in a centralized or federated architecture can be distilled to security, privacy and usability [91]. Blockchain might offer a solution to these challenges by delivering a secure alternative, where no trusted central authority is needed [91]. The shift away from a centralized or federated system to a distributed systems has some advantages as mentioned by Dunphy and Petitcolas [55, p.2]. To start (1), depending on the structure of the blockchain, there is no single authority in control or single owner of the data. A blockchain is tamper-resistant (2), which allows for individuals to build up an identity and it allows for inclusiveness (3), as there are new ways to bootstrap user identity outside the existing channels. Also, shared identity systems can lead to cost saving (4) by reducing operational activities. Lastly, blockchain provides control over the digital identity to the individual instead of the institution (5). In other words, using blockchain may help in reducing the need for trust between stakeholders, build a secure value transfer system, streamline business processes across multiple entities and increase record transparency and easy of auditability [81, p.15]. Specific for digital identity systems, Wolfond states "No single organization or industry can solve the identity challenge alone. It takes a village to make identity." [162, p.37]. As such, blockchain could pave the way for secure data sharing and collaboration in information management across the humanitarian sector.

#### Ownership of digital identities

The relation of blockchain to digital identity management becomes clearer when the concept of ownership is introduced. Ownership involves three components: the owner, the object owned and a trace of the owner owning the object. For some objects it not necessary to have a formal trace of this, but when it comes down to passports or land titles registering who owns what becomes vital and is often institutionalized. To do so, the owner and the object have to be identified. Drescher provides an overview in figure 3.4 of the concepts of ownership which clarifies how identification, but also authentication or validation and authorization is part of ownership as well as part of digital identity systems as described previously.

[10] http://www.kobotoolbox.org
[11] https://www.iformbuilder.com/
[12] http://www.commcarehq.org/home/

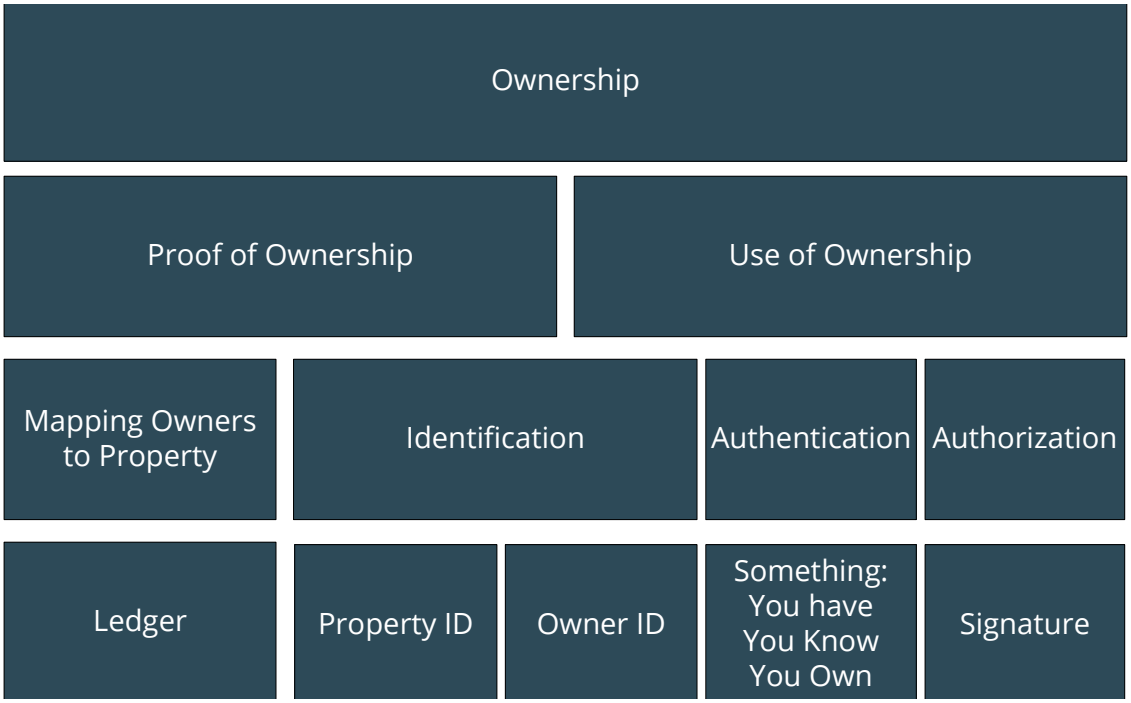



Figure 3.4: Concepts of ownership from Drescher [52]

Projecting this diagram onto CTPs, indicates that ”property ID” would be the identifier for the cash that is send to beneficiaries and ”Owner IDs” could be institutionalized IDs or a range of functional IDs depending on the context. On the ledger the transfer of cash to the ID of the beneficiary will be registered. So the ledger has two roles, to proof ownership of the cash or the identity and to transfer ownership of the cash. This demonstrates the tension between transparency and privacy, as to proof ownership identities have to be readable but one should also protect identities as they are linked to what people own, which is private information. In a purely distributed network, no single entity owns the ledger in a more private network with access regulation it could be that there is an entity ultimately owning the ledger even though the nodes are distributed across the network.

### A Layered System

Blockchains can be categorized in three essential layers [100]. The first is the *blockchain layer*, this is the underlying data structure. This will inform how and when data is stored, as well as the use of public key cryptography, which uses a public-private key pair to encrypt and decrypt data [100]. The key pair can be used for digital signatures, hence to authenticate ownership of a digital identity attribute. Traditionally trusted certificate authorities certified the ownership of these key pairs, but new encryption models like ”Pretty Good Privacy” are based on decentralized authentication models. This is an older version of encryption but is revived by the use of time-stamps. These time-stamps denote a clear chronological order. Blockchain is almost immutable, because these time-stamps are combined with the use of hashing. This hashing process ”transforms any kind of data into a number of fixed lengths, regardless of the size of the input data” [52, p.72]. This facilitates the storage of data in a secure way, the use of digital fingerprint of transaction data and creates a significant computational barrier so the data structure becomes very difficult to change [52]. A transaction in a digital identity system would be that of sharing digital identity attributes, this does not mean that these attributes are stored on the blockchain.

The second layer is the *network layer*, which ”consists of the actual peer-to-peer (P2P) network that brings a distributed ledger to life by connecting participants” [81, p.26]. The network can be specific for a use-case or an organization. The layer is concerned with the verification and transmission of data, either in an unstructured or structured P2P network. According to Oualha et al. [120, p.2] the purpose of a P2P storage system is ”to guarantee the potential retrieval of data. Since data are not stored in a centralized server and since P2P networks are assumed to be very dynamic, the stored data

should be available even if peers may leave the network. Data availability can be increased with data redundancy techniques. Data should not only be available at any time but also preserved in the long term. Data integrity thus has to be ensured and, in case of errors, a peer should be able to detect the compromised data."

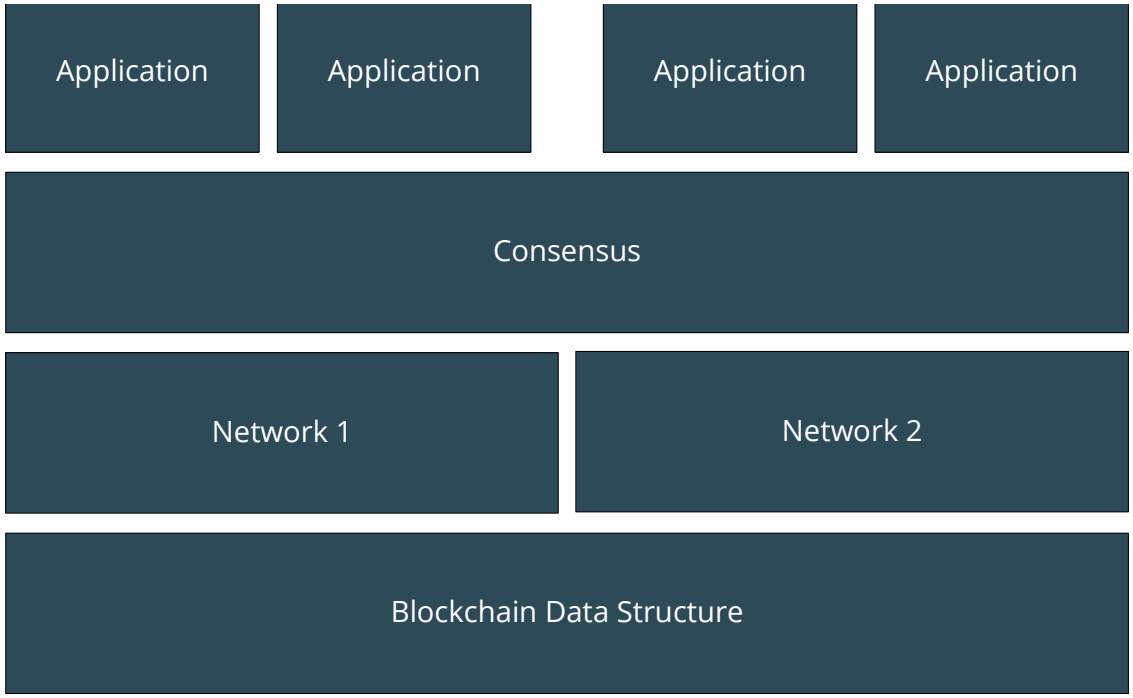



Figure 3.5: Blockchain Layered Model

The *consensus layer* is the third layer and is concerned with the procedure of how nodes in the P2P network agree on a single ledger, in specific on new transactions added to the ledger, how the ledger is stored and who stores the ledger. The consensus layer can be directly linked to the first layer and integral for all networks, but can also be specified for a specific network. Different consensus algorithms exist. There are a few consensus algorithms based on mining of tokens (proof-of-work, proof-of-stake) which is only necessary if there is a public permissionless blockchain, some are based on tokens but do not depend on mining (Tendermint, Ripple Protocol Consensus Algorithm) and others function for more private blockchains (Byzantine Fault tolerance, Hyperledger and R3 Corda) [100]. A layer that is not deemed essential by Lai [100] but regularly mentioned is the *application layer* [81, 107]. This is the user interface for interacting with the blockchain. An overview of all the layers is provided in figure 3.5.

### 3.3.6. Criticism on Blockchain Technologies

Blockchain has been said to do many incredible things, but the hype is starting to fade out [157]. According to Baars [12, p. 25] the biggest challenges with blockchain are "privacy and confidentiality of transactions", both are deemed extremely important when dealing with identities on the blockchain. Especially with public blockchains where everyone has reading rights, no private data should ever be put on the blockchain but it must still be related to a single identity for the identity owner to use it. Also, public permissionless blockchains, due to their consensus protocols, require vast amounts of energy and will take ample time to generate new blocks [45]. Other technical challenges can be found in key management issues [101], where many stories exist of people loosing access to their cryptocurrency wallets. For already vulnerable people this should be avoided at all cost. Furthermore, interoperability and integration with existing systems is difficult for blockchain technologies, especially for business process applications [101]. This is directly associated with the immaturity of the technology, which means that in general there is still a poor understanding of blockchain [98]. This comes with a lack of programmers and software architects that have blockchain experience and a lack of standards [81]. According to a study conducted by Hileman and Rauchs [81] legal risks and a lack of regulatory frame-

works stand in the way of adoption, which is confirmed by Yeoh [164]. Even though the hype is fading away and potential use-cases are crossed off, one of the six main use-cases that remain is identity [33].

#### Self-Sovereign Identities

One of the identity concepts often referred to in blockchain based identity systems is self-sovereign identity. From a centralized to a federated to a user-centred system, self-sovereignty is about the concept of entities owning and controlling their own digital identity [12]. Various sets of principles are used to define what a self-sovereign identity should adhere to, a well-known set is proposed by Christopher Allen [9] and contains ten principles:

1. *Existence*: users must have an independent existence, a digital identity only makes limited aspects of an identity available that are already public
2. *Control*: users must ultimately control their identities, this means to refer to it, update it or hide it. Yet they must not control the claims or credentials issued by others.
3. *Access*: users must have access to their own data
4. *Transparency*: systems and algorithms must be transparent, both in how they function and in how they are managed. All must be free and open-source.
5. *Persistence*: identities must be long-lived
6. *Portability*: information and services about identity must be transportable also if issuers or identity providers change or disappear
7. *Interoperability*: Identities should be as widely usable as possible
8. *Consent*: users must agree to the use of their identity
9. *Minimalization*: disclosure of claims must be minimized
10. *Protection*: the rights of the users must be protected

As stated by Baars [12], most existing solutions are enabled by third-parties who supply proprietary technology thus making the portability, access and transparency principles difficult to achieve. As with Cameron's laws [32, p.6-11], it is unlikely that any system providing self-sovereign identities will perfectly match with these principles. Yet, they can still perform a guiding function and could be aimed for.

### 3.3.7. The Current Technical Composition

To answer sub-question 1.1. *What is the current technical composition of the system and how might that change due to blockchain?* a desk study and interviews were used. The current technical system is based on federated or centralized identity systems, some of these are digital yet others are paper based. To leapfrog the inefficiencies and maturity time of these systems in developing countries, newly designed digital identity systems are being developed. A digital identity system has a life-cycle consisting of three phases; registration, identification (validation) and use (authentication and updating). enrolment is about "who you are", validation is about "are you who you say you are" and authentication about "what rights do you have that you can claim". These systems have to adhere to certain technical standards and informal "laws" to ensure interoperability as described by Cameron [32], which should be included in any digital identity system as privacy-by-design, more on this in institutional analysis. In the field, targeting, identification and registration, can be paper-based or digital. Digital systems range from full-feature information management systems and cash platforms, to excel files and registration forms on tablets. Digital identity management and the current field-practices are challenged by three issues: security, privacy and usability. A new concept of digital identity systems, enabled by blockchain aims to solve these issues. Blockchain systems deal with ownership in the digital world by strong cryptography and distributed software networks. They consist of at least three layers: the blockchain, the network layer and the consensus layer. Often a fourth layer, the application layer

functions as the interface between the user and the other layers. Blockchain enables a user-centred system in the concept of self-sovereign identity.

To conclude, the current technical composition of the system is a federated or centralized (digital) identity system. Using blockchain it can change to a digital decentralized system having a **digital identity life-cycle** with roles for an identity provider, attribute provider and service provider. This system should adhere to **self-sovereign identity principles**. For the purpose of this research, the system should be blockchain based for which a **layered blockchain architecture** could be used. Technical standards for this system should be taken into account but are not part of the further research, as it is assumed this can be later dealt with.

## 3.4. Institutional Analysis

This analysis provides a structural overview and insights into the roots of institutions in the system environment. In particular it will lay out the formal and informal regulations, as well as cultures, ethics and norms. This is of importance as the institutional foundation of an identity management system for registration, identification and targeting should have the capacity to implement it and coordinate stakeholder groups [62, p. 138]. Gathering these insights is done by drawing upon institutional analysis frameworks and aims to answer sub-question 1.2.: *In what institutional environment does targeting, identification and registration take place?*

### 3.4.1. A Framework for Analyzing Institutions

Ronald Coase pioneered with the theory of transaction cost economics (TCE) [37]. Transaction costs can be defined as the costs of participating in a market, e.g. all costs that are not directly related to the unit price of a product. If these transaction costs exceed administrative costs (the costs of producing inside the firm), they cause uncertainty and occur frequently [126], than market-forces will stimulate vertical integration (the integration of two subsequent activities into one organization). This happens for two reasons. First, it is impossible to foresee everything that can happen on the market and dealing with contingencies is easier inside a firm. This concept is also called bounded rationality. Second, opportunism is less likely to ensue when two operations take place within the same organization [160]. This concept leads to the idea that organizations can be seen as more than a production function, they can be seen as institutions [159]. Institutions can be defined as "the humanly devised constraints that structure human interaction" [111]. This is an important notion as it illustrates the possibility of analyzing institutions, or in this case analyzing the humanitarian governance structure devised to target and register beneficiaries in CTPs.

North and Scott categorize the humanly devised constraints as formal rules (laws and regulations) and informal rules (norms, cultures and ethics). These formal rules are often regulative, where informal rules are cognitive or normative [132]. These concepts have been integrated by Williamson [160] into a four level framework where formal and informal rules are seen as *embeddeness*, the *rules of the game* and the *play of the game* (see figure 3.6) [160]. For this analysis level four shall not be analyzed as this is more context specific and as such would yield limited input for a generic system design. Within this framework level one, two and three will be used for analysis but first there is a need to understand the situation in which these rules apply.

In chapter 1 and the previous paragraphs in chapter 3 we demonstrated that the local context is very dynamic. Potential beneficiaries live in very diverse environments, from urban areas to refugee camps, from inaccessible to accessible and from disaster struck to conflict bound. The CTP design is context specific and determines the inclusion criteria, but in general beneficiaries that enter the system are in need of assistance, can be internally displaced or otherwise marginalized. They are affected by disaster. It is possible they have no access to a bank account, no legal identity documents, no smart-phone and are immobile. Beneficiaries might have lost relatives and livestock, could be illiterate and have possibly experienced a disaster before.

In the areas where a disaster has struck humanitarian organizations, international NGOs, local and national authorities and others, assist in providing aid. One of the types of aid that can be provided is cash based. As stated above, frequently information silos arise and there is distrust between these organizations, which prevents efficient collaboration. Also, personnel going in and out of the disaster areas do so on a frequency of 3 to 12 months, which does not always allow for a good transfer of their tasks, data storage and other processes [153]. Targeting and registration takes place in the areas

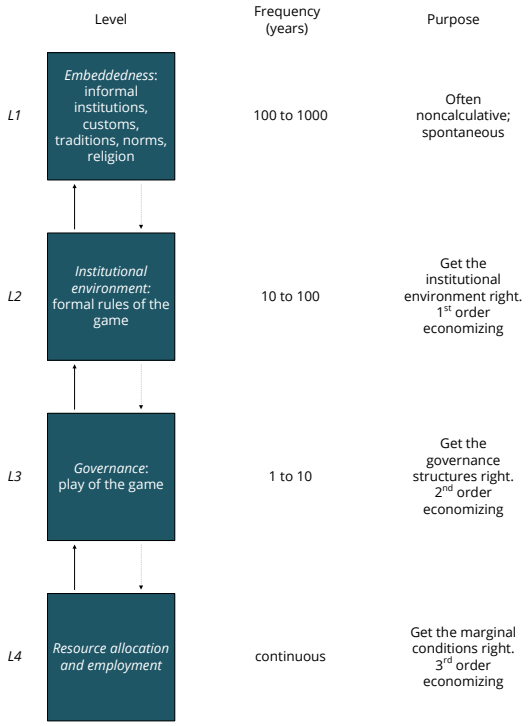



Figure 3.6: Williamson's Framework from Williamson [159]

in which beneficiaries reside. This sometimes implies there is no internet connection or electricity available, so paper based registration is also a back-up option but the aim is for digital registration, via tablets, smartphones and applications. If registrations take place in a refugee camp, there is room for more innovative tools. In a WFP program, registration took place using finger-scans and eye-scanners [122]. These two remain the two main digital identifiers, but some use facial recognition or biometric photographs as well [63]. Humanitarian assistance and the governance of it will also differ if it is an armed conflict or a natural disaster. Despite the local context or form of humanitarian assistance, registration, identification and targeting has to take place in order to find out who is eligible for which form of assistance. The registrations end up in a database, which can be centralized or offline, depending on how to verify and authenticate IDs [75]. To read, write and execute these databases software and hardware is used.

### 3.4.2. Level One: Embeddedness

Embeddedness is the concept of an informal institution, a custom, a norm or a tradition. They change over the course of hundreds of years. The norms on providing humanitarian assistance as a Western society could be categorized by two spokespersons: Jeffrey Sachs and William Easterly. Sachs believes that the developing world is trapped by poverty and that it can be saved with $75 billion per year [130], while Easterly thinks the white and western philanthropists of the current day and age will also fail in delivering effective aid and "throw away" another 2.1 trillion USD [56]. Easterly describes the "white man's burden" as the ancestral responsibility of imperialism that forces the west to do good for developing countries, whether this was based on religion, guilt or tradition remains vague [56]. In all, there is no common norm and presently there are faith based organizations, intergovernmental organizations and non-governmental organizations within the humanitarian sector and has it ceased to be an "only-Western" get-together. The norm had always been to provide those in need with food, materials and medical assistance, yet this is now also shifting to providing people with cash.

One could say that culture in the humanitarian sector is based on a shared set of values, beliefs, norms, symbols and language. In that sense the culture of humanitarian organizations is represented in

humanitarianism and its principles of *humanity*, *neutrality*, *impartiality* and *operational independence*. The UN OCHA set of icons and symbols is one of the depictions of this culture and although religious beliefs differ, the ultimate call to help people in need is approximately the same for each organization. In this view the humanitarian sector is protective of vulnerable people, also during targeting, identification and registration. Yet, there has not been a widespread adoption of protective measures as the integration with digital technologies handling information on beneficiaries is still relatively new.

With respect to the cultures, traditions, norms and religions of beneficiaries, these will be very diverse and should be looked at per CTP design. For example, rural villages in Africa will have longer lasting local traditions and norms, than would exist in one of the Greek refugee camps or in a small community in central-Asia that has been hit by an earthquake. Generalizing embeddedness for beneficiaries at this level would make little sense. Yet, many beneficiaries are likely to be aid-dependent, and as such there is a general acceptance on targeting, identification and registration where they freely give out their data, potentially not even understanding what consent means or what the implications could be. However, in some areas people have "NGO fatigue" due to the many inquiries and data collections going on in those places [58] or beneficiaries are weary of providing data because they think it is forwarded to the institutions taking care of their asylum processes (appendix B.3). Interviewees were asked what they see as the organizational culture or norms for handling Personal Identifiable Information (PII) and Demographically Identifiable Information (DII), this confirms the situation sketched above. More knowledge on data responsibility is starting to be actively integrated into their processes, yet is brought to a lower prioritization if other tasks are more demanding and is not the norm yet.

Ethical considerations concerning humanitarian information result in a contradiction. As absolute protection of people makes it impossible to collect data, while fully opening up data would endanger people [64]. So even if legal implications are lacking, a humanitarian organization should carefully balance what personal identifiable information to collect and use. A practical illustration of ethical considerations is informed consent. Beneficiaries should always be informed about what their PII is used for and agree on these uses. This sounds nice but practical constraints such as urgency, unknown procedures, low literacy and technological awareness and the remoteness of data collection often make this complex [64]. In the following paragraphs this is explained in more detail.

### 3.4.3. Level Two: The Rules of the Game

The rules of the game are formal rules and subject to change in tens of years These rules aim to get the institutional environment right. To retrieve understanding this part zooms in from international, to national to local level. According to the GSDRC international humanitarian assistance is subject to international law in various forms. First, there is international humanitarian law (IHL), which governs during armed conflict and constitutes of seven basic rules [87], that are based on the principles of humanity and impartiality. The IHL implies that the parties to a conflict shall have the legal obligation and primary responsibility to deliver humanitarian assistance to the citizens under their control [68]. However, IHL allows for humanitarian organizations to support and in occupied areas the occupants are obliged to cooperate with humanitarian organizations. The IHL states that the Red Cross or Red Crescent emblem shall be the respected sign of protection [87]. Second, there is international customary law, which consists of international human rights law (IHRL), international refugee law (IRL) and international criminal law (ICL). Together with IHL they form a comprehensive legal framework. IHRL is relevant in armed conflict and other disasters, it applies to states and provides protection and assistance to internally displaced persons (IDP). Through IHRL a citizen of a state can claim assistance from their authorities [68]. IRL also applies to states and operates at any given time, and aims to protect and assist refugees and IDPs. ICL enables private individuals to be held liable for attacking humanitarian organizations [68]. Lastly, there is International disaster response laws, rules and principles (IDRL). It complements IHL as it focuses mainly on areas where IHL is not applied. Compared to IHL, IDRL is relatively weak as it consists of many treaties, resolutions and guidelines. It is applied to states and non-states, aiming to establish a legal framework in an area where there is an undeveloped coordination mechanism [68].

These five forms of international law legitimize a humanitarian organization to start targeting and registration beneficiaries. However, in practice collaboration with national and local authorities is necessary and compliance with their national laws is mandatory. A distinction here is to be made between three types of organizations:

- International humanitarian organizations that have a local branch *with* a legal status in the country they operate in
- International humanitarian organizations that have a local branch *without* a legal status in the country they operate in
- National humanitarian organizations that have a legal status in the country they operate in

The distinction is necessary as some humanitarian organizations have to comply with laws of two national authorities as opposed to one. For example, a humanitarian organization with European Headquarters has to also comply with the art. 214 in the Treaty on the Functioning of the European Union (TFEU on humanitarian assistance, the EU consensus on Humanitarian Aid (2008/C 25/01) and the General Data Protection Regulation (GDPR)[13]. Similar regulations will apply for organizations with headquarters elsewhere. Especially the GDPR, with relation to targeting and registration is of importance as it requires explicit consent from every beneficiary that is registered. The GDPR is effect as of May 2018 and requires all organizations that recruit staff from within Europe, fundraise in Europe or are based in Europe to comply. As many organizations will have only one regime for security and privacy within an organization it is likely they will try to comply with the GDPR as it is the most stringent data protection regulation [142].


Figure 3.7: GDPR Citizen Rights from Espyder [57]

Further national regulations have to be taken into account as well. However, this regulation will not alter from the procedures that are undertaken in current practices as these are mostly administrative and financial requirements. The assumption made here is that if a system is compliant with GDPR and humanitarian organizations do not breach regulations at this moment during their operations, the system adheres to the formal regulations. This was also confirmed by Arjen Crince and an interviewee who preferred to stay anonymous (see appendix B). When asked what kind of national regulation was taken into account with respect to data protection, they stated that GDPR was more stringent than any of the national regulation they came or across.

Also noteworthy are the UN General Assembly resolutions. These are non-binding resolutions (they do not hold up in court) which are ratified by all of the 193 member states of the UN, but do carry political weight. The basis of international humanitarian coordination comes from resolution 46/182 in December 1991 and through transformation after 2005, evolved in the Cluster Approach (see figure 3.8). The Cluster Approach categorizes eight sectors and is a formal mechanism for coordination [36]. It is carried out on a national level, in a rather regulative manner, which according to Clarke and Campbell is not preferred as looser forms of cooperation are more effective in emergency situations [36]. Targeting and registration is not sector specific, but an activity that goes throughout sectors,

[13]Directive EU 2016/679

which makes cooperation for these activities difficult in the Cluster Approach. As an institutional form, the Cluster Approach governs emergency responses on paper, and sometimes in reality but it holds little power to actually enforce it workings in the affected area. This leads to increased collaboration but is still sub-optimal. Another interesting UN resolution is the acceptance of the UN Sustainable Development Goals, such as goal 1.1. "by 2030, eradicate extreme poverty for all people everywhere, measured as people living on less than $1.90 a day" and goal 16.9 "by 2030, provide legal identity for all, including birth registration" [50].

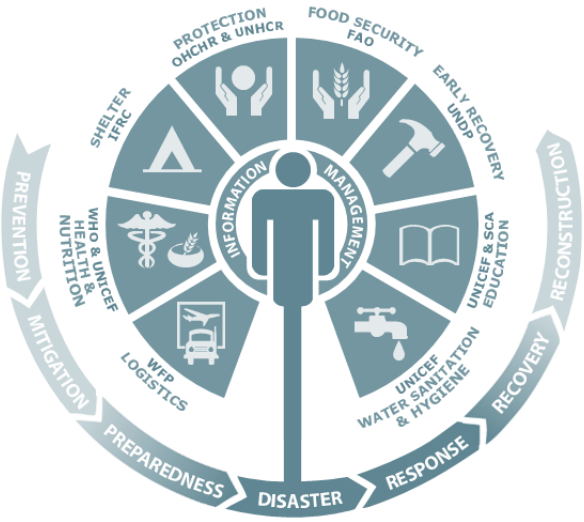



Figure 3.8: Cluster Approach from Humanitarian Response [83]

If service providers are used in the process of distributing cash or other services it could be that anti-money laundering/know-your-customer regulations would apply. Ajayi Ayobamidele, cash coordinator for UN OCHA Nigeria, states that some of the beneficiaries in a CTP he was working on, had to register at a mobile communications company to receive money (see appendix B.3). The mobile operator was operating under national laws for which know-your-customer regulation applied. Although humanitarian organizations do not prefer to share their data with service providers it sometimes is necessary for their activities.

### 3.4.4. Level Three: The Play of the Game

The play of the game is all about governance and getting governance structures right. These structures are subject to change in a matter of years. Humanitarian governance is deemed special because humanitarian organizations are often outside the sovereignty of a single state and is therefore governed by the humanitarian organizations themselves, which leaves room for politics and diverging interests [77]. This is why, the Cluster Approach as a rule seems fine but in practice is not prioritized, ignored or adapted to the needs of the organization [36]. So, where one would expect collaboration because of the humanitarian mission, in reality there is little cooperation and sometimes rivalry because organizations are competing for the same funding. As stated, the norm is to care for the most vulnerable but in respect to handling their data in practice there are several shortcomings according to Rebecca Visschedijk, Arjen Crince and Aneel Ahmed (appendix B). Which is why the ICRC and the Brussels Privacy Hub have recently launched a "Handbook on Data Protection in Humanitarian Action" and more awareness is being created throughout the sector. Targeting and registration involves PII and DII, thus a scrutinous policy on data protection should be embedded. However, targeting and registration takes place in chaotic and unstable environments, rendering it vulnerable for flaws and data-breaches. For example, the RedRose system used by multiple international humanitarian organizations for CTPs was recently breached by one of their competitors [39]. Humanitarian organizations are realizing they have to act and slowly data responsibility policies come into place [95]. Unfortunately, systems incorporating privacy-by-design are still rare. A well-known set of privacy protection principles is provided by Ann Cavoukian in "Privacy by Design- the 7 Foundational Principles" [34]:

1. Proactive not Reactive; Preventative not Remedial

2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy

These principles focus on the system and organization itself, but not on collaboration, interoperability and scalability. Standards partly fill in this gap and are part of the institutional environment if agreed upon by humanitarian actors. This requires extensive collaboration and tuning by humanitarian organizations. The governance needed for this is transnational which is burdensome since there are few formal rules that streamline collaboration, thus leaving room for improvement for the integration of standards into digital identity systems and ultimately decision making in humanitarian responses. This why next to privacy-by-design principles there are also humanitarian information management principles. There is some overlap between them, but the difference is that the former is designed from the perspective of the data subject while the latter is designed from the perspective of the system operator or the governance body. A set of them is described by UN OCHA and aim for interoperability, inclusivity and collaboration [115, p.2]:

- *Accessibility*; "Humanitarian information and data should be made accessible to all humanitarian actors by applying easy-to-use formats and by translating information into common or local languages when necessary. Information and data for humanitarian purposes should be made widely available through a variety of online and offline distribution channels including the media."
- *Inclusiveness*; "Information management and exchange should be based on a system of collaboration, partnership and sharing with a high degree of participation and ownership by multiple stakeholders, especially representatives of the affected population."
- *Interoperability*; "All sharable data and information should be made available in formats that can be easily retrieved, shared and used by humanitarian organizations."
- *Accountability*; "Users must be able to evaluate the reliability and credibility of data and information by knowing its source. Information providers should be responsible to their partners and stakeholders for the content they publish and disseminate."
- *Verifiability*; "Information should be accurate, consistent and based on sound methodologies, validated by external sources, and analyzed within the proper contextual framework."
- *Relevance*; "Information should be practical, flexible, responsive, and driven by operational needs in support of decision-making throughout all phases of a crisis."
- *Objectivity*; "Information managers should consult a variety of sources when collecting and analyzing information so as to provide varied and balanced perspectives for addressing problems and recommending solutions."
- *Humanity*; "Information should never be used to distort, to mislead or to cause harm to affected or at-risk populations and should respect the dignity of victims."
- *Timeliness*; "Humanitarian information should be collected, analyzed and disseminated efficiently, and must be kept current."
- *Sustainability*; "Humanitarian information and data should be preserved, catalogued and archived, so that it can be retrieved for future use, such as for preparedness, analysis, lessons learned and evaluation."

These principles represent a set of informal rules. Hence, they can be difficult to implement and it is likely that there is a difference between the theory and the practice. This was specifically revealed by the interviewees for CTPs, but in general for humanitarian information management [154] and becomes more understandable when realizing the dynamic, complex and chaotic environment humanitarian organizations often work in. For example, there are extensive rotations of humanitarian personnel, which forces a transfer of tasks every few weeks or months with people getting accustomed to new systems and local contexts leaving room for errors if the systems allow for this.

### 3.4.5. The Institutional Environment

To answer sub-question 1.2. "*In what institutional environment does targeting, identification and registration take place?*" a desk study and interviews were used. Information derived was put into the institutional framework of Williamson [160]. Targeting, identification and registration takes place in affected areas, which are often chaotic and unstable. There has not been a consensus on the most effective approach in emergency response over the last 100 years and even now debate still exists. The main norm is that humanitarian organizations help those in need to do good and do this with the humanitarian principles of humanity, neutrality, impartiality and operational independence in mind. Targeting, identification and registration is made possible under international humanitarian law in affected areas but has to comply with privacy regulation of which the most stringent is the GDPR. National and local regulation is often accounted for but not specifically integrated in the identity systems. GDPR and blockchain are difficult to match at the moment, since the right to be forgotten is a direct adversary of the almost immutable and transparent blockchain. So far no answers to resolve this has been found, for this reason the GDPR will not be further taken in to the system design and privacy-by-design will be assumed to cover other parts of the GDPR. Emergency response can be coordinated by the Cluster Approach, which is a form of transnational humanitarian governance. On paper this leads to enhanced collaboration and efficiency's, but in reality there is little cooperation, trust and more rivalry, leading to sub-optimal outcomes. Also, although data responsibility is more integrated in the humanitarian sector in the field it is sometimes impossible or ignored. Of the lists of principles described in this chapter, the humanitarian information management principles shall be used as a leading guide. These principles include the humanitarian principles and largely cover the privacy-by-design principles, plus they acknowledge the importance of collaboration within the sector. Although many principles exist there remains a stark difference between theory and field application. This research does not aim to cover this difference as no field research will be applied, however a final system should be thoroughly tested upon this issues.

In conclusion, the institutional environment has been analyzed using Williamson's Framework [160]. Norms, values, regulations and laws were analyzed. CTPs take place in the wider context of transnational humanitarian governance which suffers from collaborative issues. UN OCHA has set up the **humanitarian information management principles** to increase collaboration in information systems and together with **privacy-by-design principles** shall be further used in this research.

## 3.5. Stakeholder Analysis

According to de Bruijn and Herder [43] the perspective of stakeholders in socio-technical systems should be put alongside the physical-technical perspective of the system, in order to draw the strengths of both perspectives. In a socio-technical system, stakeholders will show strategic behavior and have diverging interests, which can frustrate a rational and phased decision-making process [43]. Churchman [35] defines problems in these environments as "wicked", for which there is no ready-made solution and requirements are still unknown. de Bruijn et al. [44] therefore advocate that solving these problems requires a process approach, where decision-making is the result of interaction as opposed to a project approach where decision-making is the result of planning [44, p.15-17]. For clarification, this research shall not propose a full process design for the implementation of this system. Yet, while developing a design, it is important to understand that the design could be altered later on by the implementation process as stakeholders might change their interests. In order to determine whose interests should be taken into the design requirements a stakeholder analysis is conducted, which aims to answer sub-question 1.3.: *Which important stakeholders are involved in targeting, identification and registration?*. This question is answered by looking at various ecosystems, which can be defined as a "a system of people, practices, values and technologies in a particular local environment" [110, p.49]. The ecosys-

tem perspective is often used in data dense, socio-technical contexts as it describes interrelationships between stakeholders, the data, institutions and hardware [71, 73].

### 3.5.1. Three Ecosystems: Humanitarian, Digital Identity and Blockchain

There are three types of ecosystems to be looked at. First there is a *humanitarian ecosystem* which describes the environment and stakeholders in an emergency response. Second, the *digital identity ecosystem* which describes the environment and in combination with the identity life cycle (see 3.3), it describes the environment and potential roles in digital identity systems. Third, is the *blockchain ecosystem*, which describes together with the layered blockchain overview in figure 3.5 the blockchain environment and potential roles.

Betts and Bloom [25] describe a general humanitarian ecosystem, which we adapted to the perspective of CTPs in figure 3.9. This figure is adapted to the specifics of targeting, identification and registration as opposed to the general humanitarian ecosystem. This ecosystem provides the stakeholders and roles in a humanitarian context and shows different action arena's such as the international, the national and the affected arena. The roles these organizations for CTP have can vary and may not be limited to one specific role. The middle of this figure is reserved for the beneficiaries or people affected, as not everyone will become a beneficiary of a CTP. They are surrounded by national/local humanitarian organizations, local authorities, community representatives, merchants and service providers. These actors all interact within the area that has been impacted. At a national scale, national authorities and military forces play a role. At the international scale the international authorities, international humanitarian organizations, donors and private organizations enact their parts.

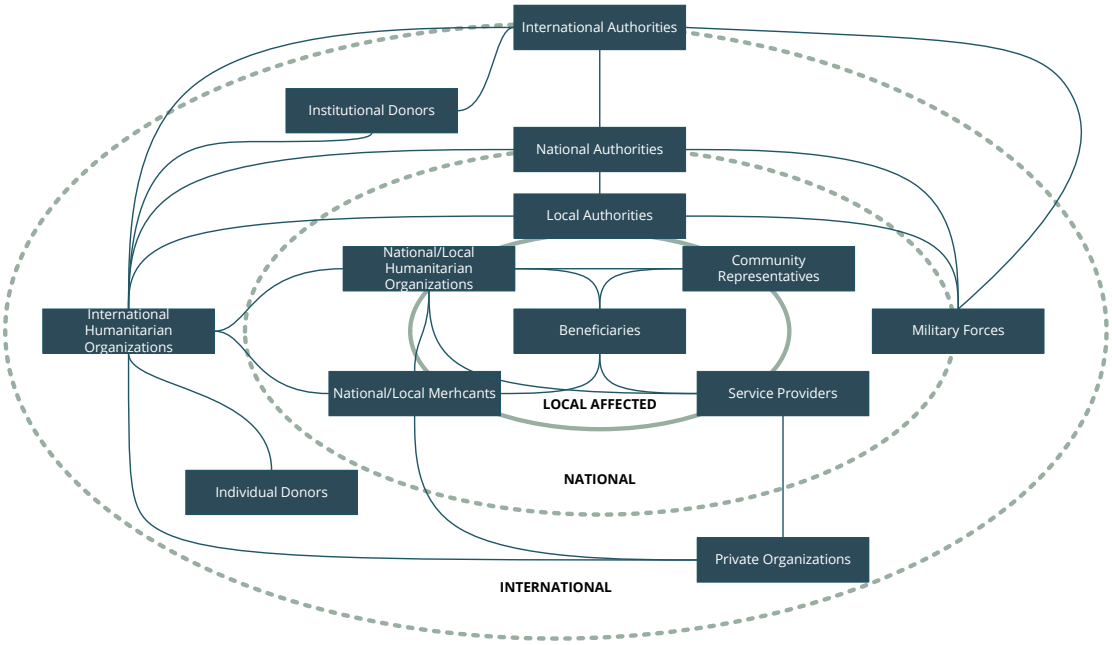



Figure 3.9: Stakeholders in the Humanitarian Ecosystem adapted from Betts and Bloom [25]

Besides the humanitarian ecosystem there is the digital identity ecosystem as shown in figure 3.10. It shows an individual ID technology, or a functional purpose for a digital identity system. This system is part of a wider identity system that has an social, political and economic context. Outside that, it has to interact with other ID systems and has relationships with it. From this figure it is derived that an issued digital identity from a CTP program does not stand on its own as it has to be embedded in social, political and economic contexts and ultimately also with other digital identity systems within the local, national or international environment. This ecosystem can be combined with the identity life-cycle )figure 3.3) and provides five roles that stakeholders could take up: end-users, identity providers, attribute providers, authentication providers and service providers. It is important to realize that an identity system is not a standalone concept, especially with the idea of self-sovereign identities that should not only be used for a functional purpose of CTPs but should also have foundational qualities

and have a wide-spread use.

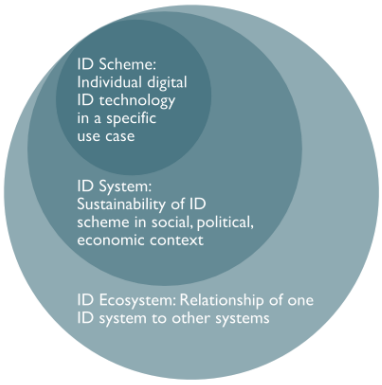



Figure 3.10: Digital Identity Ecoystem from USAID [152]

The last ecosystem is that of blockchain as presented in figure 3.11, where operators and users are shown. Not depicted but part of the ecosystem, are stakeholders that deliver the software such as infrastructure providers, who are responsible for developing the blockchain and the network, and application developers who build the applications that run on top of the blockchain [81]. There are network operators that could operate an instance of the blockchain and application operators that run applications on the blockchain. Users can either be network participants, entities or individuals that run a node or application users, that use the blockchain interface [81]. These roles should also be taken up by the stakeholders. This ecosystem is of importance because it depicts not only what should be institutionally arranged but also what technical roles have to be fulfilled.

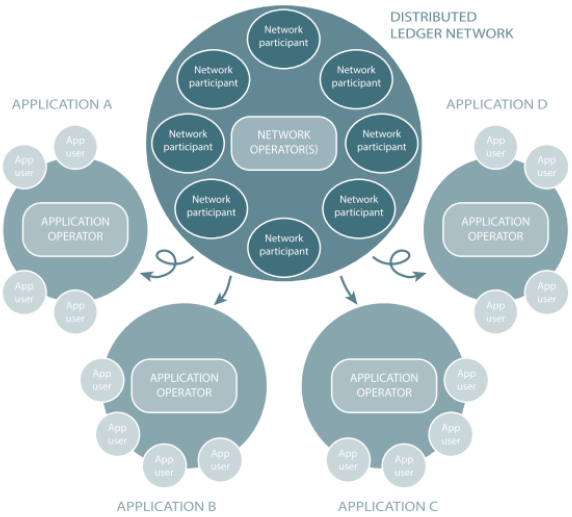



Figure 3.11: Blockchain Ecosystem from Hileman and Rauchs [81]

In the following paragraphs the stakeholders and their potential roles will be examined. A full overview of all stakeholders is presented in appendix C. Roles are indicated per ecosystem. CTP and digital identity roles are assigned based on the literature review, desk study and interviews. The blockchain roles are assigned based only on desk research. Based on these roles it should become clear why certain stakeholders perform critical roles, thus taking their requirements as a start for further design. Doing this for three ecosystems not only shows the stakeholder complexity, but also enhances understanding for future research if a process design has to be developed.

### 3.5.2. National Stakeholders

In the affected area there is turmoil and disruption of local systems for regulation, markets and welfare. National and local authorities often fall short of providing the necessary aid themselves, which allows for the creation of a humanitarian system. This system can consist of sectors or clusters, and can have different information flows. The humanitarian system consists of national/local humanitarian organizations, national and local authorities, UN cluster organizations (if used), military forces, service providers, merchants, community representatives and beneficiaries. This exact composition differs per context.

#### Beneficiaries or People Affected

Beneficiaries or People Affected are the ultimate victims of the disasters, their interest is to survive and they will receive the cash based assistance. It are these people the other stakeholders should listen to, as to find out what assistance is needed and what types of registration and targeting will work best in the local context. Their perception of targeting and registration is important for the humanitarian sector, hence feedback from beneficiaries is vital.
*CTP Roles:* Needs Assessment, Recipients, Feedback
*Digital Identity Roles:* End-users
*Blockchain Roles:* Application Users

#### National and local humanitarian organizations

National and local humanitarian organizations are National Red Cross Societies, Local NGO's and national branches of international organizations. They usually view targeting, identification and registration as essential tools for the efficient and just distribution of cash based assistance in order to prevent and alleviate more human suffering [82]. Their key interests are in local coordination, disaster response and disaster preparedness. They have limited legal power, but their informal power can be significant if national/local authorities are incapable of assisting their citizens themselves.
*CTP Roles:* Coordinator, Designer, Focal Point, Needs Assessment, Market Assessment, Operational, Monitoring
*Digital Identity Roles:* Identity providers, Attribute providers, Authentication providers and Service providers
*Blockchain Roles:* Network operators, Application operators, Network Participants, Application Users

#### National and local authorities

National and local authorities are likely to have the same view on targeting and registration as humanitarian organizations. They aim to provide welfare to their people but are sometimes helpless themselves. Authorities can be opposed to registration of their citizens, in this case it becomes difficult for humanitarian organizations to proceed with their activities as authorities hold significant formal power by making laws and enforcing regulations. In a regular situation authorities try to assist in targeting and registration, and might want to access these records. Besides the judicial roles, authorities might have their own (digital) identity systems which are in the digital ID ecosystem.
*CTP Roles:* Law maker, Coordinator, Operational, Market Assessment, Potential Opponent, Monitoring
*Digital Identity Roles:* Identity providers, Attribute providers, Authentication providers and Service providers
*Blockchain Roles:* Application developers, Network operators, Application operators, Network Participants, Application Users

#### Cluster Approach

The ICRC, UNHCR, WFP, UNDP and OCHA can be part of the cluster approach. This method was set up by the humanitarian sector to initiate a coordinated nation-wide response. It is not always used, so different entities can also be present in the affected area without a cluster approach. Each organization has a specific task which is coordinated by OCHA who puts forward an Emergency Relief Coordinator (ERC). UNHCR is responsible for camp coordination and management, WFP is responsible for food security and logistics, UNDP is made responsible for early recovery and the ICRC is made responsible for shelter [82]. Each entity has a different mission, but it is assumed that all of them share a vision for targeting and registration as being essential towards preventing and alleviating human suffering. Formally, the UN Cluster approach holds no power, it is issued by UN resolution but is not held up

in court. An exception is the ICRC, which is appointed by international humanitarian law, thus holds some formal power [87].
*CTP Roles:* Coordinator, Designer, Focal Point, Operational, Needs Assessment, Market Assessment, Complementary Programs, Monitoring
*Digital Identity Roles:* Identity providers, Attribute providers, Authentication providers and Service providers
*Blockchain Roles:* Protocol development, Network Development, Application developers, Network operators, Application operators, Network Participants, Application Users

#### Military forces
Military forces may be present in the affected area, in case of an armed conflict they have a different role (they might be one of the fighting parties) than in a natural disaster. In general they should be peacekeepers and assist with security measures. By law, they have a monopoly on violence but in regular situations only when an authority requires them to carry it out. If military parties are part of the conflict, they might oppose targeting and registration of all or certain groups of people.
*CTP Roles:* Security in disbursement, Potential Opponent
*Digital Identity Roles:* none
*Blockchain Roles:* none

#### Merchants and other Service Providers
Merchants and other service providers (e.g. remittance companies, suppliers of biometric scanners, banks) have an important part in the CTP, but not necessarily with registration and targeting. It is likely they see targeting and registration as essential tools, because it provides demand for their services, as their interest is to make a profit (or at least break-even). They can supply local knowledge which can be used for enhanced operationalization of the targeting and registration process. Service providers can be selected by humanitarian organizations by putting out a tender and drawing up contracts, in order to ensure trust and capability. These organizations hold very little formal power and limited informal power.
*CTP Roles:* Needs Assessment, Market Assessment, Collaborate in Disbursement, Operational
*Digital Identity Roles:* Authentication providers and Service providers
*Blockchain Roles:* Application developers, Application operators, Application users

#### Community Representatives
Community representatives are necessary for a community supported approach of targeting and registration. As already discussed in the literature review section but also supported by Angelika Kessler (Food and Economic Security Advisor for the Netherlands Red Cross), who states that sensitizing the community on inclusion criteria and other expectations is a very important building block in CTP execution [141]. Community representatives transform local knowledge into community support, as they are interested in the welfare of their people. Their informal power is significant if there has not been any cash based assistance before, as one of their roles is to assist in setting inclusion criteria.
*CTP Roles:* Designer, Needs assessment, Operational
*Digital Identity Roles:* Attribute providers
*Blockchain Roles:* Application users

### 3.5.3. International Stakeholders
Outside of the affected area there is an international environment with certain humanitarian standards, humanitarian governance and international humanitarian law. Within this environment there are different stakeholders, and depending on the context the configuration alters.

#### International Humanitarian Organizations
Often these organizations have national or local branches but a headquarters outside of the affected area. These organizations can be faith based such as Christian Aid or Islamic Relief, intergovernmental or other organizations. They coordinate between their organizations and their external environment, they might focus on research, funding and human capacity in the affected area. They share the vision of their local branches but also have international interests. They might set organization-wide standards and practices. They are limited by the national law of their place of registration, but have significant

informal power.
*CTP Roles:* Coordinators, Designers, Operational
*Digital Identity Roles:* Identity providers, Service providers
*Blockchain Roles:* Protocol development, Network development, Application development, Network participants, Consortia initiative, Research, Funding

### International authorities

International humanitarian organizations can collaborate with international authorities for support, funding and other shared interests. These authorities have their own strategic interests which they aim to pursue. They have some formal power by international law, but this is bounded by their international relations with the affected country. Informal, they have significant power through the UN and other aggregate bodies, but also by the amount of funding they provide. Besides these activities there are also international authorities that uphold regulations and assist in auditing digital identity systems with the aim to ensure that digital identity providers follow the correct legal standards and nest practices [144].
*CTP Roles:* Coordinators, Designers, Funding
*Digital Identity Roles:* none
*Blockchain Roles:* Network participants, Funding

### Development Partners

There are also development partners such as the Cash Learning Project (CalP), HPN, Overseas Development Institute (ODI) and the World Bank. These organizations do research on the effects, disadvantages and opportunities of CTPs, but also provide limited funds and sometimes initiate other programs. Through their activities they exert some informal power, but generally it is limited. They also, in collaboration with for example the IOM, UN OCHA and UNHCR provide technical assistance for the development of digital identity systems in certain countries [144]. Help can be given by strengthening a country's existing identity system or as a component of a CTP or other program which requires identification [144]. Digital ID development partners can be found in organizations assuring digital identity standards such as the OECD, the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU), but also private organizations like the Open ID Foundation, Open Identity Exchange and The Internet Society [134]. Blockchain development partners could be categorized per layer. Protocol support could be sought for at Hyperledger, Corda or Multichain for example, while network support and application development can be found all over the place [81].
*CTP Roles:* Funding, Research
*Digital Identity Roles:* Auditing, Consultancy, Research
*Blockchain Roles:* Protocol development, Network development, Application development, Network participants, Auditing, Consultancy, Research

### Institutional and individual donors

Stakeholders making CTPs possible are institutional and individual donors. Institutional donors such as UKAID, USAID, ECHO and other ministries, provide high value (multi-annual) funds. Institutional donors fund projects to realize their strategic ideas and have significant informal power. They might express requirements for how their money is spend and who should receive it. Individual donors provide low-value funds, but in aggregate they can add up. They have very limited formal and informal power. Both types of donors are likely to view targeting and registration as essential tools for the distribution of their funding and like to receive feedback on how their money is spent.
*CTP Roles:* Funding, Research
*Digital Identity Roles:* Funding
*Blockchain Roles:* Funding, Network participants, Volunteer coders

### Private organizations

Lastly, there are private organizations such as social enterprises and corporates. These organizations have social responsibility programs, by which they assists the humanitarian system with goods and/or services. For targeting and registration it means either they see it as essential so their support is distributed correctly, or they can assist in this by for example providing tablets for in-field registration. Another example is that of telecommunications companies releasing anonymized data on the behavior

and potential whereabouts of beneficiaries, to assist and plan humanitarian operations [150].
*CTP Roles:* Funding
*Digital Identity Roles:* Auditing, Consultancy, Research
*Blockchain Roles:* Protocol development, Network development, Application development, Network participants, Auditing, Consortia initiative, Consultancy, Research, Volunteer coders

### 3.5.4. Powers and Interests of Stakeholders

From the previous paragraphs it can be seen that there is an extensive set of stakeholders with diverging interests. Even within groups of actors such as international humanitarian organizations diverging interests exist [77]. Hence, it would be useful to distinguish between stakeholders whose interests should be translated into the design and those whose are not. Bovaird describes that a power-interest grid is a tool which can assist in distinguishing these categories [28]. This matrix has the CTP interest of a stakeholder on one axis and the power of a stakeholder on the other creating four quadrants. The figure could have a different configuration if it is analyzed for the interest into digital identity systems or blockchain infrastructures, yet the system of interest is that of CTP.

Mapping the stakeholders in these quadrants results in the overview presented in figure 3.12. It implies that requirements from the national and local authorities, national and local humanitarian organizations, international humanitarian organizations and institutional donors should be managed closely as they are seen to be key players in the system. Beneficiaries and community representatives are also key players, but in comparison with the other stakeholders they lack power. However, their requirements should also be taken very seriously. They have limited means of vocalizing their needs, so they need to be actively solicited. National and local merchants should be informed, as with individual donors. International authorities and other international humanitarian entities should be met in their needs, as they have significant power but are less interested. They should be kept satisfied as to let sleeping dogs lie. The development partners, private organizations and service providers are generally exchangeable and thus have less power. They might have some interest, especially if they are active in the affected area. These stakeholders have a low priority, but should be monitored.

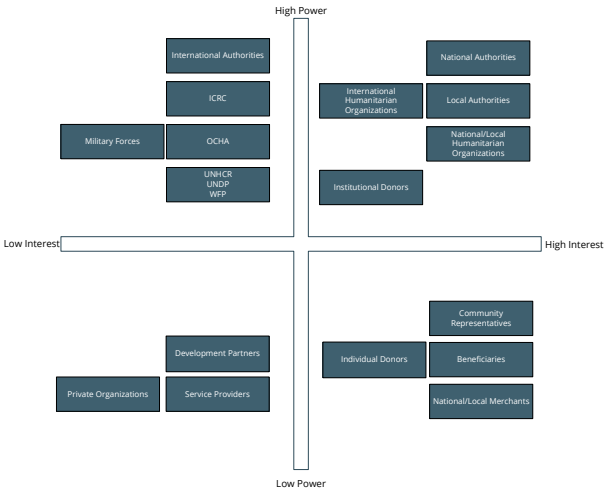



Figure 3.12: Power-Interest Grid

### 3.5.5. The Important Stakeholders

To answer sub-question 1.3.:*Which important stakeholders are involved in targeting, identification and registration?* a desk study, semi-structured interviews, an ecosystem approach and a power-interest grid was used. For simplification, it is assumed that roles that are assigned in this research are carried out accordingly. Based on the power-interest grid the most important stakeholders for targeting, identification and registration CTPs are **national/local authorities, international/national/local humanitarian organizations, donors** and the (affected) community such as **beneficiaries, representatives** and **merchants**.

## 3.6. Sub-conclusion System Analysis

In each paragraph a small sub-conclusion has already been provided that together answers the sub-question *1. What is the current socio-technical system of targeting, identification and registration in Cash Transfer Projects in a humanitarian context?*.

According to literature the procedure of targeting and registration starts with a geographical selection, followed by an eligibility check based on inclusion criteria. Individuals are targeted and registered, sometimes as being the representative of a household. Targeting the most vulnerable in emergency responses is time-intensive, dependent on access, available data and dependent on other aspects of a CTP. It is a highly complex process due to coordination, complementary programs and the worsening effects of targeting errors. Also, it influences the possibilities for monitoring & evaluation and thus for the overall process of taking responsibility by a humanitarian organization. According to the technical, institutional and stakeholder aspects of this system analysis the system described in literature might change by the inclusion of the digital identity life-cycle, self-sovereign identity principles, a layered blockchain architecture, privacy-by-design principles and humanitarian information management principles. Utilizing these characteristics to tackle the difficulties in collaborating and scaling of targeting, identification and registration makes it a unique contribution.

# 4

# Requirements Engineering

*"Football boots are very technical and have lots of specific requirements"*
- Zinedine Zidane

This chapter answers the second sub-question of this research: *Which design decisions have to be made?*. Although this thesis focuses on the use of blockchain, the program of requirements should be ambiguous to this technology. By doing so, it creates the future opportunity to compare centralized or other distributed systems developed on the same program of requirements. To answer this sub-question a desk study, semi-structured interviews and participatory research are used. Requirements engineering is a key step in the development of a system design.

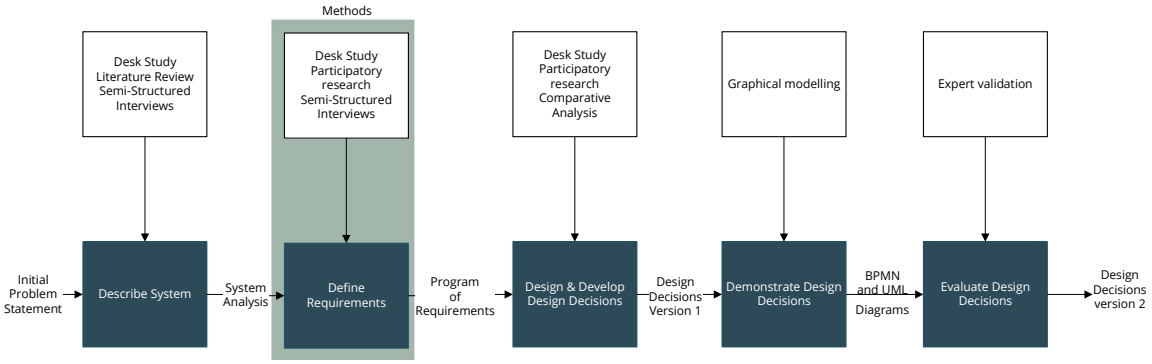



Figure 4.1: Methods for Requirements Engineering

In the first paragraph the form of the artifacts that have been introduced in chapter 2, paragraph 2.4, will be further explicated so that before requirements are elicited it is known in what type of artifacts they are integrated. In paragraph 4.2 the workings of requirements engineering are explained as well as the steps that have to be taken, which form the build-up of this chapter. In paragraph 4.4 the analysis, classification and prioritization of requirements is done. This chapter is concluded in paragraph 4.5 where sub-question 2 is answered.

## 4.1. Artifacts

The form of the artifacts is shortly addressed in chapter 2 (see paragraph 2.4) and is explained in more detail in the following paragraphs. As expressed the artifacts are models, which represent the final solution and should be used to support the construction of an instantiation of the system [93]. For this research the main artifact is the set of design decisions, which is supported by three other artifacts: a program of requirements, a BPMN diagram and UML Class diagram.

### 4.1.1. Program of Requirements

Requirements engineering is about documenting and guiding the development of requirements in order to provide traceability and only include the correct requirements, thus excluding unnecessary requirements [59, p.23]. A *requirement* is a formal structured statement which suffices a need and can be something a system must do, must possess or a constraint under which it must operate. It is about the what, not about the how. Since the to be designed system is complex, requirements should be unambiguous, correct, feasible, justifiable, verifiable, singular and necessary [59, p.48]. Furthermore, a program of requirements is a living document meaning requirements can change and should be managed throughout the design process. Besides a direct value to the designer, a set of requirements also holds value as a communicative tool for the buy-in of other organizations. There are different ways to retrieve requirements. The Program of Requirements is an overview of all the requirements gathered from diverse sources. They often show a specific identifier for traceability, a source, a rationale statement, the type of requirement and a priority.

### 4.1.2. BPMN diagram

Business Process modelling Notation is a standardized modelling language maintained by OMG, which has the purpose of providing a visualization that is readily understandable by all stakeholders, from technical developers to end-users to business analysts [118]. BPMN is a flowchart technique, thus has a dynamic quality and it links up with the underlying constructs of execution languages.

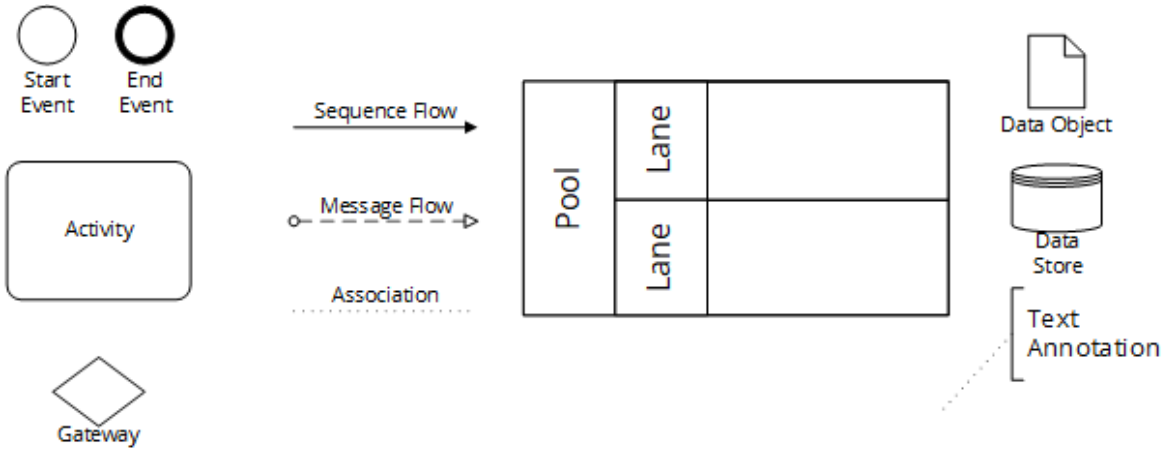



Figure 4.2: Basic BPMN elements

There are five general elements (see figure 4.2) in each BPMN [118]. First there are *flow objects* which are the main elements for defining behavior in the process and are either events, activities or gateways. Second, there is *data* which can be either a data object, data input/output or data store. These provide information on what an activity needs to be performed or to what they produce. Third, *connecting objects* which connect flow objects with each other or other information. There are sequence flows, message flows, associations and data associations. Fourth, *swimlanes* can represent participants in a process and can be joined in pools to denote an overarching relationship. A lane is a subdivision in a pool and organizes activities. Last, *artifacts* are used to provide extra information on the process similar to a post-it on a document.

### 4.1.3. UML class diagrams

UML has become the norm as a modelling language for software-intensive systems. UML is standardized language and maintained by the Object Management Group (OMG). The language is software focused, thus lacking the ability to integrate non-software components. This is why the diagram is supported by a BPMN visualization in this research. Another option is to use SysML[1] (also maintained by OMG) which is based on UML but has more systems engineering specific possibilities. SysML is an extension on UML in general, not only on class diagrams, for this research only the view of classes is sufficient.

[1]http://www.omgsysml.org/what-is-sysml.htm

UML is object-oriented meaning that each software object has a state and behavior. The state of a software object is stored in its fields and the behavior expressed through functions or methods. Using objects offers modularity, code re-use, information hiding, and pluggability and debugging ease [119].

A UML diagram can be used for analysis and for design, for which slightly different notations are used. For clarification, in this research UML will be used for design purposes. In UML a class is "the blueprint from which individual objects are created"[2], for example in the real world there are many bicycles made from the same blueprint and as such they have the same components. In this example bicycles are a class and a bicycle is an instance of this class. UML class diagrams are part of the UML structure diagrams as opposed to behavior diagrams. Their purpose is to demonstrate the static structure of the system by depicting the objects that are associated with the processes that need to be executed [22].

The representation of a class is a rectangle consisting of three smaller rectangles stacked on top of each other. The top shows the name of the class written as a singular noun, sometimes as an adjective and starts with a capital. The middle is used for attributes written as a noun and occasionally accompanied by an adjective, all in lowercase. The latter two are optional, depending on the level of detail. These classes can have different relations. The first *inheritance* or generalization, which is the ability of child-class to inherit the identical functionality of a parent-class, and add a functionality itself [22]. Inheritance is denoted by an open arrow from the child-class to the parent-class [147]. The second relation is that of *association* which demonstrates that an instance of a class is related to the instance of another class and is depicted by a line between the classes, which can be complemented with textual information. Lastly there are the relations of *aggregation and composition*. Aggregation shows that a class consists out of another class, for example the class house consists of a class door, class window and class chimney. Composition is a strong version of aggregation, in which the parts of which the whole exist only remain if the whole remains. These elements are visualized in figure 4.3, if other elements of UML will be used throughout this research, they shall be explained at that moment.

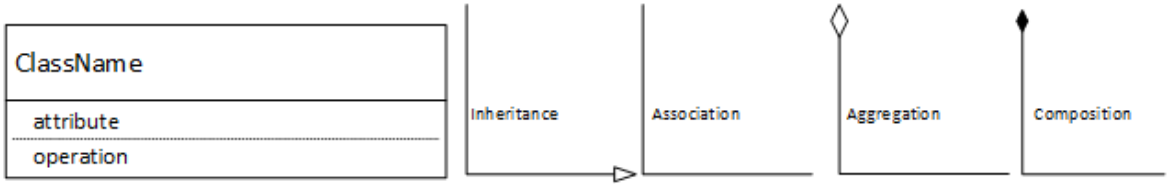



Figure 4.3: Basic UML elements

### 4.1.4. Design Decisions

Design decisions can also be described as a model artifact in the terms of Johannesson and Perjons [93] as models are "representations of possible solutions to practical problems, so a model can be used for supporting the construction of other artifacts" [93, p.30]. In a literature review on artifact types conducted by Offerman et al. [116] one could also classify design decisions as being a guideline that provides suggestions on system development. They have the form of "in situation X one could/should do Y" [116, p.84], in other words: if you want to design a digital identity system to scale up CTPs you should use or do this. This is the format that is used for the design decisions in this research. Hence, design decisions are prescriptive and in this research chaperoned by specific implications and limitations.

## 4.2. Introduction to Requirements Engineering

This step synthesizes stakeholder, technical and institutional requirements. In systems engineering the process of eliciting requirements thrives by complete and accurate definitions of the requirements that need to be included in the design.

Sommerville [135] describes a set of four activities in setting up a program of requirements which will be followed:

1. *Eliciting requirements*, collecting requirements from all sources

[2]https://docs.oracle.com/javase/tutorial/java/concepts/class.html

2. *Classifying requirements*, denote a type per requirement
3. *Analyzing requirements*, reorganizing requirements into a logical set
4. *Prioritizing requirements*, to establish the importance of requirements

The scope for requirements engineering stems from the sub-conclusion of chapter three and comes down to including the following needs:

- *Stakeholder needs*; national and local authorities, humanitarian organizations, institutional and individual donors and people within the affected area will be taken into account (named Person Affected)
- *Technical Needs*; involve the digital identity life-cycle and self-sovereign identity principles
- *Institutional Needs*; humanitarian information management principles and privacy-by-design principles

As stated, a blockchain specific focus is left out in this chapter to ensure that the final outcome of this program of requirements is useful to design a centralized or other distributed system with.

## 4.3. Elicitation of Requirements

Different methods were used for the collection of requirements such as a desk study, interviews and participatory research. Within requirements engineering it is practice to explicitly state how requirements have been elicited. There are two clear sources from which these requirements come: the system analysis and participatory research.

### Chapter: System Analysis

From the system analysis various stakeholder, technical and institutional requirements are derived. To be explicit, these requirements stem from a desk-study and semi-structured interviews:

**Desk Study** In the previous chapters a desk study was performed to provide a descriptive analysis, this information is used to further gather requirements. Based on the IDEF0 models and literature review, the CTP system is broken down into parts and analyzed to retrieve requirements. The technical analysis and privacy-by-design principles described by UN OCHA were used to gather requirements, as were the humanitarian information management principles and institutional analysis. The stakeholder analysis and their potential roles were also used to gather requirements.

**Semi-structured Interviews** A selection of humanitarian aid workers was interviewed to validate the desk study. There is no valid representation of all stakeholders so their needs are not directly translated into requirements, but indirectly if they were in line with or expanded upon the results found in the desk study. In other words, the interviews do not represent the stakeholders needs since the humanitarian eco-system is too diverse and due to time-constraints it would not be feasible to interview each stakeholder.

### Chapter: Requirements Engineering

**Participatory Research** From the participatory research at the NLRC and its development partners, process requirements are drawn. The NLRC and its collaborating developers are building an instance of the system. Their aim is to have a small scale pilot (late 2018) on the island of St. Marten which was hit by hurricane Irma in September of 2017. These experiences must be critically assessed as they represent the development of a similar design but from a very practical point-of-view as code is written and already working components from the outset for future development. However, this research does provide insights into potential directions and possibilities, as it eliminates some of the alternatives that might have been chosen. More requirements could have been drawn from this research but many are already put forward by the stakeholder, technical and institutional analysis.

Based on the needs presented in figure 4.4 there are three sets of principles that have to be included. These sets of principles have some overlap so they are merged into one set as presented in table 4.1.

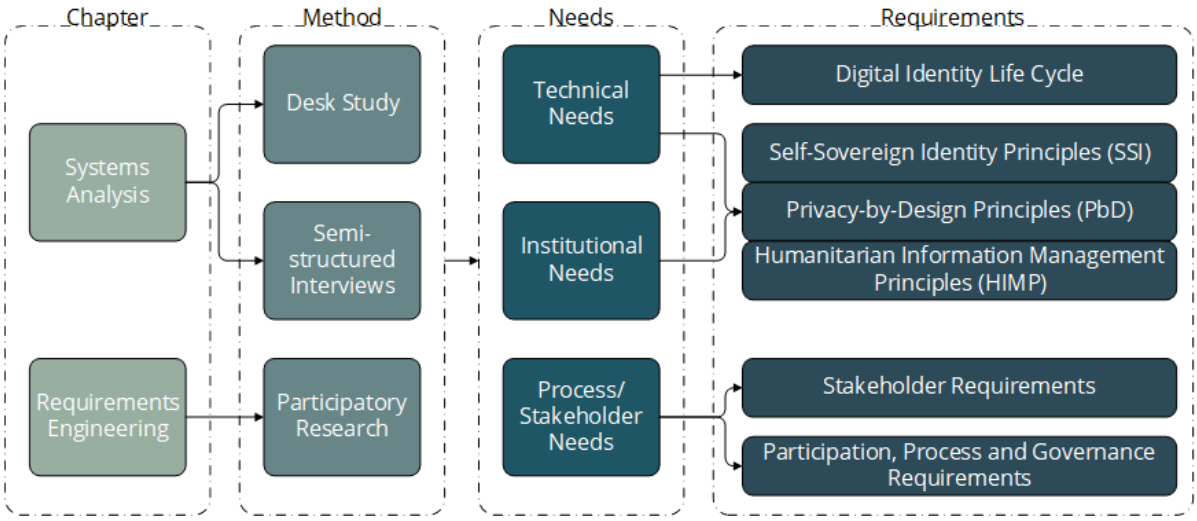



Figure 4.4: Overview of sources for requirements engineering

## 4.4. Analysis, Classification and Prioritization of Requirements

Analysis of the requirements starts with merging the three sets of principles: Privacy-by-Design (PbD), Self-Sovereign Identity and Humanitarian Information Management Principles (HIMP). In the first column of table 4.1 the final set of principles can be seen, in the second column the source is visible and in then the rationale. In the last column it can be seen where each principle is integrated in the program of requirements in table 4.2.

Table 4.1: Overview of Principles based on Allen [9], Cavoukian [34] and OCHA [115]

| Principles | Source | Rationale | Satisfied by Requirement |
|---|---|---|---|
| Existence | SSI | Users must have an independent existence | R.1 |
| Control | SSI, PbD | Users must control their identities | R.2, U.3, U.4 |
| Access | SSI | Users must have access to their own data | U.1, U.3, U.4 |
| Transparency | SSI, PbD | Systems and algorithms must be transparent | C.3, C.13, C.15 |
| Persistence | SSI, HIMP | Identities must be long-lived | U.3, U.4 |
| Portability | SSI | Information and services about identity must be transportable | I.5 |
| Interoperability | SSI, HIMP | Identities should be as widely usable as possible | C.14, R.10 |
| Consent | SSI | Users must agree to the use of their identity | R.6, U.4 |
| Minimalization | SSI, HIMP | Disclosure of claims must be minimized | U.4 |
| Minimization | SSI, HIMP | Only relevant data is collected | R.4 |
| Protection | SSI, PbD | The rights of users must be protected | C5, C.6, C.7 |
| Proactive; Preventative | PbD | Design for it in advance, prevent incidents from happening | Integral to design |
| Privacy by Default | PbD | Privacy must be embedded in the design as the default | C.7 |
| Humanity | HIMP, PbD | System must do no harm | C.5 |
| Accessibility | HIMP | Each humanitarian actor must have access | C.10, C.11 |
| Inclusiveness | HIMP | System must stimulate collaboration and partnership | C.11, C.14 |
| Accountability | HIMP | System must evaluate the reliability and credibility of the data | T.3 |
| Objectivity | HIMP | A variety of data sources must be used | R.7, R.8 |
| Timeliness | HIMP | Data must be collected, analyzed and disseminated efficiently | T.7 |

In table 4.2 an overview of all requirements is given. These requirements have been validated by an expert in systems design. In the first column an ID is visible which enables easier traceability throughout the rest of this research. The ID relates to the part in the digital identity life-cycle the requirement is related to. So R is for Registration, I is for Identification, U is for use, T is for targeting and C stands for requirements that are concern the cycle. In this categorization, targeting of Person Affected (beneficiaries and non-beneficiaries) is part of the use of the system. It can be seen as a service that is delivered. Since this program follows SSI principles, it is user-centred, which means that it is the Person Affected who requests the service and not the humanitarian organization that can initiate

the service. Furthermore, each requirement is followed by a rationale explaining why the requirement is taken in. Requirements have the following syntax: shall is binding, should and may are non-binding and must denotes a constraint. Each requirement is typified as functional or non-functional. Functional requirements state functions of a system, which can be described as input, behavior and output, they describe what the system has to do. Non-functional requirements define the qualities or properties the system must have, examples are security, privacy, interoperability and scalability.

The following paragraphs discuss the content of table 4.2.

### 4.4.1. Registration

These requirements all have to do with the registration of affected people and of attribute providers, identity providers and service providers, as they also need to be registered in the system. The requirements speak for themselves but some important mentions have to be made. First, there is no current evidence found that people affected perceive the need for a sustainable digital identification, it is the humanitarian sector that needs affected people to have one at this moment for the purpose of correctly targeting CTP beneficiaries. Second, a person should only be able to create one digital identity account, but might have different identities for different service providers in the sense that each of them sees a different set of identity attributes. Third, currently CTPs are based on a multitude of different inclusion criteria. In this system there must be a standard set of criteria to begin with, this might change later but at the beginning it increases interoperability of inclusion criteria, data quality at registration can be checked and double identities can be easier noticed. Which identity attributes should be incorporated into this standard set is not the scope of this research and should be established within the humanitarian sector. Fourth, consent here is given when starting the registration process. However, consent is given each time since an identity owner is in control of which attribute is visible to which participants of the network. Fifth, for now only humanitarian organizations can act as identity provider and service provider. Other organizations can be attribute providers. This is due to *C.16* that mentions the system should first have functional purpose and later be able to change to a foundational purpose, only then multiple service providers and identity providers can enter the system.

### 4.4.2. Identification

This entails all the requirements that have to deal with validation of registered identity attributes. Identity attributes can be validated by multiple organizations, giving the chance for objectivity. Also here, it is the identity owner that initiates the request for validation. After validation, an attribute provider creates verified credentials which can be stored by the identity owner. This way, if the attribute provider somehow seizes to exist the identity owner still holds access to the credential. Lastly, the attribute provider must also verify the geographic location of the person affected. In some cases this will proof to be difficult, since people might have seasonal work and seasonal living arrangements. Hence, the geographic location must be updated regularly.

### 4.4.3. Use

To comply with the SSI principles, the owner of a digital identity must be in full control. This implies updating and using it, but also revoking disclosure and having safe access to the digital identity. In many areas people affected will not own smart-phones, computers or tablets, so portability of the identity is important here as they must sign in to several registration terminals provided by humanitarian organizations or authorities. Digital identities are accessed using some form of authentication, depending on the form this can be lost in daily life but especially in chaotic disaster environments. Since the digital identity must be long-lived, a digital identity owner should be able to recover access in multiple ways.

### 4.4.4. Targeting

In regular CTPs it are humanitarian organizations who initiate the process of registration but for CTPs running on this new system, it should come from the person affected themselves. Via various channels they can be notified about the upcoming program upon which they can connect with the humanitarian organizations, who can then request certain identity attributes and match these with their inclusion criteria. Targeting results in either a yes or a no, but could also result in a score. For example, when it is uncertain how much funding is available people with a certain match on specific criteria are first included and other potentially later. The service providers themselves do not need to store

Table 4.2: Analysis of Requirements

| ID | Source | Lifecycle | Requirement | Rationale | Type | Priority |
|---|---|---|---|---|---|---|
| R.1 | Person Affected | Registration | Each Person Affected shall be able to register for one digital identity as an Identity Owner | In line with SSI principles | Functional | High |
| R.2 | Person Affected | Registration | Each Person Affected shall be able to self-register or register by delegate | A share of the Person Affected does not own a mobile device, a share will own a mobile device which saves resources | Functional | High |
| R.3 | Humanitarian Organization | Registration | Each Person Affected should add a geolocation when registering | CTPs are based upon a geographical area where a disaster has struck, but opening up private data is a trade-off | Functional | Medium |
| R.4 | Technical Analysis, Institutional Analysis | Registration | System shall only request a maximum amount of identity attributes | Data minimization and minimalization | Functional | High |
| R.5 | Technical Analysis, Institutional Analysis | Registration | System should check for double identities | To prevent fraud | Functional | Medium |
| R.6 | Humanitarian Organizations, Technical Analysis | Registration | Humanitarian Organizations shall ask Person Affected to provide consent for the use of data | To gain understanding of sharing their data and complying with national authorities | Functional | High |
| R.7 | Humanitarian organizations, Institutional Analysis | Registration | Only humanitarian Organizations shall be able to register as an attribute provider, identity provider and service provider | Need to be able to show who they are to others in the system | Functional | High |
| R.8 | Community Representatives, Authorities | Registration | Community Representatives and Authorities should be able to register as an attribute provider | In CTPs community reps. and authorities assist in identification | Functional | Medium |
| R.9 | Humanitarian organizations | Registration | Humanitarian Organizations, Community Representatives and Authorities must have an humanitarian registration interface | To ease the process of registration | Non-Functional | High |
| R.10 | Institutional Analysis | Registration | System must allow all humanitarian organizations to become part of it | Enables inclusivity | Non-Functional | High |
| R.11 | Humanitarian organizations | Registration | Humanitarian Organizations may integrate their legacy systems for registration forms | Would require less changes in aid worker practices | Functional | Low |
| I.1 | Person Affected | Identification | A Person Affected shall be able to have identity attributes validated by several attribute providers | To improve their trustworthiness and have a permanent proof of their identity | Functional | High |
| I.2 | Humanitarian organizations, Community Representatives, National/Local Authorities | Identification | Attribute providers shall be able to validate identity attributes and geolocations | By sending out validators or receiving lists from community representatives or local authorities | Functional | High |
| I.3 | Humanitarian organizations, Community Representatives, National/Local Authorities,Person Affected | Identification | Attribute providers shall be able to issue verifying credentials | In this way other organizations will be able to see who signed certain credentials and people can build up identities | Functional | High |
| I.4 | Humanitarian organizations, Community Representatives, National/Local Authorities | Identification | Attribute providers must have an easy to use validation interface | To ease the process of validation | Non-Functional | High |
| I.5 | Technical Analysis | Identification | Person Affected must always be able to access his her credentials in a private storage | Allows for portability of the identity | Non-Functional | High |
| U.1 | Person Affected | Use | Person Affected must have an easy to use user-interface | Different languages, illiteracy and such should be dealt with | Non-Functional | High |
| U.2 | Person Affected | Use | A Person Affected shall be able to request services throughout the system | A beneficiary will have to request to be matched with inclusion criteria | Functional | High |
| U.3 | Person Affected, Technical Analysis, Institutional Analysis | Use | Person Affected shall be able to safely access, update, disclose and revoke their identities | User-centered approach | Functional | High |
| U.4 | Person Affected, Technical Analysis, Institutional Analysis | Use | Person Affected shall be able to regain access to their identity after loss of control or loss of access | Makes for a persistent and sustainable identity | Functional | High |
| T.1 | Humanitarian organizations, Donors | Targeting (use) | Humanitarian Organizations shall be able to match Person Affected with their inclusion criteria | Determining if the most vulnerable are receiving assistance | Functional | High |
| T.2 | Humanitarian organizations | Targeting (use) | Humanitarian Organizations must have a service interface for targeting | To ease the process of targeting | Non-Functional | High |
| T.3 | Humanitarian organizations, Donors, Institutional Analysis, | Targeting (use) | Humanitarian Organizations shall be able to verify identities based on issued credentials from other organizations | Check who has validated identities and if they are to be trusted | Functional | High |
| T.4 | Humanitarian organizations | Targeting (use) | Humanitarian Organizations must only be able to set up inclusion criteria based on minimum amount of identity attributes | Standardizing inclusion criteria enables interoperability and scalability | Non-Functional | High |
| T.5 | Merchants and other service providers | Targeting (use) | Merchants and service providers may receive a minimum viable data on selected Person Affected | In some context humanitarian organizations are not able to provide services themselves, but rather not | Functional | Low |
| T.6 | Humanitarian organizations | Targeting (use) | System may be able to communicate with unregistered people | Via text-messages, social media or mailings to push them to register | Functional | Low |
| T.7 | Institutional Analysis | Targeting (use) | Humanitarian organizations should delete all information that is no longer necessary for a CTP project | Timeliness of the data and creating minimum data sets, difficult to set time-limits and keep to it themselves | Functional | Medium |
| C.1 | Technical Analysis | Cycle | The system must have roles for Identity Owners, Attribute Providers, Service Providers and Identity Providers | Are the minimum role necessary in a digital identity life-cycle | Non-Functional | High |
| C.2 | Person Affected | Cycle | A Person Affected should be able to provide feedback during use of the system | Providing feedback is necessary to improve the system and create transparency | Functional | Medium |
| C.3 | Humanitarian Organizations, Technical Analysis, Donors | Cycle | System should be able to provide open response to the feedback of people | Ensures openness and transparency | Functional | Medium |
| C.4 | Humanitarian organizations | Cycle | Humanitarian Organizations shall be able to create sub-entities to pass down responsibilities | Humanitarian organizations collaborate with local volunteers, free-lancers etc | Functional | High |
| C.5 | Humanitarian organizations | Cycle | All participants and the system must safely store all information | Prevents fraud and improves privacy and security | Non-Functional | High |
| C.6 | Technical Analysis, Institutional Analysis | Cycle | System must provide secure end-to-end encryption for all communication and sharing of data | Increases trust in the system | Non-Functional | High |
| C.7 | Technical Analysis, Institutional Analysis | Cycle | System must provide the highest form of privacy feasible | To protect Person Affected and humanitarian organizations for data loss or data breaches, do no harm | Non-Functional | High |
| C.8 | Humanitarian organizations | Cycle | System should enable an overview of where people have been registered | Humanitarian sector can see where registration should be promoted | Functional | Medium |
| C.9 | Humanitarian organizations | Cycle | System must demand high data standards for all humanitarian organizations | Enables trust in collaboration | Non-Functional | High |
| C.10 | Humanitarian organizations | Cycle | System must be inclusive and accessible for all humanitarian organizations | Enables the will for collaboration | Non-Functional | High |
| C.11 | Humanitarian organizations | Cycle | System must be accessible at all times | Registration can take place long before a disaster strikes | Non-Functional | High |
| C.12 | Technical Analysis, Institutional Analysis, Participatory Analysis | Cycle | System must be flexible and able to scale up | To grow inline with the use of CTPs and be adjustable during the implementation/use phases | Non-Functional | High |
| C.13 | Technical Analysis, Institutional Analysis | Cycle | System must be open-source | Systems and algorithms must be transparent | Non-Functional | High |
| C.14 | Technical Analysis, Institutional Analysis | Cycle | System must use interoperable standards for digital identification | To increase interoperability | Non-Functional | High |
| C.15 | Institutional Analysis, Donors | Cycle | System must open up the governance structure online | Enables transparency and openness | Non-Functional | High |
| C.16 | Participatory Analysis | Cycle | System must have a functional purpose and grow into a foundational purpose | Starts with the use for CTPs but has the potential for much more | Non-Functional | Medium |
| C.17 | Participatory Analysis | Cycle | System must be accompanied by a participation model and process approach | Complex socio-technical system, many stakeholders will want to influence it or they will not use it at all | Non-Functional | High |
| C.18 | Participatory Analysis | Cycle | System must not have a single owner | Ensures trust in the system and provides the opportunity for equal collaboration | Non-Functional | High |
| C.19 | Participatory Analysis | Cycle | System must have an incentive system to demonstrate good behavior | To make sure that all participants strive for data quality and data accuracy | Non-Functional | High |
| C.20 | Person Affected, Humanitarian Organizations | Cycle | Actors in the system shall be able to communicate with each other if communication is initiated by the Identity Owner | Messages on success of registration, success of inclusion must be send | Functional | High |

any information on the identity owners, they only need to know whether they are eligible. What they might store is an inclusion result, this should only be stored for the duration of the project. Two points deserve further explanation. First, in CTPs it is often the case that the last-mile (payment) is provided by a service provider or merchant. They would need some information on the included people to perform their services. Since this research only focuses on the identity part of CTPs and not on this last-mile solution, this export of information is seen as an end-point. Second, *T.6* stems from the concept that unregistered people cannot be part of the matching with inclusion criteria and must be invited to register. If there are any digital means such as lists with phone-numbers, mail addresses or social media channels, the system might be able based on the inclusion criteria and geographical reach to try and reach these people.

### 4.4.5. Throughout the life-cycle

The majority of the requirements are necessary throughout the entire life-cycle. There must be different roles with regards to the identity life-cycle as expressed in *C.1*, but also feedback must be provided and responded to. If response on feedback do not entail any private information they might be opened up to offer transparency. Transparency is also needed for the governance and the working of the system and its algorithms, which is why an open source approach is taken. Requirements *C.9, C.10, C.15, C.17, C.18* and *C.19* have a process management aspect to it. As stated before, this complex socio-technical problem will only find a working solution if it is accepted that implementation and final use of the system is defined by a process approach. The actual approach is out of scope, yet it is important to see if some of these aspects can be incorporated or allow for flexibility in the more technical design this thesis delivers. Another important requirement is *C.4* which states that humanitarian organizations should be able to pass down some of its responsibilities and public status, in other words, humanitarian aid workers should be able to access this system as validators and be trusted because they are vouched for by a humanitarian organization. Also many of these requirements touch upon trust and the means to collaborate within the humanitarian sector such as (*C.5*) to ensure storage of data is state-of-the-art, high data standards are used (*C.9*), accessibility of the system at all times (*C.11*) and standards for digital identity are incorporated (*C.14*). Lastly, the system must be designed so that growth and flexibility are accommodated for. Not only because of the increased use of CTPs, but also because of the process approach later and its purpose for other activities in a more foundational purpose.

### 4.4.6. Prioritization

Each requirement has been given a prioritization as can be seen in the last column of table 4.2. High, means it is part of the core system and simply must be there. Medium, implies that it should be part of the system, but the basic functions will still work if they are left out. Low, involves the nice to have requirements. They have added value to the system, but can be integrated at a later stage. In this thesis research, only the requirements pertaining a high and medium status are taken into the system design phase. Moreover, requirements that have a large process aspect might not be fully covered by the design. This will be dealt with in chapter 5, paragraph 5.5.

## 4.5. Sub-conclusion of Requirements Engineering

This chapter answers the second sub-question of this research: *Which design decisions have to be made*. The specific type of artifacts were first described to give direction to the process of requirements engineering. There is one main artifact, the design decisions and three supporting artifacts. First is the program of requirements which is the final product depicted in this chapter, then there are UML class diagrams and BPMN models. Presenting both a dynamic and static view of the system, The program of requirements is depicted in full in table 4.2. This program of requirements is there for generic use, yet for this thesis a blockchain based system shall be designed. Not all requirements are necessary to be developed for a minimum viable product, which is denoted by the priority given to each requirement.

# 5

# System Design

*"It is impossible to design a system so perfect that no one needs to be good"*
- T.S. Eliot

In this chapter sub-question *3. Which design decisions have to be made?*

3.1. What alternatives are available for the design?

3.2. Which alternatives best satisfy the program of requirements?

3.3. Do the proposed design decisions match with the program of requirements?

A variety of methods is used to answer this sub-question. First, a comparative analysis is done on four similar systems for which information is derived from desk research. Also academic literature on cryptography, centralized identity systems and self-sovereign identity are examined. Second, participatory research is conducted. Here ideas and concepts are introduced to the NLRC system which can be drawn from for this system design. Part of this participatory research were several brainstorms, design sessions and meetings.

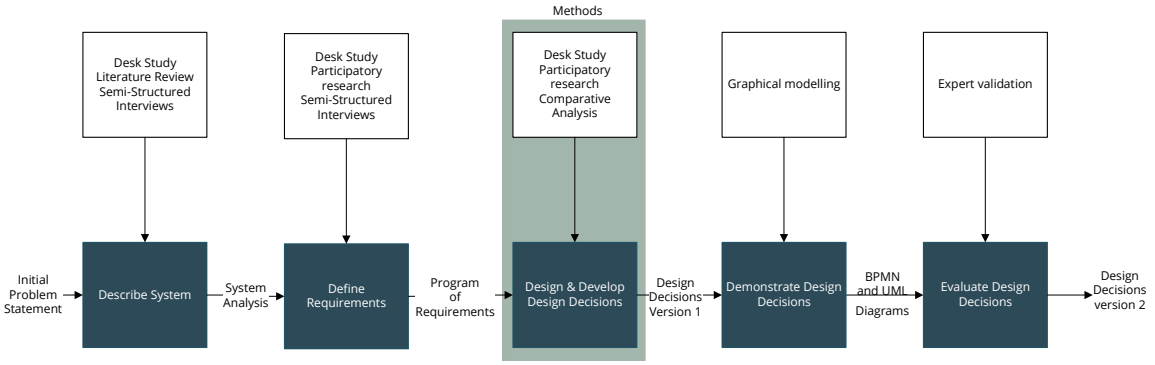



Figure 5.1: Methods for System Design

In the following paragraph 5.1 an introduction on systems design is given, this will lay out the steps that are taken in this chapter. In paragraph 5.2 four comparable systems are analyzed to generate alternatives for this system design. In paragraph 5.3 these alternatives are assessed and a set of concepts that has to be decided upon is provided. In paragraph 5.4 the design decisions are build up and in paragraph 5.5 this design is mapped on the program of requirements. In paragraph 5.6 the answers to sub-question 3 and its parts are given.

## 5.1. Introduction to System Design

System design is about translating a set of design requirements into a design which aims to solve a problem. Johannesson and Perjons [93] describe the following steps in designing an artifact:

1. *Generation of Alternatives*, which consists of imagining, brainstorming and analyzing alternatives to generate new ideas or elaborate on existing ones

2. *Assess and Select*, describes the phase where the ideas from the previous phase are assessed and which design decisions have to be made

3. *Sketch and Build*, in this phase the design decisions will be made

4. *Justify and Reflect*, where the design decisions are justified and reflected upon

During the design it is of importance to distinctly describe each design decisions and also prescribe how it suffices the program of requirements. Additionally, it should be made clear why this is an original design and should specify the sources of the design [93]. In the following paragraphs these steps are discussed.

## 5.2. Generation of Alternatives

Generating alternatives is the key to identifying the uniqueness of the to-be-designed artifacts. It answers sub-question *3.1. What alternatives are available for the design decisions?* There are various ways of generating alternatives. One could start from each requirement and create various options per requirement, these could then be displayed in a morphological chart upon which a decisions for one design can be made. This would take a lot of time and may result in an information overflow. In this research a comparative analysis of four other systems is used, this provides a concise scope but also a path dependency. These existing systems are analyzed and reflected to the program of requirements established in the previous chapter. There are many systems around the world that deal with digital identities, an overview of related or similar systems can be found in appendix D. Based on requirement *C.13 System must be open-source* and the research question pointing to the use of blockchain four systems were used to generate alternatives: Blockstack, Sovrin, the Netherlands Red Cross (NLRC) system and uPort. These four systems have been analyzed for which relatively little academic literature was available; mainly blogposts, Githubs and other grey literature was used. These systems use different terminology for similar concepts, to establish some common ground the following four roles (based on the digital identity life-cycle) are used, it is possible that some roles are fulfilled by one entity:

- Identity Owner (IO): wants to have a digital identity, can be a potential beneficiary, end-user of the system, a peer in the network

- Attribute Provider (AP): providing attributes for validation, can be a humanitarian organization, authority, peer

- Identity Provider (IdP): providing the opportunity for initial registration, is a piece of software that can be downloaded and often named a client

- Service Provider (SP): provides a service that the identity owner wants, for CTPs a humanitarian organization can also be other systems

Another note is that since this analysis talks about other systems, for clarity it will be good to talk about humanID as the system to be designed. These other systems all have a global coverage and a more foundational concept of identity, this is something humanID should grow to but it starts out as a system with a functional purpose, enabling CTPs at scale as stated in requirement *C.16*.

### 5.2.1. Blockstack

Blockstack proposes a new Internet for decentralized applications (dAPPs), which are applications that have their back-end running on a decentralized network such as a blockchain. Blockstack follows a *can't-be-evil* design philosophy, which means it cannot "alter, transfer, or revoke the user's identity, and they cannot read or write the user's data without permission"[27]. Blockstack views identity as a purpose to sign in with dAPPS, not as an institutional concept, yet their technological foundation might be of interest.

*Registration* is necessary to connect with one of the dAPPS on their network. Their foundation for registration are Uniform Resource Identifiers (URI), which is a string of characters that refers unambiguously to a certain resource, yet they are not really persistent [54]. To register an IO downloads the desktop application, agrees with the terms and conditions and then creates a Blockstack account that can hold identity attributes among other things. To access the account an IO receives a public-private key set of which the private key is stored on the desktop and the public key stored off-chain but an URI points to it from the blockchain, to create a decentralized public key infrastructure. With off-chain storage a user-managed data vault is meant which can be many things such as IPFS, an identity hub or cloud storage. The identity attributes themselves are stored off-chain as well.

*Identification* or validation is possible by peers and by organizations. There is no off-line import possible for identity attributes by APs in case of no internet connectivity, because Blockstack is fully internet dependent. Only attributes can be validated for which credentials can be given, the public key that signs the credentials enforce trust. Blockstack is a public permissionless chain, so any organization can go on there and validate without approval of the network.

*Targeting* is not possible in Blockstack. *Using* the digital identity is made easy by logging in to the desktop applications where identity attributes could be changed and disclosure to other peers can be selectively revoked [4]. Selective disclosure is the ability to only show relevant attributes and not the whole identity [148] and is a key concept in privacy preserving techniques.

With selective disclosure an attribute provider gives out a credential to a IO and the IO shows this to service provider to confirm eligibility, making the identity owner at the centre. Translating this to CTPs it would mean that a humanitarian organization, would not have to share data with SPs or authorities. In this way, the humanitarian organization has no idea where the beneficiary uses her identity for ensuring privacy [53]. Selective disclosure could be improved upon by using multi-show unlinkability, but none of the systems discussed here do so. It is used at scale by IBM Identity Mixer [133]. Upon registration someone receives a twelve word key-phrase, that is needed when their private key is lost. If this key-phrase is lost the identity is inaccessible.

Blockstack uses the GPLv3 open source license and since it is public permissionless, there is no single owner in their system. Added to the roles described before this analysis, Blockstack distinguishes Storage providers. These can be all sort of providers such as Amazon S3, Dropbox, a personal drive or a private identity hub. In figure 5.2 the Blockstack architecture is depicted, where in the top these storage providers can be seen.

Each participant in the network has the same interface, as peer-validation is similar to validation by organizations. As can be seen in figure 5.2, but also identified by Abraham [4] the following layers can be separated:

1. Blockchain layer: is Bitcoin which stores operations and provides consensus on the order in which the operations are written op the blockchain. There is a also virtualchain where new operations are stated so that the underlying blockchain only has to be include the meta-data and not entire operations.

2. Network layer: Atlas, that separates data storage and routing requests. The integrity of the routing can be checked in the blockchain layer.

3. Storage layer: Off-chain and allows for different storage back-ends, the integrity of the storage can be checked in the network layer.

4. Consensus layer: Proof-of-Work, and gives a reward to the first miner that approves of the new transaction to be added to the blockchain

5. Application layer: Desktop Application for Identity, Storage and Discovery

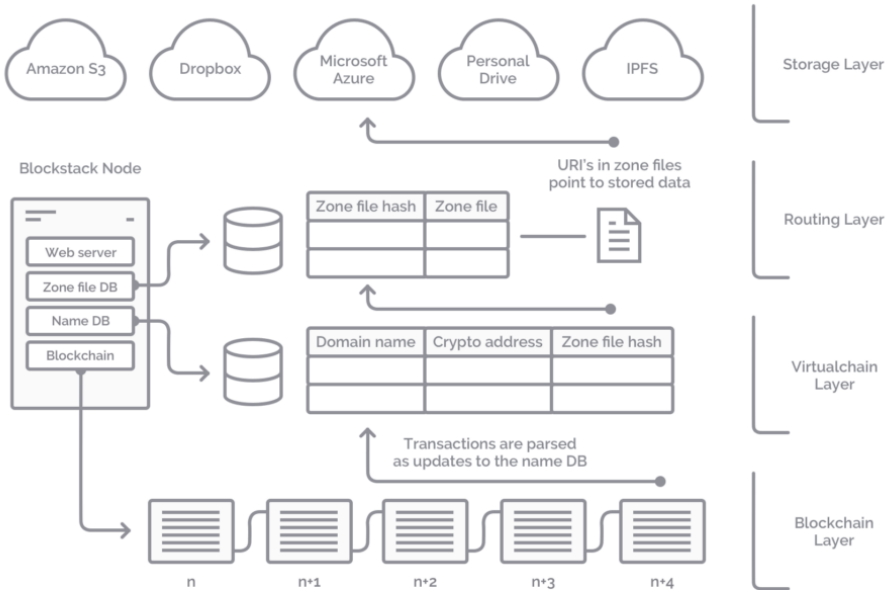



Figure 5.2: Blockstack Architecture Overview from Ali et al. [7]

In Blockstack any organization can join because it is public permissionless. Blockstack is now working on its scalability by not using the blockchain for data storage or complex logic [8]. Using existing cloud storage for storage enables scale, since these cloud solutions are highly scalable [66]. The Atlas network Blockstack uses is an unstructured network, thus there can be a lot of look-up requests slowing down the system. In a structured network the number of these request would be lower and more scalable, but the system would be less secure as stated by Ali et al. [8]. In general, it is often the underlying blockchain and its consensus mechanism, in this case Bitcoin, that infer trouble when scaling up [81]. With Bitcoin there is already a huge outcry on the amount of energy needed for transactions, which is due to the mining needed for consensus. Since Blockstack requires a similar mining protocol, the same scalability issues apply.

### 5.2.2. Sovrin

Sovrin is "a utility for self-sovereign identity" [138]. Sovrin is designed specifically for the purpose of self-sovereign identities, privacy-by-design and scalability [137]. Sovrin is a concept and is being built on a public Github[1].

*Registration* on Sovrin will be done via a mobile or desktop application and has to be portable to ensure the lifetime of a digital identity. An Identity Wallet allows for this portability, which is a digital container belonging to a single entity that holds credentials, money and other items. It has an identifiable location on the mobile phone or desktop, yet it can be moved [86]. For Sovrin it holds the DIDs and keys.

#### Intermezzo: Decentralized Identifiers (DID)

DIDs are a key component of self-sovereign identities and are standardized by the W3C [156]. They can be used on any blockchain. A DID allows anyone to create identifiers for anything, they are pairwise pseudonymous which means that they are only used between one IO and one other party. In practice an IO may have hundreds of DIDs to represent all their digital relationships. Each DID is secured by the private key of the identity owner, the public keys and pseudonymous biometrics can be stored in the DDO as can be seen in figure 5.3. This enables the IO to proof ownership of the DID. The DDO also contains information on how to connect to the IO for trusted interactions. Another part of the DID is the method, which defines how the DID is registered, resolved, updated and revoked. DIDs are similar to the URIs used by Blockstack but are more comprehensive. Figure 5.3 also presents how DIDs could work. In the middle a DID Decentralized Hash Table is located, which allows each node

[1] https://github.com/sovrin-foundation/sovrin

to quickly look up DIDs for verification [101]. An AP issues a verified credential and publishes some proof of this on the blockchain. Via the blockchain the AP can verify the identity of the IO. The IO stores these credentials in their identity wallet, or somewhere else which is secure and off-chain. The IO manages its DID for the specific connection with the AP and with the SP. To get a service, the IO sends there credentials to the SP with a pointer to its DID. The SP then checks the public proof given by the AP, whom it trusts and can verify the identity via the blockchain.

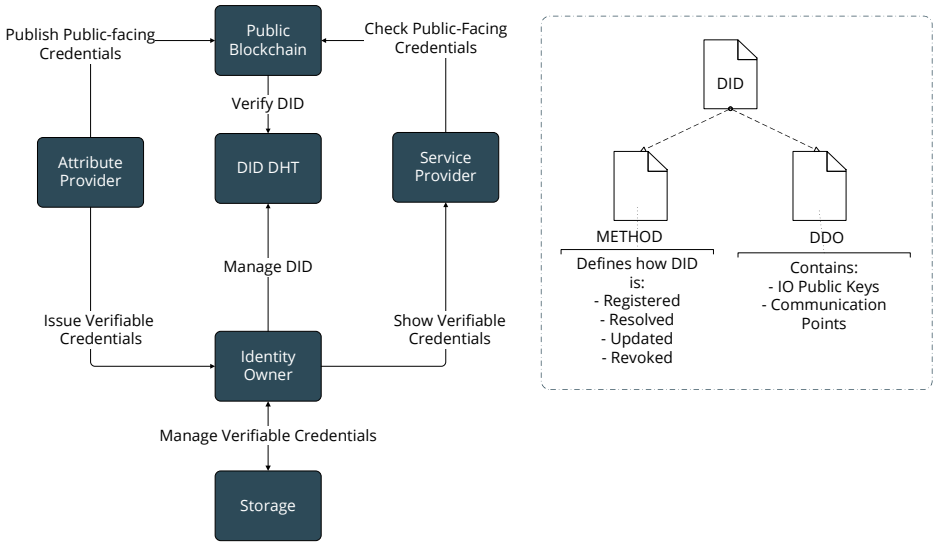



Figure 5.3: DIDs based on Sporny and Longley [139]

Back to registration, in Sovrin an IO submits identity attributes according to a pre-set data scheme [4] and Sovrin creates a public-private key set which enables asymmetric encryption of data. Since DIDs exist between two counterparts, they know each other public keys. To communicate, organization A sends a message and encrypts it with the public key of organization B, that can decrypt it with its private key. Storing the public keys in a decentralized environment such as blockchain supports the creation of a Decentralized Public Key Infrastructure, which has no single point of failure and is naturally more capable of growing.

*Identification* in Sovrin has already been described but to add on it, Sovrin also states it allows for peer-validation. Validation of identity attributes is initiated by the IO who knows that some AP is connected to the Sovrin network and has the ability to issue credentials for the IO. How peer-validation is possible and how trust-worthy it is depends on how a service provider will judge it and what incentives peers have to provide honest validation. Since Sovrin does not use a cryptocurrency for incentives, as Bitcoin does, it remains unclear how plausible peer-validation at scale will be.

*Targeting* within the system is not possible in Sovrin. *Using* identities has also partly been described above. DIDs allow for selective disclosure and can be revoked, as is specified in the DID Method. Sovrin also provides Zero-Knowledge Proofs (ZKP) as a privacy-enhancing technology. A ZKP discloses zero information about the identity attribute, but only states that it is true or false, and that it has been validated by a trustworthy AP. The use of ZKPs are computationally intensive and are therefore no common practice, yet Sovrin claims it has realized the infrastructure to enable widespread use. Potentially using shorter zk-SNARKS, that are compatible with blockchain and most notably used by Zcash [133]. Loss of a private key can be recovered in two ways, either offline or [85]. Social recovery means that an IO can identify trusted peers to help restore their access and create new key-sets, a minimum of three is recommended. Offline recovery means that a physical back-up can be made, for example a QR code or on a secured USB key. These can also be lost or stolen.

Sovrin has a different set-up of roles. There are Trustees, who form the highest entity and are a group of people formed by Sovrin. These Trustees appoint Stewards, which can be persons or organizations that have the right to appoint what they call Validator nodes. These nodes are the only

nodes that can write to the blockchain. In a layer around these Validator nodes, Observer nodes exist that only broadcast the blockchain by and provide reading access. Stewards also appoint Trust Anchors, these are organizations or people that are granted the ability to provide identities, issue credentials and deliver services. In the outer layer, the agents (pieces of software) communicate with each other off-chain. An agent represents a Trust Anchor or an IO, although IOs can also be their own agent. Agents can be developed by Trust Anchors or by other organizations, which might create a business model. To create an overview, the key elements described here are depicted in figure 5.4. So Sovrin is public permissioned, anyone can join but not all have the same rights. This set-up also implies there is no single owner, but a federation of Trustees that ”own” the system. Sovrin offers Software Development Kits to create interfaces, but as of now none of them are up and running, similar to the user interfaces.

Sovrin uses an Apache2 license. In a whitepaper from Sovrin they state it can be thought of as a three layer software stack [137] plus an application layer:

1. Blockchain layer: Hyperledger Indy
2. Network layer: Sovrin
3. Consensus layer: Plenum
4. Application layer: Mobile/Desktop application for Identity

Sovrin states it is designed for scalability [137]. The use of a core of Validator nodes and larger layer of Observer nodes allows for this scale. Yet, since Sovrin is a public permissioned chain they have much more capacity to scale since it needs less computing power to create consensus. Another way they improve scaling is the use of multiple blockchains that hold different internal information such as a pool for validator nodes [103].

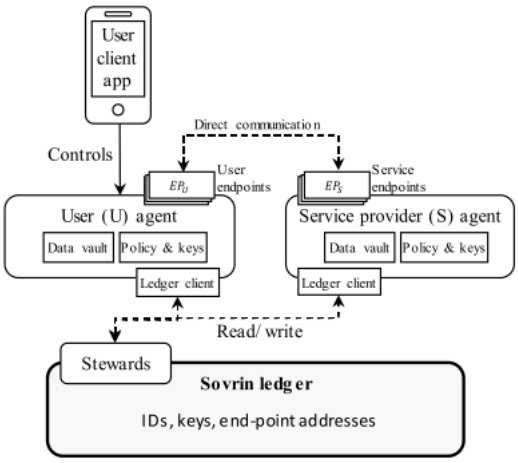



Figure 5.4: Sovrin Key Elements from [55]

### 5.2.3. NLRC

The NLRC system is still in its early phases of development and focuses on self-sovereign identities with the functional purpose of registration and identification to enable targeting in CTPs. The system is developed in-house together with several development partners and aims to later open up and include other humanitarian organizations.

*Registration* is done via a web, mobile or desktop application. This has yet to be finalized, but for the first pilot a web-application will be used. Identity owners will submit their identity attributes and information on their geographical whereabouts, since CTPs are location-bound. People will have to provide consent to use the application, yet in many ways consent is integrated into the selective disclosure of identity attributes. The information is stored in a digital wallet. In the internal documents on the system design (version 06-06-2018), a hash of the public key, a hash of the identity attributes

and a geolocation are put on the blockchain. In a block on the chain a Merkle Tree of all these hashes is presented. A Merkle tree is a data structure that combines multiple hashes into one root-hash, changing one of the data inputs will corrupt the root-hash. The private key and identity attributes are stored on the device or printed on paper using a QR code. The geolocation is used to create aggregated data on registrations, which is then visualized on a map for others to see and prioritize areas where registration needs to be done or validation is going to be worthwhile. Registration is also possible via a delegate, in that case the private key is definitely stored on paper.

*Identification* is done using humanitarian validators or peers. Self-attestation, so no validation will yield the lowest trust score. Peer-validation will result in a middle trust score and humanitarian validation in a high trust score, in this way an IO can build up a trust. In either way a validator will have its own interface and provides credentials for the validation.

*Targeting* is possible as the system allows for a specific CTP set-up which imports inclusion criteria and then requests an inclusion result on the registered identities. An IO receives a form from a humanitarian organization, which somehow has made contact with the IO. The IO fills in this form and the system creates a ZKP of the submitted identity attributes. Based on this ZKPs, the inclusion criteria are matched with the IO and an inclusion score is created. Based on this score, the IO might or might not receive cash which is the next component of this system. The system design stores these inclusion scores indefinitely. People that have not been registered are not eligible for the CTP, this system does not offer any methods to reach these people.

*Use* of the identity is momentarily still limited, but in a whitepaper published by the NLRC it shows it should be able to use it on a global level and initially for CTPs but later also for other uses. Key recovery must be a part of the system and is now done via sharding or what is known as Samir's Secret Sharing, where pieces of a key are distributed across the network. Bringing together all pieces in the right order, will yield access to the account in case of private key loss. This is similar to the social approach taken by Sovrin. Merkle Trees also allow for selective disclosure [18].

The NLRC has not chosen for a specific license yet, during participatory research it became clear that there might be a need for a specific humanitarian open source license. That does not allow for commercialization but does promote widespread use.

The roles in this system are that of PersonAffected, which is similar to the IO role. Humanitarian organizations that conduct targeting (SP) and provide identities (IdP) and Attestors that do the validation and are similar to APs. Other humanitarian organizations can be allowed in the network but can only do so by collaborating in the participation model [65]. This model describes how roles are divided, how maintenance is done and how much resources must be set free. This model is out of scope for this research, but since it is a complex socio-technical problem should be researched and implemented for the humanID design. The system is in fact a public permissionless chain. Feedback in this system shall be done via chatbots and the current local representatives, these chatbots can be accessed via the user interface.

The NLRC systems has the following layers:

1. Blockchain layer: RSK running on the Bitcoin blockchain, RSK enables smart contracts on this blockchain

2. Network layer: Ginger, a test-network

3. Consensus layer: Delegated Proof-of-Stake, which enables people to vote on witnesses by the amount of tokens they have, the witnesses are in charge of securing the network and get paid to do so

4. Application layer: Web/Mobile/Desktop application for Identity, Targeting and Cash Disbursement

RSK is a thin layer on top of the Bitcoin blockchain, similar as to how Sovrin is layer on Hyperledger Indy. RSK enables the use of smart-contracts on the Bitcoin chain, which in the NLRC system are used to link the identity module named ANA with the cash module named IOU. RSK has recently released the Ginger test-network which has the potential of scaling up to 300-1000 transaction per second (Bitcoin is at 3-24 transactions per second) [114]. However, such results have not been achieved at the moment of writing.

### 5.2.4. uPort

uPort is a dedicated self-sovereign digital identity system. The uPort mobile application can be downloaded from several app-stores and is ready for use. uPort is well known for a trial they conducted with the municipality of Zugg in Switzerland, which still needed a central institution for identification but did showcase the applicability [99].

*Registration* in uPort is quite simple. An IO downloads the application, where you give consent by agreeing upon the terms and conditions and where you add your name and country then confirm that the phone is yours by entering a code received by text. Upon registration a key-set is created, where the private key is stored on the phone, the public key is stored on the InterPlanetaryFileSystem (IPFS) enabling a decentralized public key infrastructure (DPKI). The public key could also be stored on a cloud service, but then it is not decentralized anymore [4]. The identity data itself is also stored in IPFS and not on the chain. The IPFS is a storage layer for decentralized applications, data is addressed via a hash which ensures links to data will always remain the same [23]. Ideal for blockchain because it allows for looking up large amounts of data, less ideal for private data because it aims to store links to it forever. In figure 5.5 an overview of the uPort key elements is shown. There are four smart-contracts: the controller contract, the proxy-contract, the registry contract and the application contract. The controller and proxy contract are created by a transaction to Ethereum caused by the registration [55]. The proxy contract contains encrypted references to a DID. The proxy contract can do two things: read/write the registry or call the application layer. The registry contract contains hash references of the identity attributes which can be updated by the owner of the identity and the application contract can read the status of identity attributes on the registry [55].

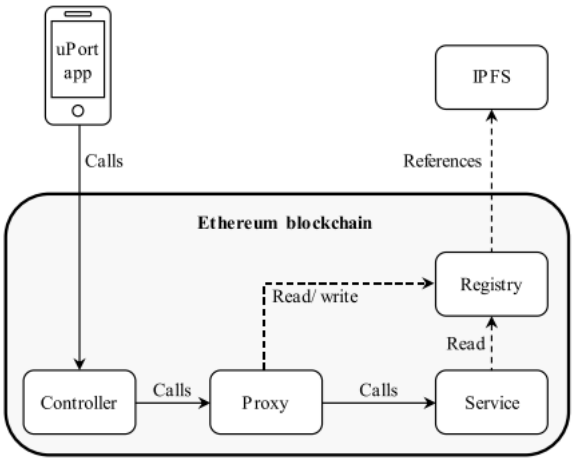



Figure 5.5: uPort Key Elements from Dunphy and Petitcolas [55]

*Identification* can be done by peers or organizations which have the same status as it is a public permissionless blockchain. How peer-validation would add value is not clearly stated by uPort.

*Targeting* is not made possible in uPort. *Use* of the digital identity is done via the mobile application. Selective disclosure and revoking are made possible by the DID format. Keys can be recovered in an offline way by making a back-up or by appointing trusted peers, that can invoke the controller contract to create a new set of keys [55]. Any feedback or questions can be dealt with via the FAQ and discussion forum.

Like Sovrin, uPort uses the Apache2 license. In uPort there are very few roles. There are IOs, APs and SPs. Identities are simply provided by the application, since there is no standard data format the identity can be a bare minimum. For each of these roles there is an interface, the IO has a user interface via the smart-phone and the others can create one by downloading a Software Development Kit and creating one.

uPort has the following layers:

1. Blockchain layer: Ethereum, which enables the use of smart contracts
2. Network layer: Rinkeby test-network by default for the mobile application, but offers to change to other networks

3. Storage layer: IPFS, but also possible on Azure, AWS, Dropbox etc.
4. Consensus layer: Proof-of-Stake, which is designed to work fast with a slow CPU [4]
5. Application layer: Mobile application for Identity

uPort is currently held small on the Rinkeby test-network and needs to be adjusted before it could be put on the Ethereum main-network which does have the potential for scale. At the moment this test-net ensures there are no real costs for executing the smart-contracts, but by putting it on the main-network these costs would become too high to be a viable solution [129].

## 5.3. Assessment and Selection of Alternatives

Comparing Blockstack, Sovrin, NLRC and uPort has showed a variety of technologies, architectures and system components that can be used by humanID. To compare these four systems, they are mapped to the program of requirements as can been seen in table 5.1. The NLRC project is very similar to humanID in its overall objective to scale up CTPs, while Blockstack is most farthest from the objective as it is less focused on a self-sovereign identity and more on a new decentralized internet. To determine what design decisions should be made in the coming paragraph, it is of importance to look at the differences between these systems and evaluate if the similarities are also relevant for humanID. Please note that all of these systems are continuously being developed and their features/architecture might have changed from the moment of writing.

### 5.3.1. Differences Between the Systems

Based on these differences it is assumed that certain trade-offs can be made for which a design decision is necessary. The first clear difference is that of being a public permissioned (Sovrin) or public permissionless (Blockstack, NLRC and uPort) chain. This is reflected by *R.10* which shows that with Sovrin not all organizations can join automatically. It is also reflected by the scalability in *C.12* that shows that permissionless chains are less scalable. Each has its own advantages and disadvantages, which is why a decision has to be taken. This choice will have a ripple effect on other choices such as the layered architecture, roles and interfaces and a user-centred design. Which layers are used determines for example the use smart-contracts such as in RSK (NLRC) or Ethereum (uPort), while others offer no smart-contract solutions. A network can be built from scratch, or an existing network could be used like Blockstack and the NLRC do which runs on top of Bitcoin. A permissioned chain allows for different roles outside the blockchain, as it requires trust in code and trust in organizations. This translates into a different application layer. For example, the NLRC distinguishes between roles for humanitarian organizations while Blockstack and uPort do not. The latter view the humanitarian organizations as just one of the service providers (*T.1, T.2*). This aligns better with the self-sovereign principles and the foundational purpose of an identity system, which is why it conflicts with *C.16.*. Hence, after deciding upon the type of blockchain a design decision on the layers and roles is required.

Each of these identity systems is based around identifiers which identify a unique object, or in this case person or organization. Blockstack uses URI's, Sovrin and uPort use DIDs. The use of a type of identifier reflects on the user-centred design (*C.20*) and interoperability of standards (*C.14*). A true self-sovereign system would rely on identifiers that enable this. The type of identifier can determine a great deal in the system and should therefore be carefully selected.

There are also differences to be seen in the use of open source licenses. These licenses range from being permissive to strongly protective based on the objective. The Apache 2.0. license is a more permissive one and used by Sovrin and uPort, while Blockstack uses a GPLv3 license that is strongly permissive. There are no specific humanitarian open source licenses so a decision on what is best suitable for this use-case must be made.

Sovrin, uPort and Blockstack store private keys on the device or within the application. While the NLRC also offers to store the private key on a paper-card. Storage on the blockchain is reserved for little data because the blockchain is not an ideal database, so there is a need to pick an offchain storage. uPort uses IPFS, Blockstack lets you integrate with various storages and for Sovrin and the NLRC it remains unclear for now. A decision on how to deal with offchain storage should be taken.

Key loss is also dealt with differently by each of the compared alternatives, although each of them uses a DPKI structure. Sovrin and uPort both offer a social recovery scheme, where Blockstack only

Table 5.1: Comparison of Alternatives versus Requirements

| ID | Requirement | Blockstack | NLRC | Sovrin | uPort |
|---|---|---|---|---|---|
| R.1 | Each Person Affected shall be able to register for one digital identity as an Identity Owner | No | No | No | No |
| R.2 | Each Person Affected shall be able to self-register or register by delegate | No | Yes | Yes | No |
| R.3 | Each Person Affected should add a geo-location when registering | No | Yes | No | Yes |
| R.4 | System shall only request a maximum amount of identity attributes | No | Yes | Yes | No |
| R.5 | System should check for double identities | No | No | No | No |
| R.6 | Humanitarian Organizations shall ask Person Affected to provide consent for the use of data | Yes | Yes | Yes | Yes |
| R.7 | Only humanitarian Organizations shall be able to register as an attribute provider, identity provider and service provider | No | Yes | No | No |
| R.8 | Community Representatives and Authorities should be able to register as an attribute provider | Yes | Yes | Yes | Yes |
| R.9 | Humanitarian Organizations, Community Representatives and Authorities must have an humanitarian registration interface | Yes | Yes | Yes | Yes |
| R.10 | System must allow all humanitarian organizations to become part of it | Yes | Yes | No | Yes |
| I.1 | A Person Affected shall be able to have identity attributes validated by several attribute providers | Yes | Yes | Yes | Yes |
| I.2 | Attribute providers shall be able to validate identity attributes and geolocations | Yes | Yes | Yes | Yes |
| I.3 | Attribute providers shall be able to issue verifying credentials | Yes | Yes | Yes | Yes |
| I.4 | Attribute providers must have an easy to use validation interface | Yes | Yes | Yes | Yes |
| I.5 | Person Affected must always be able to access his/her credentials in a private storage | Yes | Yes | Yes | Yes |
| U.1 | Person Affected must have an easy to use user-interface | Yes | Yes | Yes | Yes |
| U.2 | A Person Affected shall be able to request services throughout the system | Yes | No | Yes | Yes |
| U.3 | Person Affected shall be able to safely access, update, disclose and revoke their identities | Yes | Yes | Yes | Yes |
| U.4 | Person Affected shall be able to regain access to their identity after loss of control or loss of access | Yes | Yes | Yes | Yes |
| T.1 | Humanitarian Organizations shall be able to match Person Affected with their inclusion criteria | Yes | Yes | Yes | Yes |
| T.2 | Humanitarian Organizations must have a service interface for targeting | No | Yes | No | No |
| T.3 | Humanitarian Organizations shall be able to verify identities based on issued credentials from other organizations | Yes | Yes | Yes | Yes |
| T.4 | Humanitarian Organizations must only be able to set up inclusion criteria based on minimum amount of identity attributes | No | Yes | No | No |
| T.7 | Humanitarian Organizations should delete all information that is no longer necessary for a CTP project | No | No | No | No |
| C.1 | The system must have roles for Identity Owners, Attribute Providers, Service Providers and Identity Providers | No | Yes | Yes | No |
| C.2 | A Person Affected should be able to provide feedback during use of the system | Yes | Yes | n/a | Yes |
| C.3 | System should be able to provide open response to the feedback of people | Yes | n/a | n/a | Yes |
| C.4 | Humanitarian Organizations shall be able to create sub-entities to pass down responsibilities | Yes | n/a | n/a | Yes |
| C.5 | All participants and the system must safely store all information | No | n/a | n/a | No |
| C.6 | System must provide secure end-to-end encryption for all communication and sharing of data | Yes | Yes | Yes | Yes |
| C.7 | System must provide the highest form of privacy feasible | No | Yes | Yes | Yes |
| C.8 | System should enable an overview of where people have been registered | No | Yes | No | No |
| C.9 | System must demand high data standards for all humanitarian organizations | n/a | n/a | n/a | n/a |
| C.10 | System must be inclusive and accessible for all humanitarian organizations | Yes | Yes | No | Yes |
| C.11 | System must be accessible at all times | Yes | Yes | Yes | Yes |
| C.12 | System must be flexible and able to scale up | No | n/a | Yes | No |
| C.13 | System must be open-source | Yes | Yes | Yes | Yes |
| C.14 | System must use interoperable standards for digital identification | Yes | n/a | Yes | Yes |
| C.15 | System must open up the governance structure online | Yes | n/a | Yes | n/a |
| C.16 | System must have a functional purpose and grow into a foundational purpose | No | No | No | No |
| C.17 | System must be accompanied by a participation model and process approach | No | Yes | Yes | No |
| C.18 | System must not have a single owner | Yes | Yes | Yes | Yes |
| C.19 | System must have an incentive system to demonstrate good behavior | Yes | Yes | Yes | Yes |
| C.20 | Actors in the system shall be able to communicate with each other if communication is initiated by the Identity Owner | No | No | Yes | Yes |

offers a twelve-word random key phrase. As people might loose their keys due to a disaster, theft or another act of God they must be able to retrieve their keys. Preferably many options are given, but maybe the options described by these four alternatives do not cut it. humanID must choose to put them altogether or single some of them out.

Lastly, in Sovrin, Blockstack and uPort targeting of people for a service is not possible. The initiative is always coming from the identity owner as is in accordance with self-sovereign principles. Until now targeting has been seen as something a humanitarian organization must initiate, which might be possible as demonstrated by NLRC but could not be favourable. How far a user-centred design should go must thus be decided upon and if targeting is seen as something separate or simply as a service that is provided.

### 5.3.2. Similarities Between the Systems

All systems are based around digital identity and for this they can all perform the main functions of a digital identity system such as registration, identification, using and maintaining the identities. It is evident that humanID should at least perform these tasks. On a technical basis, the main similarity between these systems is that they are all blockchain based, but since the program of requirements is blockchain agnostic it must be argued why blockchain is chosen for the humanID design. Each of these systems offer the option for peer-validation which makes sense for the permissionless systems as in essence everything is peer-validation. Sovrin also offers this feature, but it is difficult to see why since peer-validation in a permissioned system would mean that it has a different value than validation by other roles. Whether this is something that should also be integrated in humanID remains to be judged.

## 5.4. Sketch and Build of the Design Decisions

Assessing these four systems resulted in the selection of ten design decisions to be made, which answers sub-question *3.2 Which alternatives best satisfy the program of requirements?*.

### 5.4.1. Design Decision #1: Use blockchain technology

This decision was made at the start of this research and reflects upon several of the requirements. To recap why blockchain was seen as a viable part of this system, the following four reasons were mentioned:

- To enhance collaboration and interoperability in an untrusted environment by coding control to partly replace governance
- To enable sustainable self-sovereign identities that improve processes in CTPs but outlast the duration of a single CTP and are interoperable with other identity ecosystems
- A distributed architecture accommodates growth better than a centralized architecture
- Privacy-by-design is lacking and will be under more pressure when CTPs are scaled up, blockchain and its cryptographic protocols could enhance privacy at scale

Of course blockchains can be designed in various ways and this will influence how they will satisfy the requirements. Yet, blockchains enable the use of self-sovereign identities (SSI) at which the user is the centre of the design. This matches with requirement *U.3*, that a person should be able to safely access, update, disclose and revoke their identities. Having some sort of public blockchain also allows organizations in the system to verify who is issuing credentials (*T.3*) which creates more trust. Furthermore, the use of blockchain complies with a lot of requirements that are needed throughout the life-cycle. Safe storage, *C.5* is partly arranged via the blockchain, yet no private data will be stored there. This is why the requirement is not 100% fulfilled because depending on where you store private data there will always be room for error. As blockchain enables SSI, it enables one of the highest forms of privacy feasible *C.7*. Since, it is a distributed network there is no single point of failure which means the system should always be accessible and working (*C.11*). This distributed architecture also helps to scale up and since there is only one system needed for the humanitarian sector, it enables the use of interoperable standards (*C.14*) and there does not need to be a single owner (*C.18*). Additionally, the use of asymmetric encryption is common use in blockchain based

systems which ensures encrypted communication and transactions are possible and secure. In all the other systems asymmetric encryption was used to generate public-private key sets for access and signatures for messages. Asymmetric encryption is also used in humanID.

### 5.4.2. Design Decision #2: Use a public permissioned blockchain

uPort, NLRC and Blockstack both use public permissionless chains, while Sovrin uses a public permissioned chain. One could also use private chains, but this would prevent anyone from outside being able to register for a digital identity so it must be a public blockchain (*R.1, R.2*). Reasons for permissionless chains are that they can already run on an existing set of nodes, so it requires less time to build up a network and they are truly open thus have more transparency which increases trust. For a future where this blockchain is not only used for CTPs this might be a preferred choice. Yet, it might prove hard to implement and gain traction because there is little governance possible. Once the system is out there it is out there. The permissioned model offers a more efficient way of providing different roles with different levels of authorization, which better resembles the formal humanitarian governance model *R.7,R.8*. For example with a Cluster Approach or with a federated system from the IFRC. Also it creates a buy-in from stakeholders making them less likely to leave, which matches with setting up a participation model (*C.17*). Sovrin uses a publicly available Trust Framework for this [136], which must be signed by specific roles in their system. humanID should publish a similar statement as in accordance with *C.15*. This framework could also be part of incentivizing good behavior in the system (*C.19*). In such a framework agreements can be made on how participant must store information (*C.5*), who holds which legal responsibilities, how they must deal with feedback (*C.3*) and who runs which nodes to ensure access is available at all times (*C.11*). A permissioned chain also enables agreement on a standard set of identity attributes to be asked upon registration (*R.4*), something that has to be decided upon by certain roles in the system. A permissioned blockchain goes against the grain of pure self-sovereignty, since not all humanitarian organizations are be able to join by default (*R.10*). In practice this is still possible, but there is a barrier that is not there in a public permissionless chain and could prevent organizations from wanting to join. Yet, if they have joined they have created a buy-in and should be willing to further develop the system and participate in its success. Lastly, a permissioned chain offers more chances for scalability because it requires less CPU intensive consensus protocols. It fulfils more of the functional purpose that is required for CTPs and it is exactly that which the system should assist in scaling up (*C.16*). The functional purpose is specific for CTPs and results in a clear use-case, with a clear demarcation of important stakeholders and institutional environment. The functional purpose creates an installed base and lets developers deal with growing pains before scaling it up even further, outside the humanitarian sector. Because, to have a persistent added value there must be a continuous value proposition alongside the use for CTPs. Hence, it must become foundational at some point in time, where not only humanitarian organizations provide services. A permissioned blockchain enables this controlled growth. It creates a buy-in for organizations to join and lets the authorities decided when to open up, opposed to a public permissionless chain where any organization can join and leave as they please.

### 5.4.3. Design Decision #3: Use DIDs and and a fully User-centred Design

DIDs can be used on any blockchain and are specially designed for self-sovereign identities [156]. They allow for selective disclosure, for different subsets of identity attributes per connection and for revocation. Instead of DIDs, Blockstack uses URIs. The difference is that ownership, meta-data and public keys can be cryptographically verified with DIDs, this is necessary for validation of identifiers [156]. Also URIs today are likely to be based on Domain Name System (DNS) names or Internet Protocol (IP) addresses that do have a central authority behind them [156]. Another solution could have been to use Universally Unique Identifiers (UUIDs), which are the precursor of DIDs. They are similar, but DIDs can be resolved and revoked, plus the DDO contains cryptographic material needed for authentication of the IO, which UUIDs have not [156]. In other words, DIDs allow an identity owner to access, update, disclose and revoke their identities (*U.3*). DIDs conflict with the concept of only having one identity (*R.1*), because it enables people to have multiple identities depending on which organization they have relations with. All of these identities should refer back to one human being, which is difficult if identity attributes are only self-attested but is not necessary when identity attributes are validated by organizations. This makes checking for double identities (*R.5*) redundant. DIDs also enable multiple validation for one identity attribute because communication per attribute provider

cannot be correlated, this could improve objectivity (*I.1*). An attribute provider can issue credentials based on DIDs, and sign them with a public key to be verified and checked by others (*I.2, T.3*). In general DIDs enable the user-centred design because of the pairwise pseudonymous characteristics, it is then the identity owner that initiates the request for service (*U.2*) and communication with all other roles in the system (*C.20*), this process is visualized in figure 5.6.

Now that they have been standardized by the W3C, they can be interoperable and are the best future choice. This choice also entails the use of a decentralized public key infrastructure (DPKI), which was common use in all four compared systems. In a DPKI the public keys, which are part of the DID, are stored on the ledger, while the private keys are stored locally or on paper. Since each Person Affected must be able to register or access an identity but does not always have a connected device, this paper based key is of importance. To really enhance privacy, ZKPs (used by Sovrin and NLRC) and multi-show unlinkability (used by IBM Identity Mixer) should be added to the system. However, both have not been applied at scale in blockchain solutions and are therefore currently excluded of the design. If solid proof exists and if possible, they should be added later.

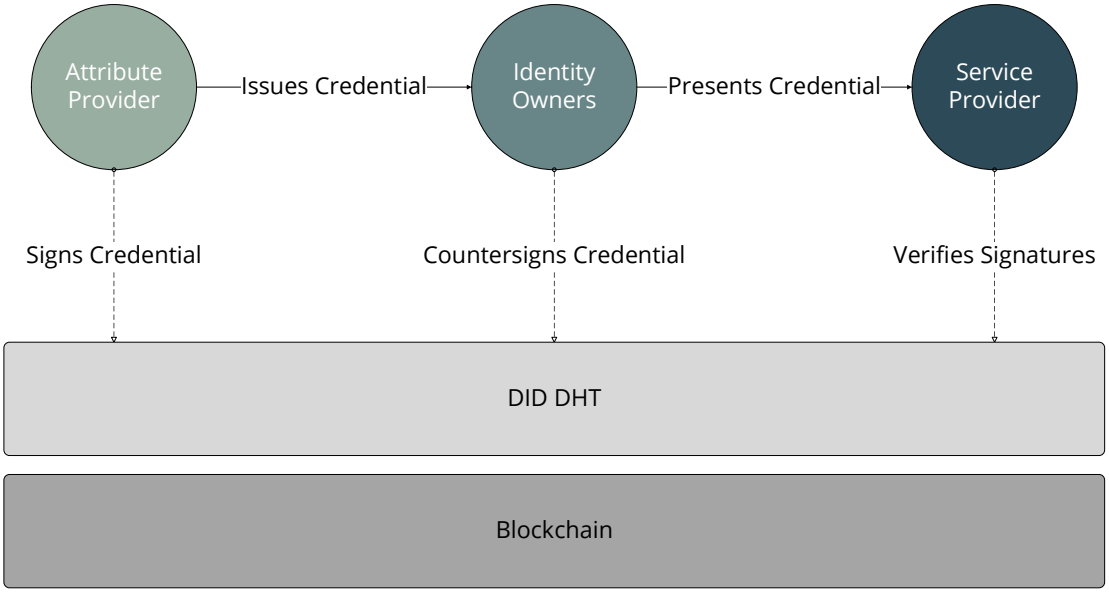



Figure 5.6: User-centred Verification Process based on Sovrin Foundation [137]

### 5.4.4. Design Decision #4: Use Hyperledger Indy, a dedicated network, Plenum and four applications

There are very limited public permissioned blockchains to choose from and since Hyperledger Indy is specifically build for digital self-sovereign identities this is momentarily the best choice. Indy has also been designed for scale and privacy (*C.7, C.12*). Hyperledger Composer can be used to make a network specific for humanID [84], this network will be small at first which brings some risks but will eventually grow making it more secure. The base of Hyperledger Indy is the Plenum protocol, which controls the ordering of blocks by Stewards and incentivizes good behavior (*C.19*). The consensus protocol is supposed to be plugable so others like Kafka or Solo could be used which offers flexibility [131]. During implementation another protocol might become more favorable but for now the Plenum protocol is suited best as it specifically developed for Hyperledger Indy. The application layer will consist out of three applications (*C.4, R7, R.8*):

1. IO Application: for the Identity Owner to register, access, update, revoke and disclose their identities, part of this application is an Identity Wallet

2. Identity Application: for organizations that function as attribute provider such as community representatives, humanitarian organizations, authorities and other people validating for humanitarian organizations
3. Service Application: to enable identity providers, attribute providers and service providers to perform their actions
4. Admin Application: for Trustees and Stewards to appoint other roles and direct nodes

Before using the IO Application, a Person Affected or Identity Owner must comply with the terms and conditions and provide consent (*R.6*). Furthermore, consent is given each time a service is requested by the identity owner itself. The Identity Wallet in the IO application allows the IO to hold multiple DIDs and credentials, which it visualizes.

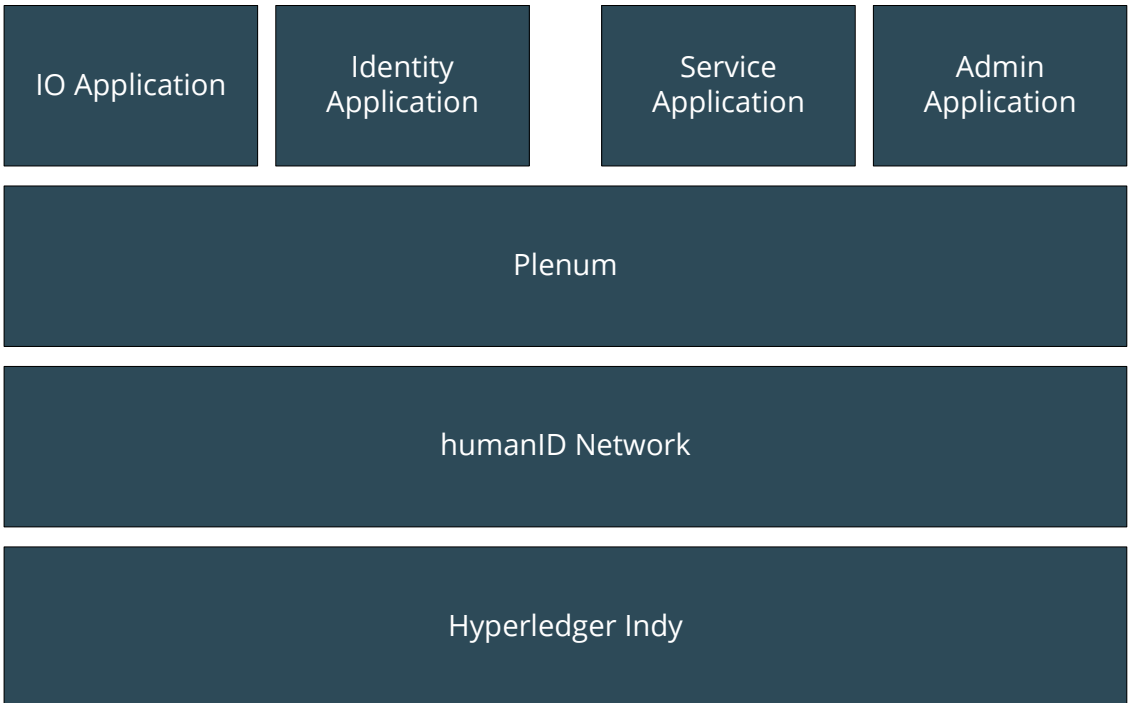



Figure 5.7: Layered blockchain architecture of humanID

### 5.4.5. Design Decision #5: Use the GPLv3 License

Sovrin and uPort use the Apache2 license which requires license and copyright notice and allow for commercial and private use [1]. Blockstack uses the GPLv3 license which is a strong copyleft license, where other organizations need to open up their source code and modifications. GPLv3 also mentions license and copyright notice, and can be used for commercial use and private use [1]. The idea of open sourcing here is that other organizations should be able to build on it and share what they have built open source too, in this case the GPLv3 license has the best match [78]. All these copyleft licenses allow for commercial use and this might not comply with the humanitarian principles. Thus for the moment the GPLv3 is used as an open source license as encourages a viral use, but a future humanitarian license might be a preferred choice (*C.13*). Other systems within the NLRC toolkit are also licensed under GPLv3, it could be enriched with a humanitarian clause directing it to be used only for humanitarian purposes.

### 5.4.6. Design Decision #6: Use Hyperledger roles and matching interfaces

Based on the program of requirements the following interfaces are needed:

- Trustees Interface linked to Admin Application

- Steward Interface linked to Admin Application
- User Interface for IO (*U.1*) linked to the IO Application
- Registration Interface for Identity providers, Attribute providers and Service providers (*I.10*) linked to the Identity and Service Application
- Validation Interface for Attribute providers (*I.4*) linked to the Identity and Service Application
- Service Interface for Service providers, at first only for Humanitarian Organizations (*T.2*) linked to the Service Applications
- Feedback Interface (*C.2*) linked to the IO Application

Similar set-ups of interfaces can be found in the NLRC and Sovrin system. There is no separate interface for registration by delegate, the difference is that in that case the user-interface is seen on a screen provided by the humanitarian organization and has an extra option stating that the validation is done by a delegate who has its own identity in the system, and has been granted responsibilities to do so. How such an interface will look and work best for illiterate, visually impaired people or other difficulties is out of scope but should be further researched. The feedback interface can be done by a service desk or as proposed by the NLRC using chatbots. uPort and Blockstack use an FAQ or forum to handle feedback, which is transparent. The conversations between the identity owner and a chatbot or service desk, might be private thus should not be instantly opened up. If the questions are more generic they could be put into a open FAQ. How this will work requires an community engagement approach, which should be further researched.

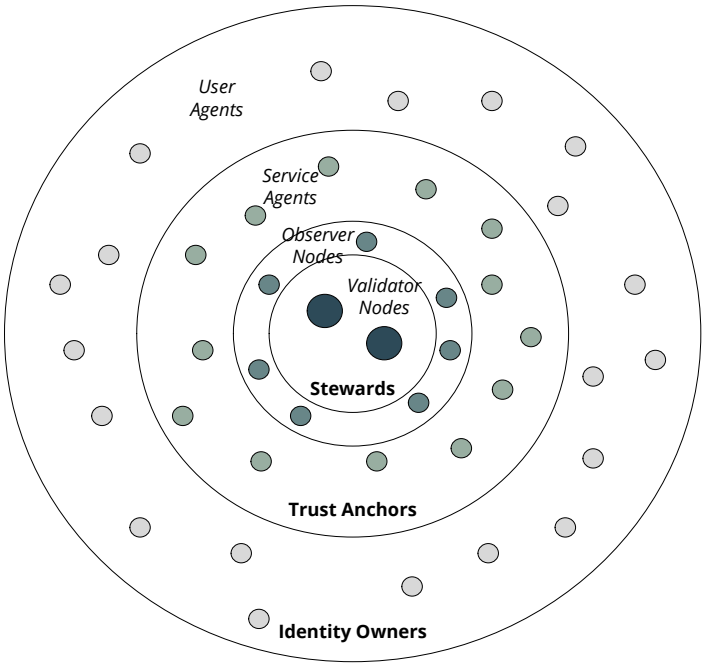



Figure 5.8: Roles in humanID based on Sovrin Foundation [137]

The roles that Hyperledger and Sovrin propose are similar to those in this system. In figure 5.8 it can be seen how these roles are related to each other. The following can be distinguished:

- Trustees, highest in rank and appoint Stewards
- Stewards, second highest in rank and appoint Trust Anchors
  - Validator Nodes, software which is run by Stewards and update the blockchain

  - Observer Nodes, software which is run by Stewards and provide reading access of the blockchain

- Trust Anchors, outside the blockchain and can be Identity Providers, Attribute providers or Service providers
  - Trust Anchor agents, software which can be designed and provided by anyone and allows the Trust Anchors to communicate, store data and perform operations
- Identity Owners, control their own identities and initiate all communication
  - User Agents, software which can be designed and provided by anyone and allows the Identity Owners to communicate, store data and perform operations

Who will be Trustees and Stewards will be decided upon later as it is part of the participation model, and also subject to a decision-making process and context of the CTP. For the remainder of this research it is displayed that all main roles can interact with each other directly without the use of agents or nodes.

### 5.4.7. Design Decision #7: Off-chain storage is to be determined by context

Local devices, IPFS, cloud storage are all possible alternatives to centralized storage. Local devices can be lost, but offer some space for safe and secure storage. An example is the Iphone that has separate secure enclaves for storing biometrics. IPFS aims for an internet where nothing can be lost, it remains unsure how the exact workings are for uPort and IPFS but it seems that storing private data on it might not be ideal if it is stored forever. Cloud storage was also mentioned, certain standards exist to make these very secure and although they can be rather centralized, distributed cloud storage also exists. Private keys could also be stored on Smartcards, that have a built-in microprocessor so it can initiate transactions. A normal card or paper could also store a private key, but similar to the Smartcard can be lost. As not everyone owns their own devices it seems that some kind of secure and encrypted cloud storage would be best suited if no device is available (*I.5*). With the Hyperledger Indy set up, it could be the agents that provide back-ups and safe storage of private information. This introduces some centrality, but it also introduces the business-model within this system [137]. Agencies could provide their services for a small payment, taking away efforts from Trust Anchors and Identity Owners. Introducing this revenue model might not be preferred since Identity Owners in a humanitarian context should not pay for these particular services as part of the CTP, but since humanitarian organizations might save money they could pay for these service. Nevertheless, it demonstrates that there are several options for offchain storage. To conclude, no final decision can be made on how to arrange storage off-chain. For now, the design will simply refer to off-chain storage for which several options exist. This is why *C.5* on safe storage for all participants is hard to fully comply with because it is context dependent.

### 5.4.8. Design Decision #8: Social, off-line and 2-factor authentication are used for key recovery

Blockstack offers the concept of a random twelve word key phrase. In a humanitarian context, this might be lost easily and is hard to remember. uPort and Sovrin both offer a social recovery of a key, by assigning trustees. If these trustees are also based in the disaster area, which is likely, then it will be difficult for them to generate a new key if they do not have access to a smart-phone or computer. The offline recovery Sovrin offers, has the drawback of also potentially being lost. Another option would be to have a two factor-authentication to regain access, combining a biometric identifier and a pass-phrase. This would be available on a phone but also at registration terminals. This does require for IO to submit biometric information at some point, which is possible by using Simprints[2] or in the future IDBox[3] as both do not require continuous internet connectivity. This identity should be self-sovereign, long-lasting and should serve digitized IO and IO that do not own any devices. As such, offline and social recovery are chosen but also two factor authentication using biometrics and a pass-phrase, is implemented (*U.4*).

[2] https://www.simprints.com/
[3] https://www.idbox.io/

### 5.4.9. Design Decision #9: Targeting is seen as a service not as a separate activity

One important result from the user-centred design that there is no separate targeting interface, but it is presented as service interface. This is done because the system is user centred and humanitarian organizations should thus not be privileged to connect directly or at default with identity owners. Yet, since many affected people will not have the means to register for a digital identity it is of importance that humanitarian organizations know where to provide assistance in this process. This is why a geolocation is requested (*R.3*) and put on a map to show coverage (*C.8*). For privacy matters, this geolocation should not be coupled publicly to the identity and preferably not even correlated, only service providers are allowed to see this map. This does result in an issue for targeting CTPs as these are location specific. So upon registration this location is entered at an aggregated level of for example province, encrypted, not connected to the identity and send to a central server. It will be stored as an identity attribute and it can be validated, but it leaves humanitarian organizations to find new means of letting people know they run a CTP for which they might be included. Initial contact can be made possible by offchain communication via the interfaces of users as a generic ”news feed” they can subscribe to per region, or to reach people that do not have a phone or device, local methods like social media, radio, community representatives or the like could be used.

From there on an identity owner could make a request for a service. Upon this request a service provider could send a request for specific identity attributes to be verified. The same applies for targeting. Based on the available identity attributes a set of inclusion criteria can be made which can be send out as a request to the identity owner (*T.1,T.4*). To ensure the highest form of privacy and objectivity, matching the criteria with the request attributes is done by an algorithm as proposed in the NLRC system. The result of this process is an inclusion score that is stored for the duration of the process and can be send back to the identity owner with a signature from the service provider (*T.7*). In this way the Identity Owner could use it for other purposes, for example to verify to a remittance company that he/she is entitled to the money that is disbursed via this organization.

### 5.4.10. Design Decision #10: Peer-validation, validation by attribute provider and by appointed validator

In the other systems peer validation is offered but only in the NLRC system a value of this process can be grasped as it results in a trust score. Peer validation is difficult because it requires a real-life connection between people to hold value. Yet, for future purposes peer validation might become handy as is exemplified by a system named BanQu[4]. They use peer validation to denote land ownership, ownership of machinery and the like, without the necessity of a central authority [152]. It is for this future purpose that peer validation is designed as part of the system. Since humanitarian organizations collaborate with volunteers or hired professionals for validation they must be able to assign these people to perform validation services for them. In all cases the Attribute Provider can validate the Identity Owners themselves and issue credentials.

## 5.5. Justification and Reflection of Design Decisions

By making the design decisions it is possible to map humanID to the program of requirements as can be seen in table 5.2, which allows for justification and reflection of the design decisions and answers sub-question *3.3. Do the proposed design decisions match with the program of requirements?* An overview of how humanID is compared to the other four systems can be found in appendix D.For each requirement is stated whether the design decisions satisfy the requirement and also in which decision this is decided. This offers full traceability from the system analysis to the program of requirements to the design decisions.

There are three important clarifications to be made. First, *R.1* specifies that only one digital identity may be available per Identity Owner and *R.5* states that the system should be checked for double entries. If the system is user-centred and uses DIDs then it is possible for people to register multiple identities, however their identities only hold value when they are validated. Validation will only take place if the attribute provider knows the identity of this person in the analogue world, so the assumption is that false identities will not be validated. To be clear, it remains possible to have double identities.

[4] http://www.banquapp.com/

Table 5.2: humanID mapped onto program of requirements

| ID | Requirement | humandID | Decision |
|---|---|---|---|
| R.1 | Each Person Affected shall be able to register for one digital identity as an Identity Owner | **No** | **2,3** |
| R.2 | Each Person Affected shall be able to self-register or register by delegate | **Yes** | **2** |
| R.3 | Each Person Affected should add a geo-location when registering | **Yes** | **6** |
| R.4 | System shall only request a maximum amount of identity attributes | **Yes** | **2** |
| R.5 | System should check for double identities | **No** | **3** |
| R.6 | Humanitarian Organizations shall ask Person Affected to provide consent for the use of data | **Yes** | **4** |
| R.7 | Only humanitarian Organizations shall be able to register as an attribute provider, identity provider and service provider | **Yes** | **2,4** |
| R.8 | Community Representatives and Authorities should be able to register as an attribute provider | **Yes** | **2,4** |
| R.9 | Humanitarian Organizations, Community Representatives and Authorities must have an humanitarian registration interface | **Yes** | **6** |
| R.10 | System must allow all humanitarian organizations to become part of it | **No** | **1,2** |
| I.1 | A Person Affected shall be able to have identity attributes validated by several attribute providers | **Yes** | **3** |
| I.2 | Attribute providers shall be able to validate identity attributes and geolocations | **Yes** | **3** |
| I.3 | Attribute providers shall be able to issue verifying credentials | **Yes** | **3** |
| I.4 | Attribute providers must have an easy to use validation interface | **Yes** | **6** |
| I.5 | Person Affected must always be able to access his/her credentials in a private storage | **Yes** | **7** |
| U.1 | Person Affected must have an easy to use user-interface | **Yes** | **6** |
| U.2 | A Person Affected shall be able to request services throughout the system | **Yes** | **3** |
| U.3 | Person Affected shall be able to safely access, update, disclose and revoke their identities | **Yes** | **1,3** |
| U.4 | Person Affected shall be able to regain access to their identity after loss of control or loss of access | **Yes** | **8** |
| T.1 | Humanitarian Organizations shall be able to match Person Affected with their inclusion criteria | **Yes** | **9** |
| T.2 | Humanitarian Organizations must have a service interface for targeting | **Yes** | **6** |
| T.3 | Humanitarian Organizations shall be able to verify identities based on issued credentials from other organizations | **Yes** | **1,3** |
| T.4 | Humanitarian Organizations must only be able to set up inclusion criteria based on minimum amount of identity attributes | **Yes** | **9** |
| T.7 | Humanitarian Organizations should delete all information that is no longer necessary for a CTP project | **Yes** | **9** |
| C.1 | The system must have roles for Identity Owners, Attribute Providers, Service Providers and Identity Providers | **Yes** | **2,6** |
| C.2 | A Person Affected should be able to provide feedback during use of the system | **Yes** | **5** |
| C.3 | System should be able to provide open response to the feedback of people | **Yes** | **2** |
| C.4 | Humanitarian Organizations shall be able to create sub-entities to pass down responsibilities | **Yes** | **2,4** |
| C.5 | All participants and the system must safely store all information | **No** | **1,2,7** |
| C.6 | System must provide secure end-to-end encryption for all communication and sharing of data | **Yes** | **3** |
| C.7 | System must provide the highest form of privacy feasible | **Yes** | **1,4,7** |
| C.8 | System should enable an overview of where people have been registered | **Yes** | **6** |
| C.9 | System must demand high data standards for all humanitarian organizations | **Yes** | **2** |
| C.10 | System must be inclusive and accessible for all humanitarian organizations | **No** | **1,2** |
| C.11 | System must be accessible at all times | **Yes** | **1,2** |
| C.12 | System must be flexible and able to scale up | **Yes** | **1,2,4** |
| C.13 | System must be open-source | **Yes** | **5** |
| C.14 | System must use interoperable standards for digital identification | **Yes** | **1** |
| C.15 | System must open up the governance structure online | **Yes** | **2** |
| C.16 | System must have a functional purpose and grow into a foundational purpose | **Yes** | **2** |
| C.17 | System must be accompanied by a participation model and process approach | **Yes** | **2** |
| C.18 | System must not have a single owner | **Yes** | **1** |
| C.19 | System must have an incentive system to demonstrate good behavior | **Yes** | **2.4** |
| C.20 | Actors in the system shall be able to communicate with each other if communication is initiated by the Identity Owner | **Yes** | **3,6** |

This has been a problem for the entire Internets lifetime and is nicely depicted in figure 5.9. On the internet you can be anyone, although this has slightly changed it remains possible to fake identities or acquire multiple. A solution has been sought in creating centralized institutions that provide certificates, which are called Trust Service Providers (TSP). Often, multiple TSPs are available which have been authorized by for example a nation state. This is what has been described previously as federated or a brokered architectural modal for digital identities, which is exactly what a self-sovereign system is trying to steer away from. Unfortunately, there is no solution within distributed architectures at the moment. Hajialikhani and Jahanara [72] propose to use a combination of biometrics, inconsistency-checking by peers and an incentive system that punishes malicious actors while rewarding honesty. They also claim to that throughout this process the users' privacy can be respected. Although this method is not waterproof as well, one could enter biometric data from someone else for example, some advancements have been made. However, an impervious system seems to be an impossible dream.

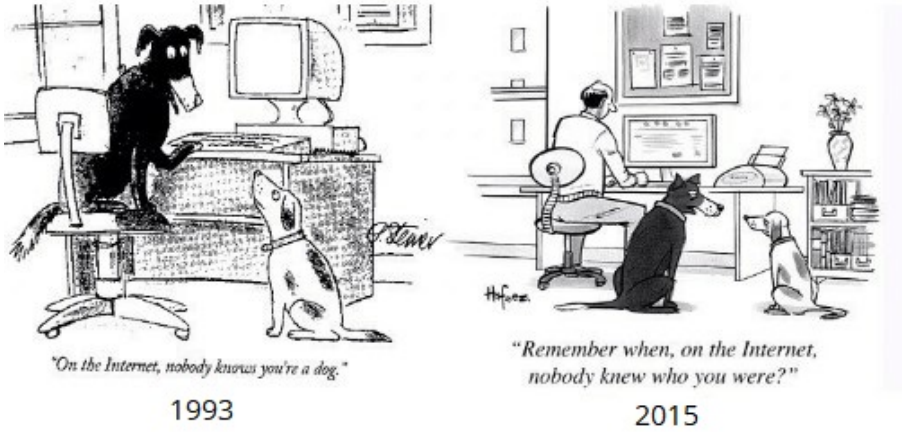



Figure 5.9: Identities on the Internet

Second, requirement *R.10* and *C.10* are not satisfied which is due to the decision for a permissioned chain. This is unfortunate but a result of the trade-off. All humanitarian organizations may join but need to be approved by Stewards, depending on what criteria these Stewards will use a decision on inclusion is made. One could make these criteria easily attainable by many humanitarian organizations but it will leave out some. Third, this design focuses on the user or identity owner and is functional from the start. The design proposes to only give humanitarian organizations the ability to be a service provider, but later the role of service provider could also be assigned to other organizations that provide services. In essence the whole system is designed to be foundational, but only used as functional thus barricading its full potential. This change in policy must be made by the Trustees and Stewards, but they may be more invested in the functional purpose.

## 5.6. Sub-Conclusion of System Design

*3.1. What alternatives are available for the design decisions?* was answered. Blockstack, Sovrin, the NLRC system and uPort fitted with being open source and blockchain based. These were analyzed on their functions, scalability, layers and roles. From their differences and similarities, ten design choices were derived. *3.2. Which alternatives best satisfy the program of requirements?* lead to a balanced choice for ten design decisions as can be seen in figure 7.1. *Do the proposed design decisions match with the program of requirements?* is answered by mapping the design decisions onto the program of requirements and it shows that on four requirements it does not satisfy. These have to do with two concepts: using DIDs and using a permissioned chain. It is assumed that the DIDs render the requirement for a unique identity and checking for doubles obsoleted, because it is not about the number of identities but about the ones that are validated. A permissioned chain interferes with a requirement stemming from humanitarian information management principles in that each organization should be able to join. Each organization could request to join, but in a permissioned chain their request could also be denied. To answer the full sub-question 3 *Which design decisions have to be made?* its

parts can be added up and results in a prescriptive set of design decisions, visually represented in figure 7.1.

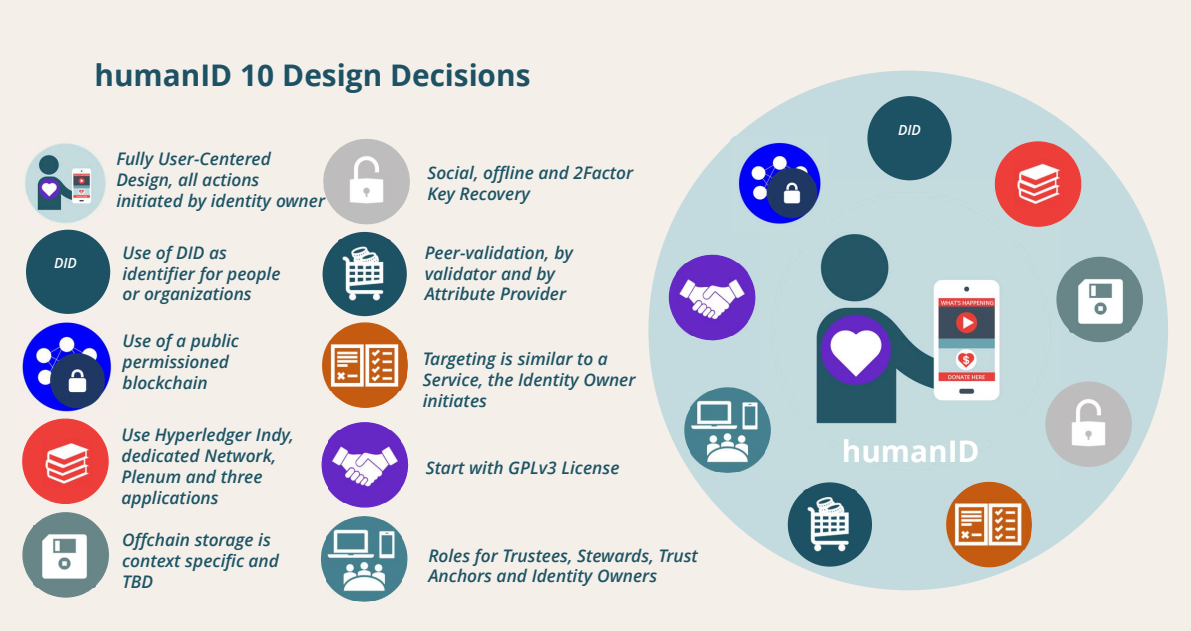



Figure 5.10: Design Decisions Version 1

# 6

# Demonstration & Validation

*"Better a diamond with a flaw than a pebble without"* - Unkown

In this chapter sub-question 4: *How can the design decisions be used in the an illustrative Cash Transfer Project?* and sub-question 5: *What is the value of the design decisions in a humanitarian context?* will be answered. Sub-question 4 is answered by a model validation that consists of a walk-through based on BPMN and UML models. The walk-through demonstrates how the design decisions can be interpreted in business process and object oriented models. These models are only depicted for the illustrative story of Alice, but can partly be generalized and used as a blueprint for future development. Sub-question 5 is answered by conducting an expert meeting in which the design decisions have been validated. An expert interview protocol was set-up and can be found in appendix E. Five experts have been approached with whom the set of design decisions were assessed. This results in various improvements upon the design decisions to better perform in the humanitarian context.

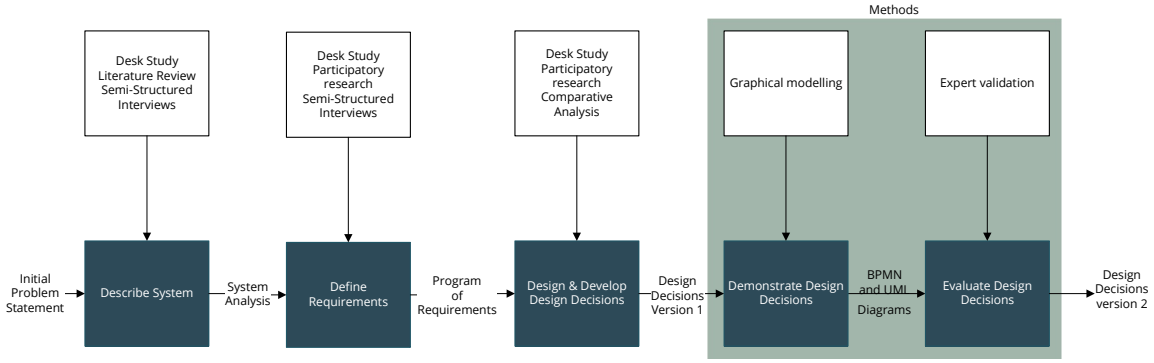



Figure 6.1: Methods for Demonstration and Validation

## 6.1. Demonstration

A demonstration is used to show how the design can solve the explicated problem [93]. A walk-through can combine a demonstration with a validation. Johannesson and Perjons [93] describe a walk-through as a form of peer-validation where the designer leads others through the artifact upon which comments can be given. In this research the walk-through has been organized as a form of model validation, so instead of taking peers through the design, it is the designer who validates the design decisions by creating a walk-through. The walk-through is both visualized and written out. The visualizations are build in Microsoft Visio using the *BPMN Basic Shapes* and *UML Class* formats. To set up these models it is important to understand how Hyperledger Indy works. Joosten [94], has analyzed a significant amount of information on Sovrin and Hyperledger Indy and came to the conclusion that there is much ambiguity in terminology but also in its workings. The source that has

the most up-to-date information on Hyperledger Indy is its Github[1], which was partly used to draw up the BPMN models. The BPMN models lead to insights in the business processes and should be made understandable for each stakeholder, therefore many of the technical workings are left out. To transform the design decisions, they have to be perceived as a collection of interrelated activities which are performed as a response to a trigger and aim for a specific result. The UML Class model can be made on the basis of these BPMN models and demonstrate how the software could actually be designed if it is programmed in a object oriented approach. For this walk-through the following fictional case is used:

> Alice has been living in rural flood-risk area, she knows that floods are coming and has heard that her local Red Cross (RC) branch might be giving out CTP support. To be included she needs to prove that she is eligible. She gets notified by the community leaders that people can register online for a digital identity to see if she can be included for a CTP. Alice owns a smart-phone and can travel to a place with a good internet connection. In her residential area, a local volunteer named Bob works for Oxfam Novib and assists in validation. Care International is also active in the network and performs the role of identity provider.

This storyline assumes that the network is already set up and Trustees and Stewards have been chosen.

### 6.1.1. A Dynamic Representation

#### Step 0: Communication, DID verification, setting up Requests

There are three processes that are repeatedly used and would decrease understanding of the business process if continually depicted in full. Therefore in this step the processes are visualized so that in other BPMN diagrams they can be used as ”collapsed sub-processes” which are squared activity boxes denoted with a + in the bottom. To begin, in decision #1 it was introduced that asymmetric key-pairs are used for communication. This ensures that each outgoing message, request or form is encrypted and decrypted by the receiver. The process is depicted in figure 6.2.

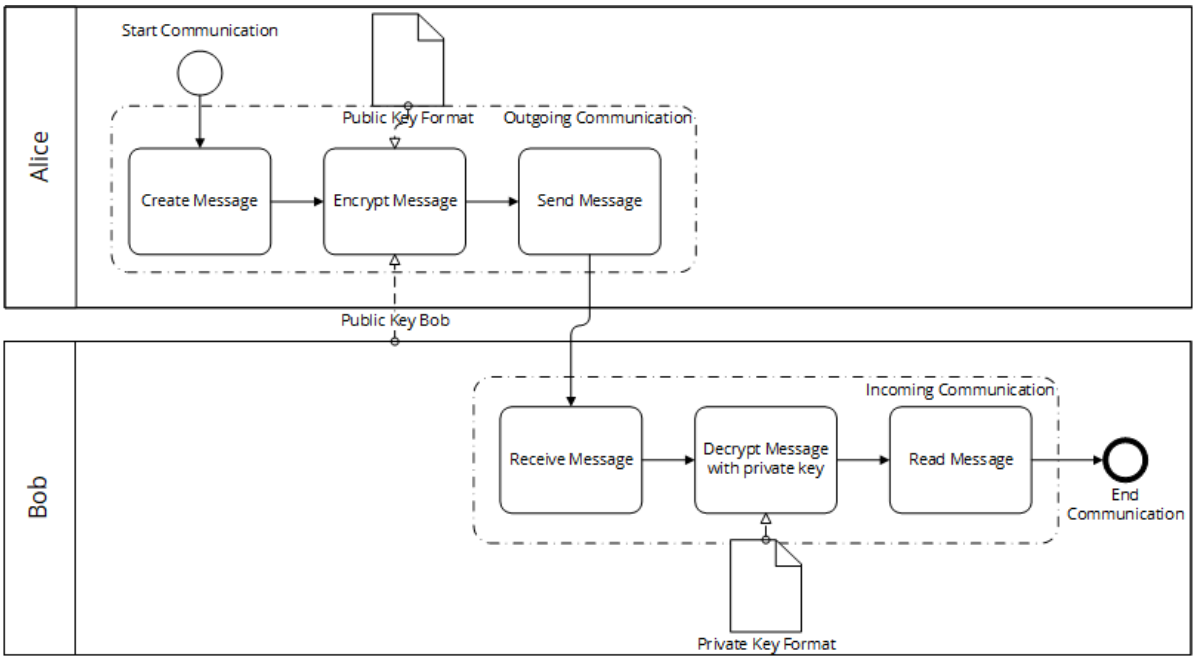



Figure 6.2: BPMN Model of Asymmetric Encryption

For the example Alice and Bob are used. Alice creates a message of sorts and encrypts this with the public key of Bob. This public key could have been sent by Bob or she could have retrieved it from the blockchain. Alice sends the message and Bob receives it. Since his public key is used to encrypt

[1] https://github.com/hyperledger/indy-node/blob/master/docs/transactions.md

it, Bob can use his matching private key to decrypt and read the message. Hence, the private key is important and should be stored very securely.

Another process that occurs frequently is the verification of DIDs. DIDs are pairwise pseudonymous, so once a DID is made and connected to both sides they should be able to check if the DID indeed belongs to their counterpart. The DID holds information on how to connect to the counterpart. This process is shown in figure 6.3, where Alice verifies the DID from Bob. Since DIDs are published on the blockchain she can check the DID and receive the DDO which holds information on how to connect with Bob and his public keys. She can than connect with Bob knowing that the DID indeed belongs to him and Bob is verified.

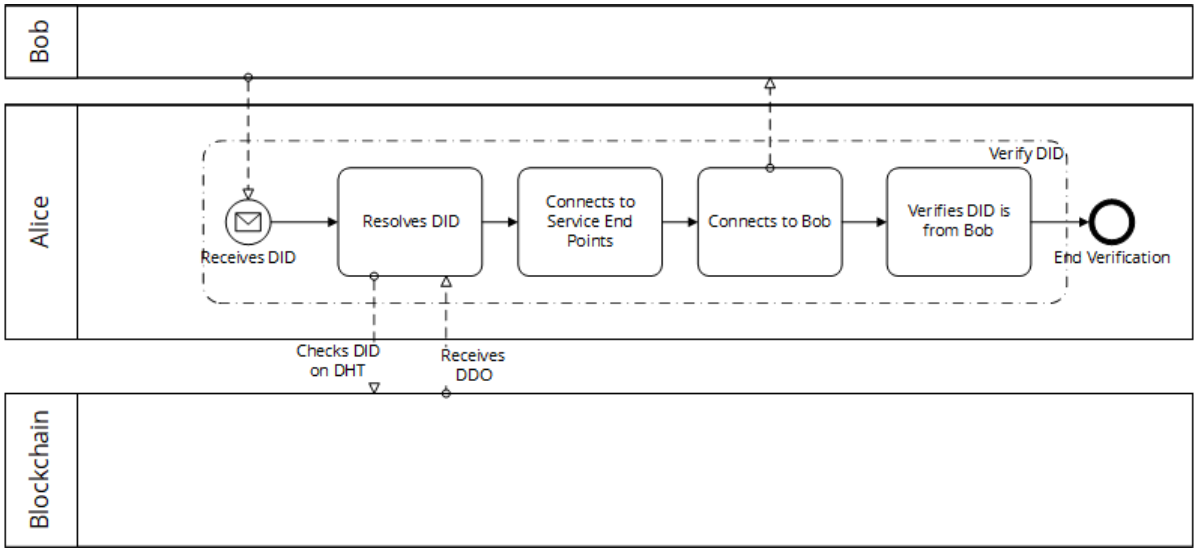



Figure 6.3: BPMN Model of DID Verification

A last process that is used throughout the system is setting up requests which can be used for the validation process in which the request consists of request form, in the service process in which the request consists of a service form or in the registration process where it consists of a registration form. Each of these forms require the counterpart to fill in information such as credentials, identity attributes or the like. In this figure 6.4 Alice is the identity owner and since the system is user-centered it is always Alice that initiates the request. The following activities are described in this process:

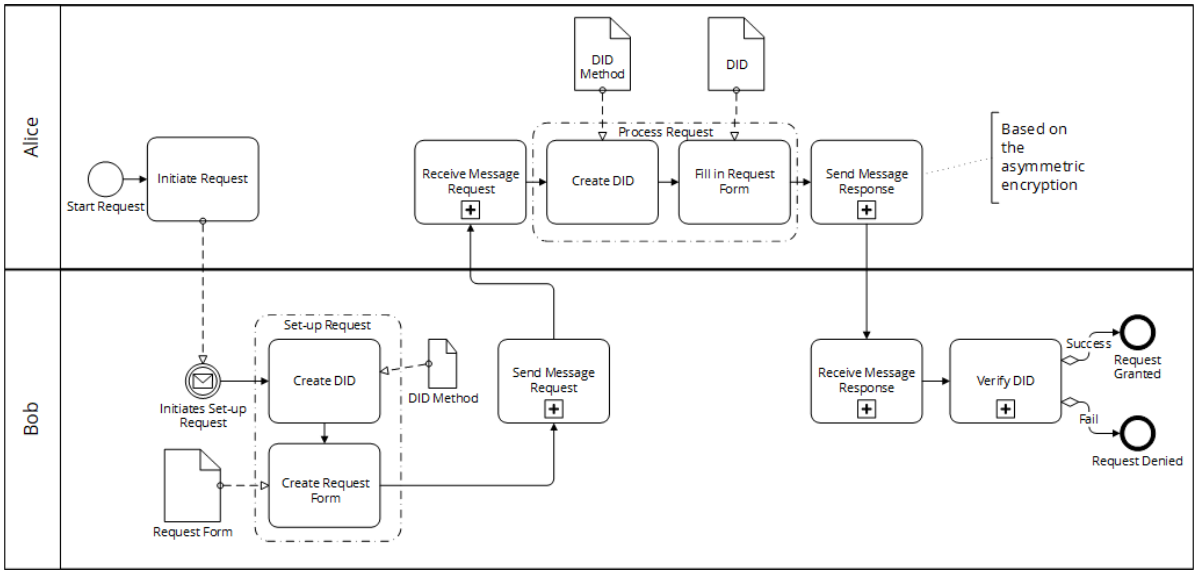



Figure 6.4: BPMN Model of setting up and processing requests

1. Alice initiates the request
2. Bob receives Alice her message and sets up the request
3. Bob creates a DID based on the DID method which applies to all DIDs
4. Bob creates the request form which can serve various purposes
5. Bob sends a message with the request
6. Alice receives this message
7. Alice creates a DID based on the DID method and fills in the form attaching her DID, this is called processing the request
8. Alice sends the response
9. Bob receives this response and verifies the DID
10. If DID is correct than request is granted otherwise it is denied

These processes have introduced how communication is secured, how DIDs can be verified to ensure that identities are belonging to the ones that claim them and how request are set up and processed.

### Step 1: The Red Cross, Care and Oxfam Novib need to become Trust Anchors

At the start, the Red Cross (RC), Care and Oxfam have to become Trust Anchors and connect to a Steward. The process is displayed in figure 6.5 and describes the following activities:

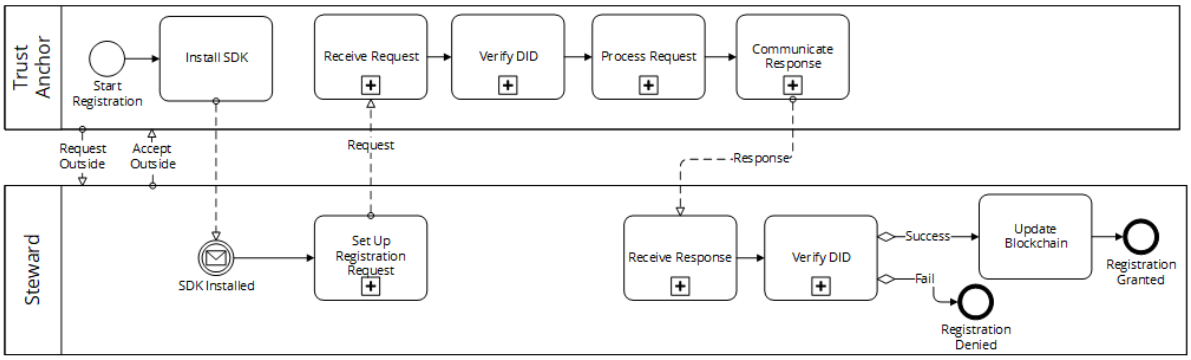



Figure 6.5: BPMN Model of registration of Red Cross, Care and Oxfam based on Hyperledger [86]

1. RC, Oxfam and Care have approached a Steward outside the system because they want to become Trust Anchors (TA), this initiates the process
2. They install the SDK relevant to them
3. Steward receives notice that the SDKs have been installed and set-ups a registration request
4. RC, Oxfam and Care receive their requests and verify the DID of the Steward which is publicly available on the blockchain
5. RC, Oxfam and Care process the request and communicate their response
6. Steward receives the response and verifies the DIDs
7. Verification is successful then the Steward updates the blockchain with the Public Addresses of the Trust Anchors so that like the Steward they can always be found and the registration is granted
8. Verification is unsuccessful, then the registration is denied

The Red Cross in this case has downloaded the SDK for the Service Application, while Care and Oxfam have downloaded the SDK For Identity Applications. As there is a public verification of the TA on the blockchain they can now be found, this shall not be the case when identity owners register.

### Step 2: Alice registers and Care provides a registration

To be clear, in this example Care is the identity provider, yet this could also have been Oxfam since they are both TAs with Identity applications. Before Alice can become a digital identity owner she needs to download the mobile application for her smart-phone. Alice goes to a place with internet connectivity and downloads the app, she then proceeds to take the steps depicted in figure 6.6 and described in the following steps:

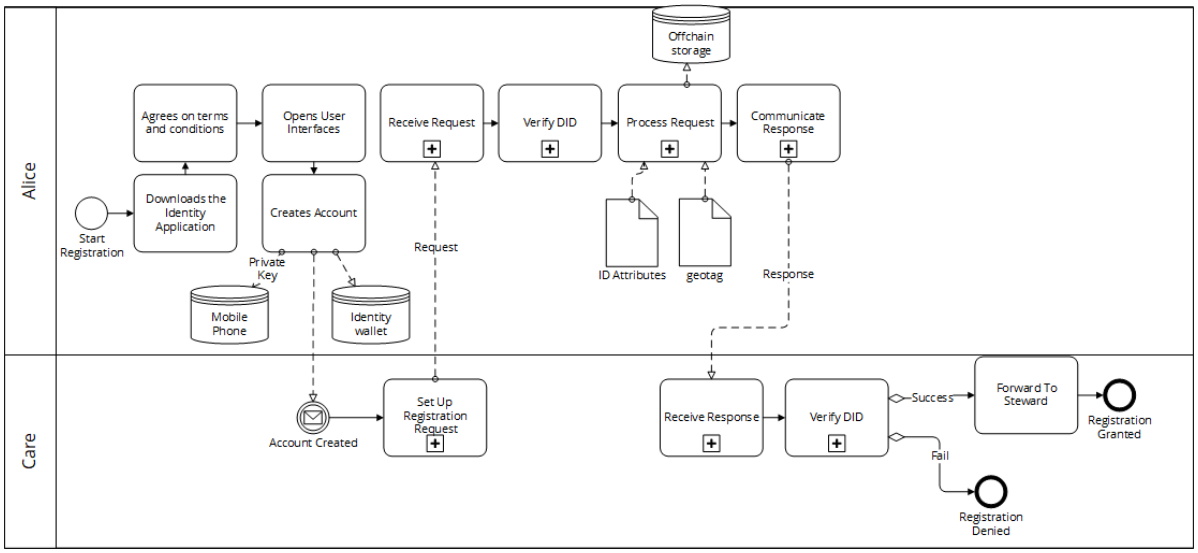



Figure 6.6: BPMN Model of Alice registering at Care partly based on Hyperledger [86]

1. Alice downloads the mobile application for and agrees on the terms and conditions, which are either written or in audio-format preferably in her native language

2. She opens the user interface and creates an account, which has an identity wallet storage and stores a private key, for Alice this is on her phone for others this could be on a paper-card

3. Care receives a message that Alice wants to create an account and sets up a request for registration

4. Alice receives the request and verifies the DID of the Care to ensure she is dealing with a trusting organization

5. Alice processes the request and adds ID attributes and a geo-tag, which are stored in an offchain storage

6. Alice communicates her response

7. Care receives the response and verifies Alice her DID

8. If successful Care forwards the registration to the Steward who then updates the blockchain, the registration is granted

9. If unsuccessful the registration is denied

Alice is now registered and has stored some self-attested claims about her identity attributes in an off-chain storage. She has a private key for access and to sign with and an identity wallet in which she can have an overview of all her DIDs.

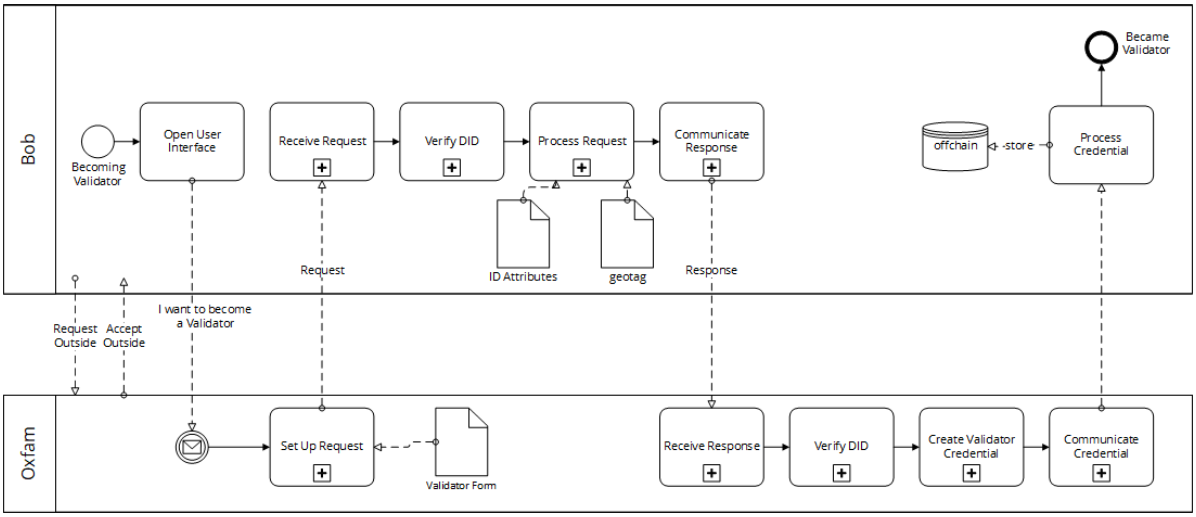



Figure 6.7: BPMN Model of Bob getting a Validator Credential from Oxfam

### Step 3: Bob needs to become a Validator

Oxfam collaborates with multiple validators throughout their CTP programs. In the area where Alice is living, Bob is their validator for the time being. Bob has also registered a digital identity just like Alice and is now looking for a public credential from Oxfam so he can show Alice that he indeed works for Oxfam. The process is displayed in figure 6.7 and described in the following activities:

1. Bob and Oxfam have been in touch outside the system and agreed that Bob will work for them
2. Bob opens the user interface and sends a message to Oxfam whose public address can be found on the blockchain
3. Oxfam sets up a request using a validator form which requires Bob to fill in some attributes
4. Bob receives the request and verifies the DID from Oxfam
5. Bob processes the request and communicates his response
6. Oxfam receives the response and verifies the DID
7. Oxfam creates the validator credential and communicates this to Bob
8. Bob processes the credential and stores it offchain with his other credentials
9. Bob is now a validator

This process is the same in essence as when Alice wants to receive credentials. In the overview the activity ”Create Validator Credential” is depicted as a collapsed sub-process. In figure 6.8 this process is displayed. It lays out that after verification of the DID, the identity attributes that are requested to be validated are checked on the basis of a field validation and other existing data. Please note, the identity owner does not send out his or her own credentials it only points to which attributes he or she wants to have validated. The credential is then build and signed. A public facing signature is published on the blockchain so others know who has signed it, while the private facing credential is send to the identity owner.

Now Bob has become a validator and can show Alice that he has been vouched for by Oxfam. The process where Bob validates Alice her identity attributes and issues credentials can be seen in figure 6.9. This process is very similar to how Bob received his credentials but with the following differences. First, Bob and Alice did not have any communication previously. So Alice must somehow know that Bob is validating in that area, this has not been covered by the design so far. However Bob can be found via Oxfam and its public address linking to Bob. Second, Alice can decide whether she trusts Bob his credentials signed by Oxfam by verifying the public key signature on Bob his credential. Lastly, authentication of Alice her attributes takes place in real-life. Bob might have access to some existing data, or asks and looks around.

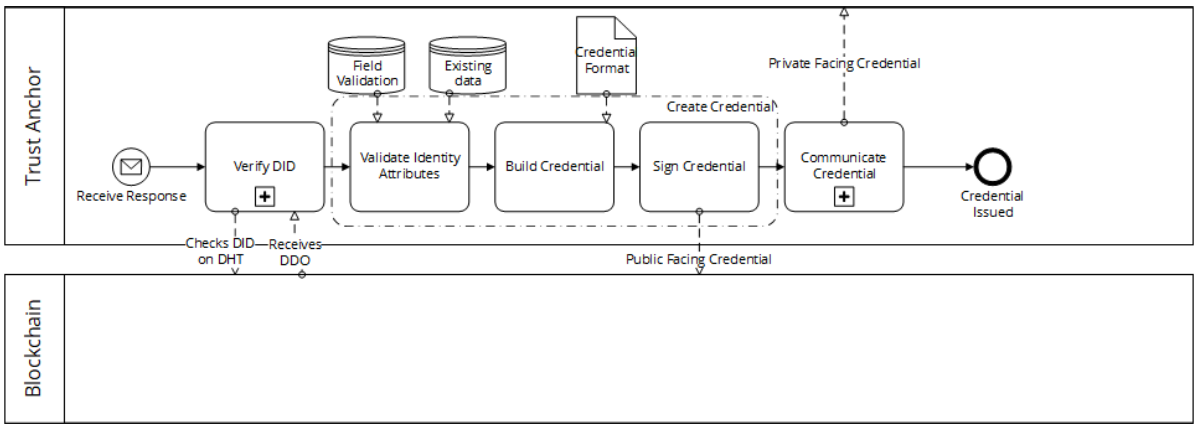



Figure 6.8: BPMN Model of creating Credentials

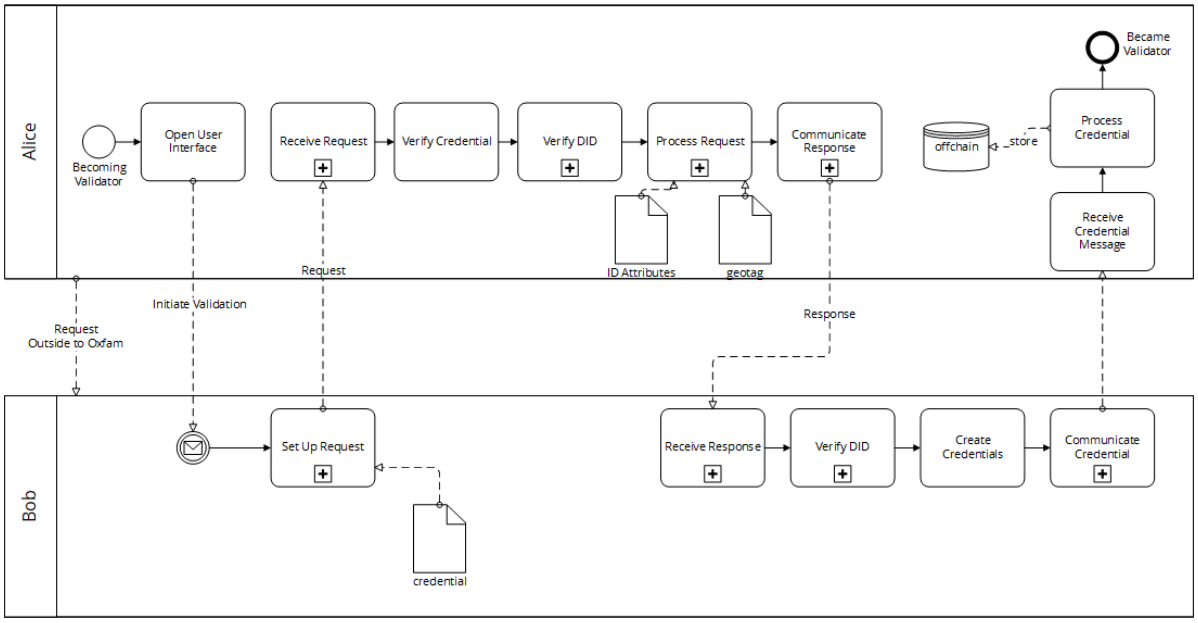



Figure 6.9: BPMN Model of Bob validating Alice

### Step 4: Alice Requests a Red Cross CTP Service

Alice hears about the RC setting up a CTP that she might be eligible for. The RC has broadcasted the inclusion criteria via her community representatives and Alice saw it in the newsfeed in her user-interface that she subscribed to. Alice wants to apply for the service. In figure 6.10 an overview of the process is given. The following activities are spread out:

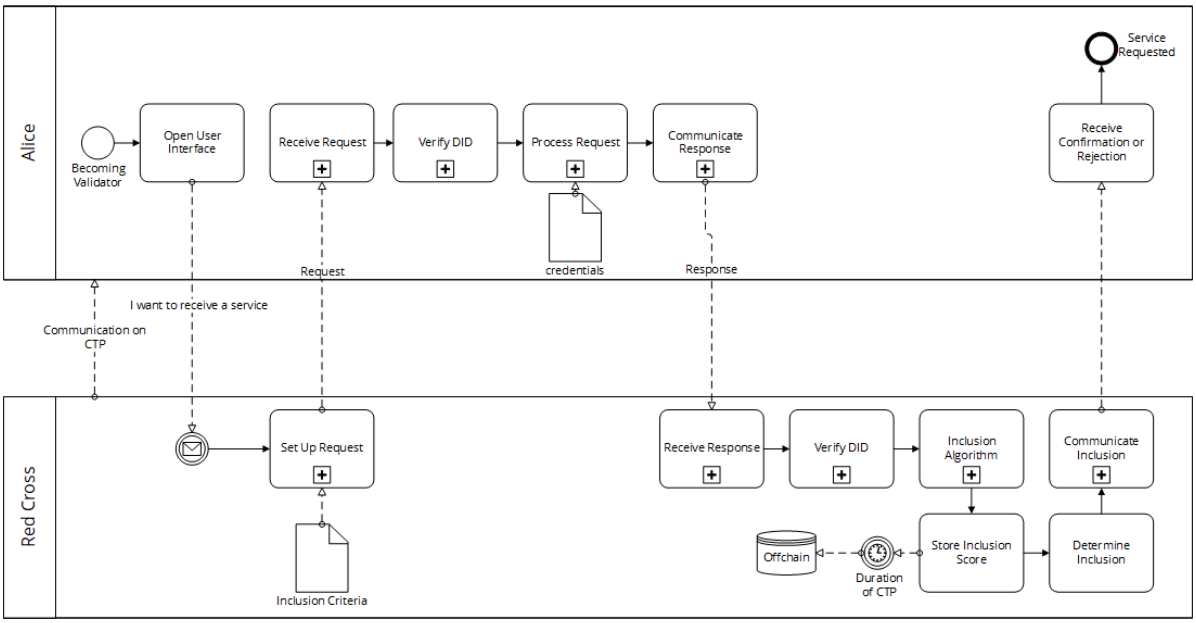



Figure 6.10: BPMN Model of Alice requesting a service from the Red Cross

1. Alice opens her user interface and sends a message to the Red Cross who can be found due to their public address
2. Red Cross creates a request which includes the criteria
3. Alice receives this request and verifies the DID of the Red Cross
4. Alice process the request and submits her credentials, if she does not have any she can submit her self-attested attributes
5. Alice communicates the response to the Red Cross
6. Red Cross receives the response and verifies the DID
7. Red Cross includes the credentials into the inclusion algorithm which spits out an inclusion score
8. The inclusion score is stored for the duration of the CTP
9. Red Cross determines if score is above the threshold abd if Alice is included
10. Red Cross communicates the result
11. Alice receives the result and knows if she is included
12. The service request is finished

The inclusion algorithm is also a collapsed sub-process and entails the activities such as decrypting the message, verifying the credentials and determining a score per credential or self-attested claim. These scores are added up and constitute an inclusion score, if the score is above the threshold set for the CTP an identity owner can be included. In this way the Red Cross does not have to store the credentials ensuring data minimization. To be clear, services are at first only offered via the Service Application for humanitarian organizations. In the future other organizations could also receive this role.

### Step 5: Alice maintains her Identity

Alice lost her private key and wants to renew her access. As described in the design decisions, three methods are offered for her to recover her access. In figure 6.11 the process of key recovery is presented. Alice has already appointed trusted peers with which she has a DID for communication, also the assumption is that Alice has lost control over her account but still has access to a phone. In case she does not have access to a mobile device, she goes to a registration terminal and at the end receives a new paper-based key. The process steps are as follows:

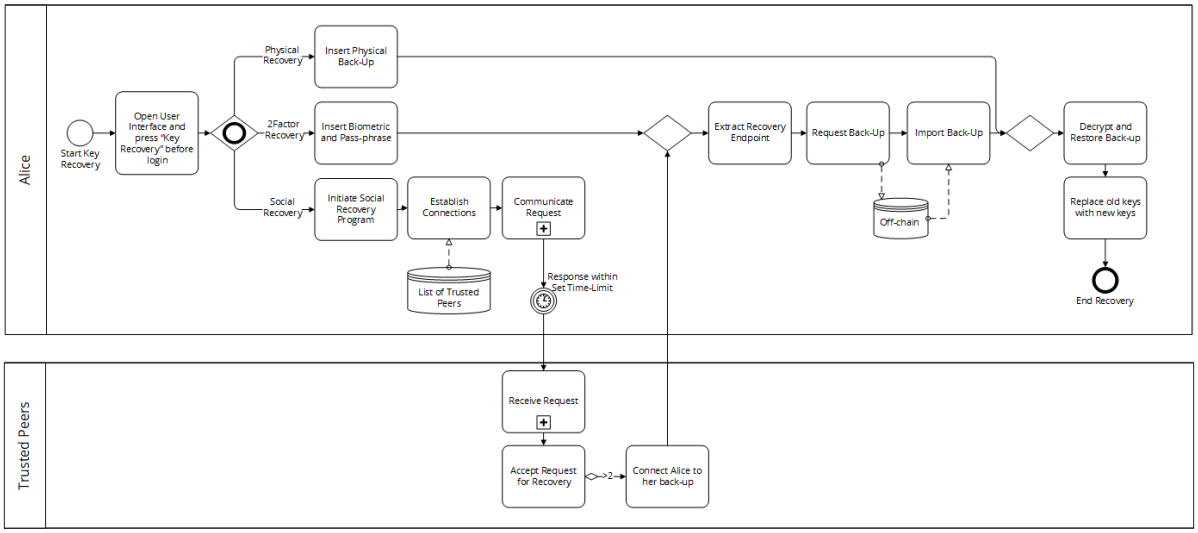



Figure 6.11: BPMN Model of Alice recovering her key based on Hyperledger [85]

1. Alice accesses the user interface and clicks the button ”key recovery” and three options appear:
   - Physical Recovery
   - 2Factor Recovery
   - Social Recovery
2. Alice picks Social Recovery and the chosen Trusted Peers are sent a request containing the DID
3. Trusted peers receive the request and after more than 2 accept, they connect Alice to her back-up
4. Application extracts the recovery endpoints so it can request a back-up that is stored off-chain
5. Application receives the back-up and decrypts and restores it
6. The old keys are replaced with new keys

Alice might also want to revoke access or communication with the Red Cross after she has received her cash-based assistance. Or she might want to update her identity attributes. According to Hyperledger Indy [85] there are two ways of doing so. First, Alice might have set a time-boundary on how long the DID is valid, in that case an automatic key rotation can take place when the end-date has passed. Second, Alice might want to delete the entire connection. The second option is depicted in the figure 6.12. Where Alice opens her Identity Wallet and revokes the DID. The blockchain needs to be updated afterwards and Alice could send a message about it to the Red Cross but she does not have to.

Key rotation would be more fitting in this scenario for Bob from Oxfam. Lets say that Bob has decided that the credential he has given is only valid for one year and then needs renewal. In that case it would not be necessary to delete the connection, but the keys are rotated so that for the time being the credential is not valid. Alice would than need to request a renewal. The same goes for when Alice wants to update her identity attributes. She could simply do this in the IO Application that she access to, but it would require to renew her credential for that specific attribute.

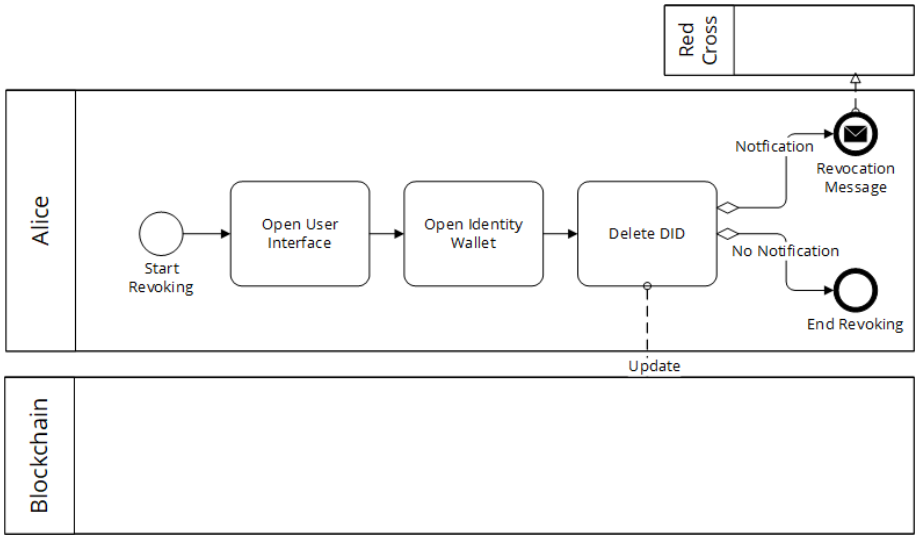



Figure 6.12: BPMN Model of Alice revoking her DID by deleting it based on Hyperledger [85]

### 6.1.2. A Static Representation

Based on these BPMN models several classes can be distinguished that need to exist if this system is developed. An overview of the UML diagram is presented in figure 6.13. UML Class diagrams can be even more detailed but for the purpose of model validation this suffices. This diagram has also been validated by a former technology consultant with a background in computer science.

In this diagram two different relations are shown, associations and inheritance. Associations are displayed with multiplicity, which defines how many instances of the one exists in relation to the other. For example, the Identity provider can provide identities for zero or more identity owners, but each identity owner only has one identity provider. Parent classes are denoted by a line with an open arrow head, for example a trusted peer which is needed for key recovery is a child class of IdentityOwner. This means that it inherits all of the public attributes and methods of the parent class, public means they are preceded by a + as opposed to private which are preceded by a - [21]. With an association relation this is different is the same.

What becomes clear in this diagram is that Stewards and IdentityOwners are the two main classes, which can also be seen by the amount of methods or operations they have in the lower block of each class. These methods describe how a class interacts with data, in other words what kind of operations they can do [105]. The middle block of each class describes the qualities of the class or the attributes, these can be attached to an instance of the class. So an instance of a mobile application must have a device it is on. Likewise an instance of an identity owner must have a DID, identity wallet, login, account, identity attributes, geotag, credentials and a list of trusted peers.

#### Stewards

This UML diagram shows that Stewards are a parent class with TrustAnchors as a child-class, since ”all Stewards are automatically Trust Anchors” Hyperledger [86]. Stewards have contact with DID which are stored on the blockchain, so for simplification only the class DID is depicted. The TrustAnchor class is a parent itself, which inherits three child classes: ServiceProvider, AttributeProvider and IdentityProvider. They have inherited all public attributes and operations of the Stewards and TrustAnchor classes.

#### IdentityOwner

IdentityOwner has interaction with each childclass of TrustAnchor. The IdentityProvider class is interacted with for registration, the validation process takes place with the AttributeProvider and the ServiceProvider is interacted with for requesting a service. While the IdentityOwner might only interact with one IdentityProvider, it can interact with zero or more instances of the ServiceProvider and AttributeProvider class. This simulates that an identity owner can have multiple credentials from various sources and request multiple services.

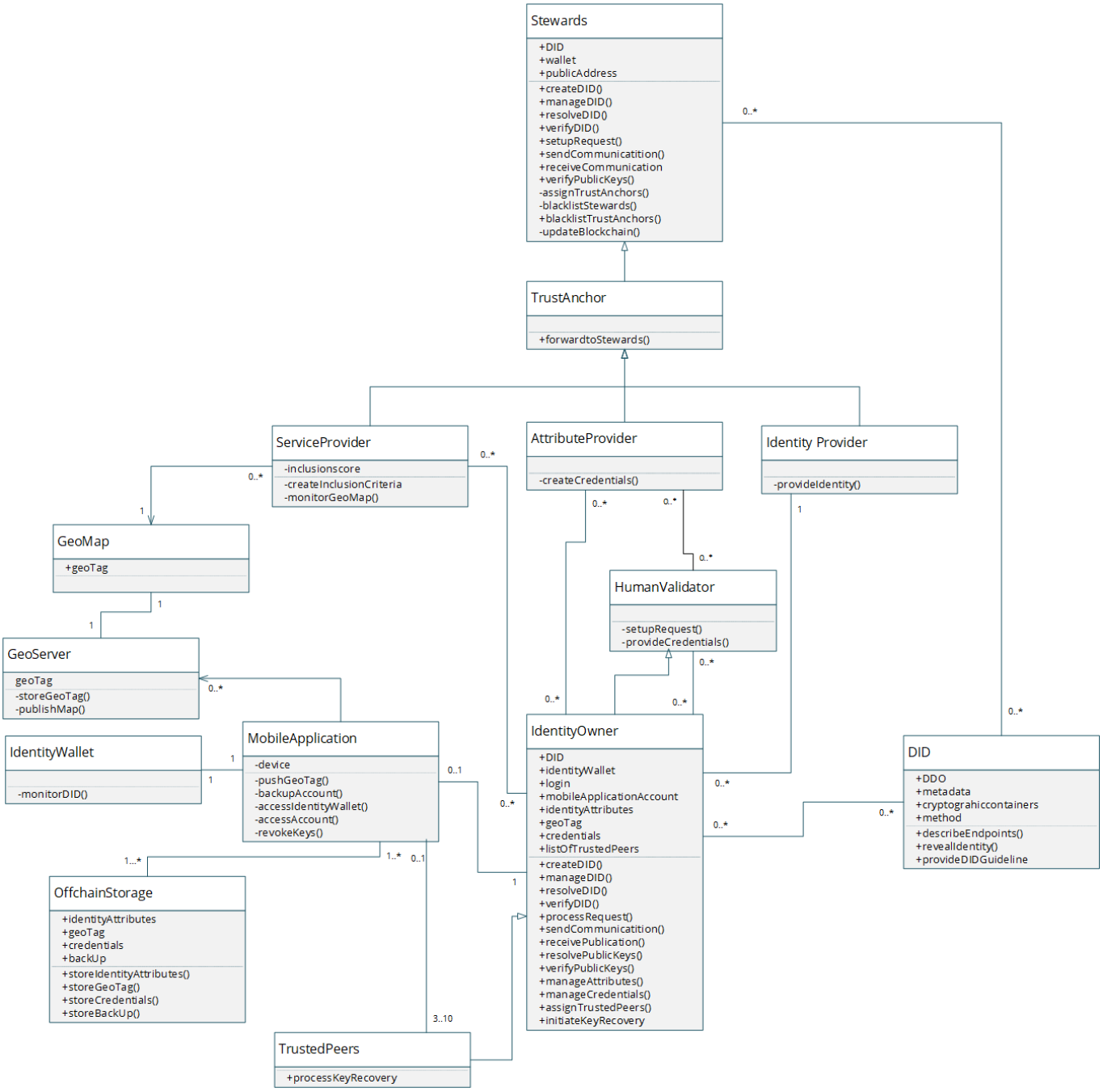



Figure 6.13: UML Class diagram based on business processes

#### MobileApplication

MobileApplication class interacts with the IdentityWallet of which it has one instance and is used to monitor the DIDs. The MobileApplication also interacts with OffchainStorage, where it stores attributes, credentials, geotags and back-ups of the application. An IdentityOwner class uses one MobileApplication in this illustrative case study this is via her smart-phone, Alice must login to get access to the application. MobileApplication also interacts with IdentityOwner to ask for acceptance of the terms and conditions. IdentityOwner uses MobileApplicaiton to assign TrustedPeers, for key recovery. Lastly, the MobileApplication can push aggregated and anonymized geotags to a geo-server.

#### GeoServer

The GeoServer receives and stores geo-tags from the MobileApplication class, but this direction is unidirectional so it can not retrieve any other information. The GeoServer interacts with a GeoMap which is available and monitored only by ServiceProviders. At this moment these are the only actors that are always humanitarian and they can use this map to see where more promotion for the system is necessary and where more validators are needed.

### 6.1.3. Realizations from model validation

The model validation resulted in several realizations for the design decisions that have been made which can be summed up:

- *Design Decision #2*: The decision for a permissioned chain complicates the registration procedure significantly as opposed to a permissionless chain. This will slow down implementation and has to be taken into consideration.
- *Design Decision #6*: First time registration requires only one Steward, yet updating the blockchain and performing consensus requires more than one Steward to keep it legitimate. A minimum number of Stewards should be assigned before launching the system.
- *Design Decision #6*: An appointed validator will need a special interface, which can be accessed via the user interface
- *Design Decision #9*: This system does not depict how the inclusion score and DID are attached and how these can be dereferenced
- *Design Decision #9*: All service providers must have a list of organizations they trust to establish inclusion scores because credentials are judged on who they are signed by, this is not mentioned by the design decisions
- *Design Decision #9*: The system for geo-tags will only work as long as only humanitarian organizations are service providers
- *Design Decision #10*: This system depicts Bob both as an Identity Owner and as an extension of an Attribute Provider, the latter can be publicly be found while the former should be hidden, this is structurally incorrect
- *Design Decision #10*: In this design the highest value is for validated attributes and self-attested attributes will result in low trust scores. It has not been taken into account that self-attested attributes have a different format than credentials, while they should also enter the inclusion algorithm. In a humanitarian context it is likely that many people will only have self-attested attributes so a solution is necessary.
- *Design Decision #10*: In this design attribute providers give credentials for unlimited time while this might not be preferable, attribute providers should also be able to rotate their keys so that credentials have to be revalidated if necessary or so that appointed validators like Bob have to put in a new request to become a validator.

These points shall be integrated in the iteration of design decisions in paragraph 6.5.

## 6.2. Expert Validation of Design Decisions

The goal of this expert validation is twofold. First, to retrieve new knowledge as described by Meuser and Nagel [109], since the use of blockchain and digital identity systems is a novel concept and this research has an exploring the abilities of its bundled capacities. Second, it is used to provide feedback on the design decisions in order to refine them. Verschuren and Hartog [155] would state this to be a "plan evaluation", where the quality of the design is assessed before a design is actually being developed.

Experts were either chosen for their experience within digital identity management and/or blockchain for a technical validation or for their experience in digitizing humanitarian assistance. It would have been preferred to interview experts knowledgeable in both fields, unfortunately these were not available. In the table E.1 the experts that were interviewed are listed.

| Name | Organization | Background | Validation |
|---|---|---|---|
| Djuri Baars | Blockchain Lead at Rabobank | Self-sovereign identities and Blockchain | Technical, Blockchain Architecture |
| Arnold Daniels | Co-founder at Legalthings | RegTech and Blockchain | Technical, Blockchain Architecture |
| Sander Dijkhuis | Product Owner at Cleverbase | Trust Service Providers, Digital Certification | Technical, Identity System |
| Vincent Graf | ICT Innovation Officer at ICRC | Digital Humanitarian Aid | Humanitarian Practices |
| Maarten van der Veen | Visionary Lead at 510 | Digital Humanitarian Aid | Humanitarian Practices |

Table 6.1: Overview of Expert Interviews

All interviews were conducted face-to-face and in Dutch, with the exception of a skype interview in English with Vincent Graf. Each of the audio files is available upon request and each interview is summarized in appendix E. For these interviews a protocol was set up which is available in the same appendix. As experts had different backgrounds specific questions were also prepared and asked.

### 6.2.1. Assessment of Design Decisions

The expert feedback can be categorized per design decisions, with an additional category for overall feedback. Within the next sections each of the interviewees is denoted by their `surname`.

#### #1: Use of blockchain technology

According to `van der Veen`, blockchain has an important role in digital identity systems since it enables self-sovereignty and in his experience distributed systems are more likely to offer stability. The experts are critical on the use of blockchain but do see opportunity in this use-case. `Baars` mentions that blockchain is a valid choice for self-sovereign identity but warns that there are existing blockchains that have the same use-case and with whom can be collaborated with in order to reduces inefficiencies (energy consumption, costs and time needed for mining) encountered when adding yet another blockchain to the list. This notion is added as a limitation to the design choice.

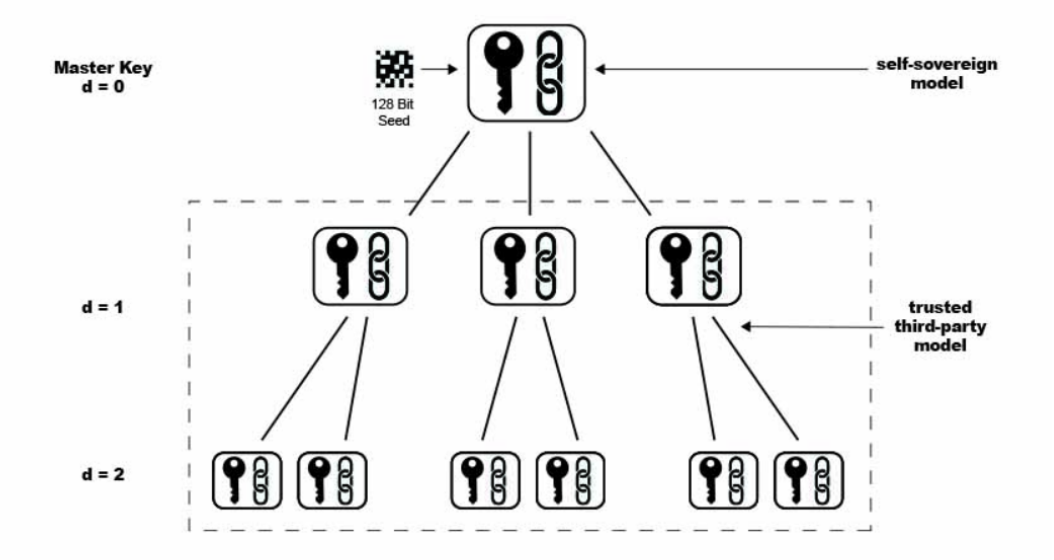
#### #2: Use a public permissioned blockchain

`Daniels` and `Baars` both stated that for a pure self-sovereign system only a public permissionless chain could be used and both understood the trade-off for a permissioned chain. However, permissionless chain would offer more security and transparency. Roles could be assigned in a similar fashion with all trust encoded. Not choosing a permissionless chain therefore introduces a governance problem, trust should also be managed outside the system. As `Dijkhuis` explains, you would need a framework to express trust among Trustees and Stewards and translate this to the outside world to counter the opportunities it creates for fraud and corruption. `Graf` states it is the "least bad way", he does not directly recognize that the humanitarian sector would be more likely to adapt a permissioned system. Nonetheless, it is agreed upon that a permissioned chain creates a barrier to join and with that a buy-in the development of the system. There will be no changes to this design decision based on the expert validation.

#### #3: Use DIDs and a fully User-centred Design

Once again, a pure self-sovereign system should incorporate a fully user-centred design. Deciding to go for DIDs should be evaluated against its need according to `Daniels`. He introduces the concept

of Zooko's Triangle which describes trade-offs when giving names or identifiers to participants in a network. They can be secure, decentralized and human-meaningful, pick any two [121]. DIDs are not human-meaningful, which in some cases might be preferable, however the W3C sees many solutions to this problem [156]. These solutions should consider the numerous attempts to retrieve personal information and the potential for global correlations based on human-readable identifiers. Baars recognizes the potential for DIDs now that they have been put into a standard even naming them the new "Rolodex for identities". Baars also mentions that preferably in a user-centred design multi-show unlinkability would be used. He presents a tool named Hierarchical Deterministic Key Pairs which work with master, child and grandchild keys, and can only be traced form old to young [128]. This one-way traceability enables the unlinkability if for each interaction a different grandchild key is used.




**1.1 Self-Sovereign Model.** Placing the individual at the core root of the derivation (depth 0), where the user is the holder of the seed and master key is the self-sovereign identity model. Here the user has the greatest degree of control and responsibility in managing their identity client-side.

**1.2 Trusted Third-party Model.** Placing the individual at a depth of 1 or any subsequent derivation is the trusted third-party model. In some cases where an individual is not willing or capable of managing their own keys on their device.

Figure 6.14: Hierarchical Deterministic Key Pairs from Robles and Appelcline [128]

As DIDs allow for multiple identities, by doing so it emphasizes the use of credentials to determine which identity is valid. This puts an extra responsibility on the attribute providers, potentially resulting in a dangerous imbalance if there are only few available to certain identity owners. This might lead to people only having self-attested credentials to request services, in this case multiple identities are a problem. van der Veen mentions using fraud-detection algorithms checking how many identities come from a specific area or limiting the use of applications per device with an exemption for registration terminals. The decision is to stick with the use of DIDs since they are best suited for this system, but Hierarchical Deterministic Key Pairs should be integrated as are fraud-detecting algorithms and limits for the number of registration coming from one device.

#### #4:Blockchain Layers: Hyperledger Indy, humanID network, Plenum and four applications

Baars agrees on choosing for Hyperledger Indy but explains there are other permissioned blockchains out there such as Quorom[2], developed by the bank JP Morgan. The system is also open-source but build on Ethereum. Similar to uPort, it costs gas to run smart-contracts which could be worked around by setting up a private network which goes against the principles for self-sovereign identities not to mention at least 1000 nodes are needed as stated by Daniels. E.g. this will not change the design

[2] https://www.jpmorgan.com/global/Quorum

decision. Baars states that not using the Sovrin network is inefficient, yet a dedicated network is necessary if a new system is to be set-up as new Trustees and Stewards are appointed.

#### #5: Use the GPLv3 License

Open sourcing this systems makes sense according to Graf, since many humanitarian organizations are funded with public money. Open source licensing is often used to encourage wide spread adoption and lower barriers for use but Graf states that a significant barrier is more likely to be found in national authorities. These authorities might not be open for a parallel distributed system alongside their own federated or centralized systems. This does not change the design decision but should be integrated in the process approach.

#### #6: Use Hyperledger Indy Roles and matching interfaces

The experts in general understood these roles and interfaces, which follow logically from the decision to use Hyperledger Indy. Baars, van der Veen and Graf all propose to add one role, that of a custodian for different reasons. Either so that parents can control the identity of their children, or because in some cultures these things are managed by central figures for example for their elderly. Baars mentions custodians could be needed because many people do not trust themselves with storing their private keys, or making back-ups. During the interviews it was not made sufficiently clear that agents (for the identity owner and trust anchor) partly fulfil these roles. Agents could be denoted to take full responsibility, or might pass on some of the responsibility to another identity owner. Similar to how the Dutch system for digital identities lets a user login to control the identity of their child or dementing parents. The concept of a custodian should be added as a role and requires a matching interface.

#### #7: Offchain storage is to be determined by context

Experts agree that private keys should be stored on a single device, paper-card or smart-card. Dijkhuis, co-responsible for an attribute provider in a centralized environment states that one could also use Highly Secure Modules (HSM) which are ISO-certified and very secure but they require some centrality. These could be used by agents. Daniels mentions that it would also be possible to not store attributes at all but upon registration they are printed out as a QR-code which could be scanned each time it is used. This would imply less storage and loosing this card might not be that bad since the information can be submitted again. It should be added to this design decision that HSM is an option for storage and that identity attributes might be stored in a QR code for people without a device.

#### #8: Social, off-line and 2-factor authentication are used for key recovery

This was an important topic during the interviews as it is vital to the self-sovereign concept. The design proposes three methods which all have some shortcomings. What was previously not discussed but put forward by Dijkhuis, is that an identity owner must be protected if they lose their key or access because the identity could be misused. One way to solve this is mentioned by Daniels who states that an identity owner should always be able to login using two-factor authentication (biometrics plus passphrase), yet this does not take away the concern of forgetting the passphrase. Another way is possible due to some centrality in the form of agents which might as well be used for benefit. An owner could report key loss to the agent of the identity provider, if the keys have been divided as hierarchical deterministic keys than the master key could provide new ones and delete old ones or multi-signature signing could be used according to Baars.

This is exemplified by Bitgo[3] where an identity owner would have three wallets (see figure E.2). For each transaction the identity owner needs two signatures using two private keys, by default the BitGo wallet signs with the identity owner, however if the owner signals a key loss the BitGo signature stops signing. Together with the recovery wallet it signs to transfer all value (DIDs) to another wallet where a new key set is published, in this way one cannot lose its identity. This design decisions should integrate the use of multi-signature signing by agents to its solutions for key loss because agents are already there and it provides a permanent solution for key loss.

[3] https://www.bitgo.com/info/

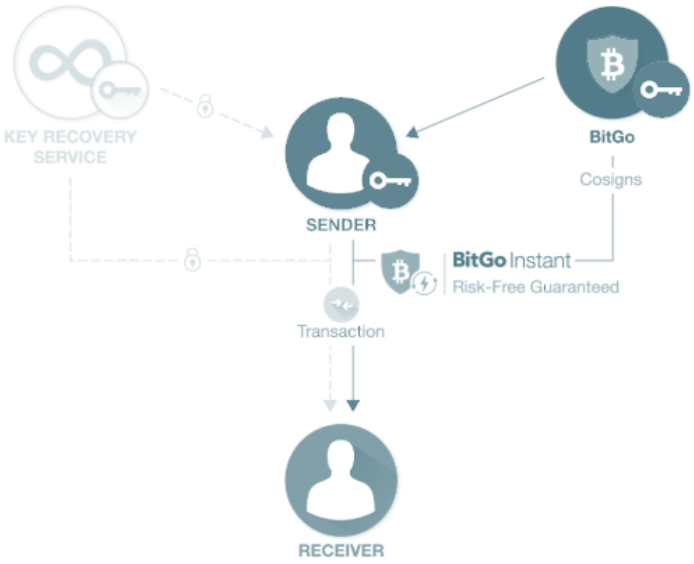



Figure 6.15: Multi-signature signing in BitGo [26]

### #9: Targeting is seen as a service not as a seperate activity

`van der Veen` posed the question whether the inclusion algorithm could also be send to the identity owner upon request, instead of the identity owner having to send credentials to the service provider. Even though the service provider will not see them, there is a risk they might be intercepted. This is a valid question and in a later scheduled expert meeting, `Baars` confirmed that this should be possible. Targeting is used as a service but only utilized by humanitarian organizations for functional purpose, this limits the opportunity for a continuous value proposition according to `van der Veen`. The value proposition should ensure that the system can be embedded within local communities and hook on other potential service providers, more like a foundational purpose. If Stewards and Trustees agree at one point that it is better to include service providers they could arrange for this as it is a similar role, the timing of decisions shall be depending on the context and which other service providers would like to join. Targeting as a service should make sure that credentials are not send but only an inclusion algorithm is send, which communicates back an inclusion score. This might be limited by the device or internet connection as it must execute some more complex logic.

### #10: Peer-validation, validation by attribute provider and by appointed validator

According to `Daniels`, it is difficult to value what peer validation contributes. From a humanitarian and self-sovereign perspective it could be used to build up a reputation without being dependent on attribute providers, e.g. it gives humanitarian organizations a better sense on who to include by relying on more than just self-attested attributes. However this would mean that a peer would sign credentials that have a public facing side and are stored on the blockchain, which compromises the privacy of the peer signing the credential. This is already a problem for an assigned validator, but a conscious choice nonetheless plus after the work is done the credential can be revoked. For this reason the design decision shall be reversed, there will be no peer validation until a solution can be found for this problem.

### Overall

People without a digital identity or with their keys lost, unable to control their account, could become the new ”most” vulnerable people if this system becomes a de facto standard. Giving life to such a system does not mean that people without digital identities should not be given aid stated by `Graf`. It will take time before there is enough coverage before regular activities can be put on hold and in the meantime current practices must be able to continue. There is a rat race to who designs and implements the first large scale global identity system according to `van der Veen`. It would make no sense if there are many scaled up systems or they should all be highly interoperable. `Graf` and

van der Veen question whether the mandate of humanitarian organizations suffices to take part in this rat race. Upon questioning Baars on this topic, he stated that the humanitarian sector should collaborate with Sovrin and Hyperledger as their system has the same purpose. Another issue regarding mandate, is the fact that humanitarian organizations have limited power before a disaster takes place. So rolling out such a system might not even be possible for humanitarian organizations alone if there is no disaster. In general implementation will proof to be difficult as the system might compete with national identity systems. Hence, it must be backed by a significant and powerful group of Trustees and Stewards. Since this thesis shuns the part of a process approach this has not yet been covered in the design decisions, yet it must be dealt with sooner than later. This feedback is not translated into the design decisions but serves as input for the discussion in chapter 7.

## 6.3. Design Decisions Second Version

The improvements from the model validation and expert validation are added to the design decisions which are displayed in figures 6.16 and 6.17. In *cursive* these improvements can be distinguished from the first version of the design decisions. This design now holds more value in a humanitarian context as it recognizes that fraud is an issue in a permissioned chain using DIDs and must be dealt with by using fraud-detection algorithms and opening up a clear trust-framework. Integrating Hierarchical Deterministic Key Pairs enables multi-show unlinkability, which was preferred but thought of as unfeasible. A more realistic view of implementation using the four layers was provided as time and the right constituency are essential to a successful roll-out. The new role of a custodian is added, examples of this role are known in a centralized system but it has to be seen how privacy of the custodian can be granted in a decentralized system. Multi-signature signing is introduced as a way to protect someones account if they loose access, a crucial extension of the design but at the cost of utilizing more centralized approaches. Lastly, a structural decision to only show service providers the anonymized and aggregated maps results in a review of this decision once a more foundational route is headed for. This iteration of the design decisions will result in more value in the humanitarian context. It can be used as a baseline to set up a process management approach in which it can be transformed to a final set of design decisions, guided by a clear participation model.

## 6.4. Evaluation

In chapter 1 the following issues with regard to CTPs were mentioned:

- Collaboration and interoperability
- Identity
- Centralization
- Privacy and data-protection

These issues are evaluated in the coming sections.

### 6.4.1. Collaboration & Interoperability

Added value to collaboration and interoperability could be perceived from looking at several existing challenges. *First*, a lack of the right tools. The design decisions propose a tool that can be used by anyone joining the network and agreeing on a trust framework. To use a distributed technology such as blockchain to store DIDs and public-faced credentials, takes away the need for several centralized systems. This system would indeed create an interoperable tool. *Second*, a lack of trust. In this system trust is encoded and put in a trust-framework. A service provider must decide if it trusts the credentials that identity owners supply. As stated by one of the expert interviewees, ”organizations must have a list of trusted organizations at all times” and by another ”identity owners will have to shop for credentials”. In this way, organizations distrusting each other might still prevail, as they simply do not trust the credentials of several attribute providers or validators upon which a service can be denied. *Third*, a difficult environment. This system does provide the option for long-lasting identities that are legitimate before, during and after disasters. It puts less pressure on registration, identification and targeting after a disastrous event has happened because some information is already out there. Aid

## humanID

| # | DECISIONS | IMPLICATIONS | LIMITATIONS |
|---|---|---|---|
| 1 | Use blockchain technology | • Use strong asymmetric encryption<br>• Enables self-sovereign identity<br>• Accommodates growth<br>• Encode trust in the system | • Uncertainty due to nascent technology<br>• *Multiple blockchains with the same use-case are inefficient* |
| 2 | Use a public permissioned blockchain | • Open to all to register<br>• Creates a buy-in for stakeholders<br>• More scalable than permissionless<br>• A trust-framework is needed outside the system | • Not open to all to validate, identify and provide services<br>• Could create a barrier for adoptability<br>• *Technically complicates the first registration for participants*<br>• Not a pure self-sovereign identity<br>• *Less transparency and more chances for fraud* |
| 3 | Use DIDs and a fully User-Centered Design | • All contact is initiated by the identity owner<br>• Identity owner controls all private data<br>• Identity owners can have multiple identities based on the digital relationship because they are pairwise pseudonymous<br>• Attribute providers become the center of gravity<br>• A Decentralized Public Key Infrastructure is used<br>• Multiple validation for one credential is possible<br>• DIDs may be used for other systems<br>• *Hierarchical Deterministic Key Pairs enable multi-show unlinkability*<br>• *Fraud detecting algorithms should be used to counter corruption with multiple identities using self-attested attributes only* | • Hundreds of DIDs are needed which should be maintained<br>• *DIDs are not human-readable a solution is necessary to maintain them*<br>• *Fraud is more likely if there are limited attribute providers or few validated credentials* |
| 4 | Use Hyperledger Indy, HumanID, Plenum and four applications | • A blockchain designed for only one use-case<br>• Different consensus mechanism can be plugged in<br>• An Identity Owner Application to register and maintain an identity<br>• An Identity Application to approve registrations and provide credentials<br>• A Service Application to provide services only accessible by humanitarian organizations<br>• An Admin Application for Trustees and Stewards to appoint other roles and direct nodes | • *Time is needed to set up a dedicated humanID network with a minimum a mount of nodes to grant security*<br>• *Identity Wallet not directly necessary as DIDs only stem from humanID and not from other blockchains* |
| 5 | Use the GPLv3 License | • Does allow for commercial use as long as it is opened up which creates a business model as proposed by Hyperledger Indy and Sovrin | • *It does not fully comply with the humanitarian principles* |

Figure 6.16: Second version of Design Decisions #1 to #5

**humanID**

| # | DECISIONS | IMPLICATIONS | LIMITATIONS |
|---|---|---|---|
| 6 | Use Hyperledger roles and matching interfaces | • Roles for Trustees, Stewards, Trust Anchors (Identity, Attribute and Service Providers), Identity Owners, *Custodian*<br>• Interfaces for Identity Owners: Feedback, User, *Custodian*, *Validator*<br>• Interfaces for Trust Anchors: Registration, Validation and Services<br>• Interfaces for Stewards and Trustees: Admin interfaces<br>• Feedback via FAQ, Chatbots and face-to-face | • A community engagement approach is necessary<br>• UX/UI must allow for illiteracy, the visual impaired, other disabilities and various languages<br>• Before implementation there must be enough Stewards and Validator nodes to grant secure and fair consensus<br>• *Uncertain how the custodian role is integrated in the system*<br>• *Custodian might endanger their own privacy* |
| 7 | Offchain storage is to be determined by context | • Options are local devices, paper-based, smartcards, secure cloud storage, *Highly Secure Modules*<br>• Private keys are stored on the device or paper based<br>• Identity attributes could be stored on a device or *on paper via QR codes*<br>• Agents back-up data | • Single points of failure arise if chosen for specific options<br>• There will always be attacks to retrieve private data |
| 8 | Social and off-line key recovery, two-factor authentication and *centralized account protection* | • An option based on social recovery<br>• An option based on offline back-up<br>• Two-factor authentication as *a permanent way to access an account*<br>• *Multi-signature signing to block an account and create a new account*<br>• *Hierarchical Deterministic Key Pairs to block an account* | • Social recovery depends on others ability to access their accounts<br>• Paper based solutions can get lost too<br>• *People often forget to make back-ups*<br>• *Multi-signature signing and Hierarchical Deterministic Key Pairs introduce some centrality with agents* |
| 9 | Targeting is seen as a service not as a separate activity | • Service provider role reserved for humanitarian organizations in functional purpose phase<br>• *Service providers can retrieve a map to see registration coverage without revealing any private information or specific location*<br>• *Inclusion algorithm is send to the identity owner, only an inclusion result is send back*<br>• *Service providers must keep a list of organizations they trust to validate credentials*<br>• Inclusion scores can only be stored temporarily<br>• Trustees and Stewards must open up the role of service provider to create a foundational system | • *Device of identity owner must be able to process inclusion algorithm*<br>• *Visualizations of geotags are available to service providers, if the system becomes foundational this connection must be reviewed*<br>• *Trust lists must be kept up to date* |
| 10 | Validation by attribute provider and by appointed validator | • *No peer validation as it is difficult to value and opens up private information*<br>• Validation by Attribute Providers<br>• Validation by appointed Validators for predefined periods only by using key rotation | • *The Validator role has to have a public facing credential opening up the identity of an individual for a specific time frame*<br>• *There is no method of assuring there are enough Validators and Attribute providers, which have a central role* |

Figure 6.17: Second version of Design Decisions #6 to #10

workers do not have to transfer files, people are not repeatedly registered. However, fragile internet and mobile connections might put the system out of order and there is no way back to a paper version. Although registration can be done upfront, the mandate of humanitarian organizations is very limited before disasters according to one expert. Especially as this system might compete with a centralized governmental identity system. Additionally, according to experience, people tend to be badly prepared for disasters to come. *Fourth*, differing interests. These lead to using several sets of inclusion criteria throughout the sector, different preferences for aid distribution and competition for funds. In the design decisions a standard set of identity attributes is proposed. This enables a faster set-up of CTPs since only inclusion criteria based on this standard set can be proposed, which people can retrieve in advance, given the availability of attribute providers. But, it requires an agreement among the Stewards and Trustees, plus it must be open enough for other organizations to participate.

### 6.4.2. Identity

There is a lack of proof-of-identity in ongoing CTPs, which is necessary to establish if people are eligible or match the inclusion criteria. This system empowers people to get identities for which it was previously impossible. For others that already had an identity, like a passport or ID card, it provides the opportunity to have it digitized. For people that own digital devices this is within reach as long as they have an internet connection, people without devices are for now tied to humanitarian organizations or other identity providers for making available registration terminals. This system thrives by having attribute providers issuing credentials and in this sense identity is not only about having a digital identity, but about having it validated. The role of attribute provider might be taken up by humanitarian organizations, field validators, national or local authorities, community representatives or others that hold any centralized information on people. If these are not continuously available then people will only hold self-attested credentials. This undermines the trust granted to digital identities, as self-attested credentials can be manipulated to match inclusion criteria. A lack of attribute providers and credentials thus limits the use of this system and the purpose of having a digital identity.

### 6.4.3. Centralization

Centralization in many identity systems leads to single point of failures. For example, the RedRose system used by multiple international humanitarian organizations for CTPs was recently breached by one of their competitors [39]. No harm was done, but it demonstrates the vulnerability of centralized systems as a majority of information is stored in one location. These design decisions propose a distributed solution where data is stored decentrally, thus single points of failures are not possible. Nonetheless, some data is still stored in central storage's and could be breached but the effects are much less severe [113]. Central systems often have a single owner, which is the opposite of what is proposed by the design decisions. The purest form of not having a single owner would be to have a public permissionless chain, where the system is controlled by all participants in the network. In this public permissioned chain the system is controlled by Trustees and Stewards, that can be of different organizations, geographical areas or sectors. There is some centrality involved. They have the power to blacklist each other if malicious behavior is noticed and a consensus mechanism that deals with the correct ordering of transactions, instead of a central authority [52]. Not having a single owner might proof beneficial for a process design, because it is more difficult to oppose a diverse group of involved organizations. More than that, it creates the opportunity to involve organizations of different backgrounds and expertise which could increase adoptability and shows widespread support to national authorities. Centralized systems are difficult to scale up, where distributed systems scale up much easier. However, that is only possible if there is a solid structure for a distributed system. The structure is provided by the design decisions and from there growth and evolution of the system is much easier than in a central system. Yet, a rapid and uncontrolled proliferation of the system might not be beneficial as the network has to keep up. Which is why a permissioned structure allows for some control in the scaling process [161].

### 6.4.4. Privacy & Data protection

The fully user-centred design best describes how privacy is embedded into the design and data is protected. Full user-centred designs are not currently used and are enabled by using blockchain and self-sovereign identities. Not storing data in a central place and not storing any private data on the blockchain are the foremost forms of protection, but the whole concept of a fully user-centred and

self-sovereign design is what holds the most power for privacy purposes. An added layer of privacy protection is provided by multi-show unlinkability, which implies that service providers will not be able to build up a profile based on previous interactions as each interaction is seen as new [12]. This is used at scale by IBM Identity Mixer [133] and using a cryptographic protocol named Hierarchical Deterministic Key Pairs, could also be possible in blockchains [12]. There is always more to be done as another privacy enhancing technology called zero-Knowledge Proofs (ZKPs) could be used. ZKPs allows to assert an identity attribute without revealing what the content is of this attribute, e.g. a person in a bar can demonstrate she is older than 18 but not when she is born or how old she exactly is [113]. This is a computationally intensive technology [53] and so far they cannot be used at scale until the right architecture allows for it. Sovrin and Hyperledger Indy claim to have created the architecture, which will be launched in August 2018.

## 6.5. Sub-Conclusion of Demonstration and Validation

This chapter answers two sub-questions. Sub-question 4, *How can the design decisions be used in the an illustrative Cash Transfer Project?* has been answered by demonstrating that it can register a digital identity, validate identity attributes, request a service and maintain or update a digital identity. This demonstration was enabled by a UML Class diagram and BPMN diagram. During the walk-through some realizations about the workings led to several improvements of the design decisions. Similar improvements came about from answering sub-question 5, *What is the value of the design decisions in a humanitarian context?* for which five experts were individually interviewed. The goal of these interviews was to gain more knowledge on the technical and social aspects, plus to assess the value of the artifact. It is difficult to assess the system in its entirety, so this was done per design decision. The overall assessment was positive, as experts recognized the potential for blockchain and self-sovereign identities. Two significant recommendations were about leaving out peer-validation (#10) and using some of the centrality in a permissioned chain to create an infrastructure in which it becomes very difficult to ever loose access to an account (#8). With regard to a more general evaluation of the design decisions, reflected on the issues that were defined in the first chapter, we can see that the added value for collaboration and interoperability lies mainly in the provision of a tool. Although this tool takes away a lack of trust in data sharing, blockchain technology is not trustless, even more so if a permissioned chain is used [81]. There is also added value for a self-sovereign identity for people that were undocumented before, but also for people to digitize their identities so loss of physical documents might have less impact. How valuable these identities are is very much dependent on what can be validated and by whom. Attracting various attribute providers and having trust in them is crucial for the value of a digital identity. Without, there is little added value compared to the existing systems. The design decisions provide a more stable solution than current systems, yet some centrality still exists. The system also has added value in that it can grow organically compared to a centralized system and more controlled compared to a permissionless system. With regards to data protection and privacy, a fully user-centered system is more capable of providing privacy but it also creates more responsibility for people to take care of their own identities. This might be burdensome, especially for the less digitized, illiterate communities or for people where identity holds a different value than to what the humanitarian sector perceives. The biggest added value of these design decisions might be that it mobilizes the humanitarian organizations that are in favor of this system, to make a process design and to make decisions on how CTPs should be conducted as a sector in the future.

# 7

# Conclusions and Discussions

In this thesis a design artifact has been developed to support the humanitarian sector in scaling up cash transfer projects. This chapter summarizes each step that has been taken and each sub-question that has been answered.

## 7.1. Conclusions

This research project focuses on registration, identification and targeting in the popularized field of protective Cash Transfer Projects. Using a Design Science Research strategy and a systems engineering perspective, the following main research question has been considered:

> *Which design choices need to be made to develop a blockchain based system that allows registration, identification and targeting in protective Cash Transfer Programs to scale up?*

To answer this main research question it was partitioned into five sub-questions, discussed over the chapters and these answers combined solve the main question. The sub-answers are briefly discussed below. In chapter 1 CTPs were introduced and it became apparent that protective CTPs are conducted by many stakeholders with varying levels of formal and informal powers, in dynamic and chaotic environments. Understanding this environment is of great importance if a new design has to be implemented in it. This has lead to the first sub-question:

> *1. What is the current socio-technical system of targeting, identification and registration in Cash Transfer Projects in a humanitarian context*

To answer this question a combination of desk research, a literature review and semi-structured interviews with cash delegates from the humanitarian sector were used. A systems engineering approach divides this sub-question into three parts: technical composition, institutional environment and important stakeholders. The proposed solution, a blockchain based identity system, has its own technical challenges and is still very nascent. This leads us to the follow-up sub-questions.

*1.1. What is the current technical composition of the system and how might that change due to blockchain?* is answered in a technical analysis. The current technical composition of the various identity systems is a federated or centralized (digital) identity system. To leapfrog inefficiencies and create new identity systems, blockchain technologies are introduced. Each digital identity system has a digital identity life-cycle with roles for an identity provider, attribute provider and service provider. Blockchain based systems can be represented in a layered blockchain architecture. Technical standards for this system should be taken into account but are not part of the further research, as it is assumed this can be dealt with in a later stadium.

*1.2. In what institutional environment does targeting, identification and registration take place?* is answered using Williamson's Framework [160]. Norms, values, regulations and laws were analyzed. CTPs take place in the wider context of transnational humanitarian governance which suffers from

collaborative issues. UN OCHA has set up the humanitarian information management principles to increase collaboration in information systems and together with privacy-by-design principles are further used in this research.

*1.3. Which important stakeholders are involved in targeting, identification and registration?* is answered using stakeholder analysis and a power-interest depicting the formal power versus the expected interest of organizations into the system. The most important stakeholders are described. For CTPs these are national/local authorities, international/national/local humanitarian organizations, donors and the (affected) community such as beneficiaries, representatives and merchants. Their preferences and demands have been represented throughout the remainder of this research.

The system analysis introduces many concepts which sketch the system-of-interest and answer sub-question 1. The digital identity life-cycle, important stakeholders, layered blockchain structure, self-sovereign identity principles, privacy-by-design principles and humanitarian information management principles are used as an input to answer the next sub-question.

*2. What are the requirements that must be satisfied in a design?*

This second sub-question was answered by performing a desk study, conducting semi-structured interviews and participatory research. This is the first deliverable or artifact of this study. It is ambiguous to the use of blockchain technology, hence it could also be used to design a centralized or federated system. The other artifacts are a set of prescriptive design decisions, a set of BPMN models explaining the dynamic business processes and a UML Class diagram to show the static object-oriented structure. The set of design decisions is the main deliverable in this research. The requirements for these artifacts can be found in table 7.1. Requirements were first elicited, then analyzed and categorized. Functional requirements state what the system must do and non-functional requirements state what the system must be. A full version that includes the source and rationale per requirement can be found in chapter 4.

Table 7.1: Summarized Program of Requirements

| ID | Requirement | Type | Priority |
|---|---|---|---|
| R.1 | Each Person Affected shall be able to register for one digital identity as an Identity Owner | Functional | High |
| R.2 | Each Person Affected shall be able to self-register or register by delegate | Functional | High |
| R.3 | Each Person Affected should add a geo-location when registering | Functional | Medium |
| R.4 | System shall only request a maximum amount of identity attributes | Functional | High |
| R.5 | System should check for double identities | Functional | Medium |
| R.6 | Humanitarian Organizations shall ask Person Affected to provide consent for the use of data | Functional | High |
| R.7 | Only humanitarian Organizations shall be able to register as an attribute provider, identity provider and service provider | Functional | High |
| R.8 | Community Representatives and Authorities should be able to register as an attribute provider | Functional | Medium |
| R.9 | Humanitarian Organizations, Community Representatives and Authorities must have an humanitarian registration interface | Non-Functional | High |
| R.10 | System must allow all humanitarian organizations to become part of it | Non-Functional | High |
| I.1 | A Person Affected shall be able to have identity attributes validated by several attribute providers | Functional | High |
| I.2 | Attribute providers shall be able to validate identity attributes and geolocations | Functional | High |
| I.3 | Attribute providers shall be able to issue verifying credentials | Functional | High |
| I.4 | Attribute providers must have an easy to use validation interface | Non-Functional | High |
| I.5 | Person Affected must always be able to access his/her credentials in a private storage | Non-Functional | High |
| U.1 | Person Affected must have an easy to use user-interface | Non-Functional | High |
| U.2 | A Person Affected shall be able to request services throughout the system | Functional | High |
| U.3 | Person Affected shall be able to safely access, update, disclose and revoke their identities | Functional | High |
| U.4 | Person Affected shall be able to regain access to their identity after loss of controll or loss of access | Functional | High |
| T.1 | Humanitarian Organizations shall be able to match Person Affected with their inclusion criteria | Functional | High |
| T.2 | Humanitarian Organizations must have a service interface for targeting | Non-Functional | High |
| T.3 | Humanitarian Organizations shall be able to verify identities based on issued credentials from other organizations | Functional | High |
| T.4 | Humanitarian Organizations must only be able to set up inclusion criteria based on minimum amount of identity attributes | Non-Functional | High |
| T.7 | Humanitarian Oganizations should delete all information that is no longer necessary for a CTP project | Functional | Medium |
| C.1 | The system must have roles for Identity Owners, Attribute Provders, Service Providers and Identity Providers | Non-Functional | High |
| C.2 | A Person Affected should be able to provide feedback during use of the system | Functional | Medium |
| C.3 | System should be able to provide open response to the feedback of people | Functional | Medium |
| C.4 | Humanitarian Organizations shall be able to create sub-entities to pass down responsibilities | Functional | High |
| C.5 | All participants and the system must safely store all information | Non-Functional | High |
| C.6 | System must provide secure end-to-end encryption for all communication and sharing of data | Non-Functional | High |
| C.7 | System must provide the highest form of privacy feasible | Non-Functional | High |
| C.8 | System should enable an overview of where people have been registered | Functional | Medium |
| C.9 | System must demand high data standards for all humanitarian organizations | Non-Functional | High |
| C.10 | System must be inclusive and accesible for all humanitarian organizations | Non-Functional | High |
| C.11 | System must be accessible at all times | Non-Functional | High |
| C.12 | System must be flexible and able to scale up | Non-Functional | High |
| C.13 | System must be open-source | Non-Functional | High |
| C.14 | System must use interoperable standards for digital identification | Non-Functional | High |
| C.15 | System must open up the governance structure online | Non-Functional | High |
| C.16 | System must have a functional purpose and grow into a foundational purpose | Non-Functional | Medium |
| C.17 | System must be accompanied by a participation model and process approach | Non-Functional | High |
| C.18 | System must not have a single owner | Non-Functional | High |
| C.19 | System must have an incentive system to demonstrate good behavior | Non-Functional | High |
| C.20 | Actors in the system shall be able to communicate with each other if communication is initiated by the Identity Owner | Functional | High |

The program of requirements is the foundation for a system design. In this research the design is presented as a set of design decisions, which leads to the following sub-question:

*3. Which design decisions have to be made?*

A variety of methods is used to answer this sub-question. Participatory research entailed several brainstorms, meetings and design sessions. Also a comparative analysis was conducted, where four open source, blockchain based, identity systems were compared to answer part *3.1. What alternatives are available for the design decisions?*. The result constituted of ten aspects that had to be decided upon, based on the differences and similarities between these four systems. These ten aspects were decided upon as part of answering part *3.2. Which alternatives best satisfy the program of requirements?*. From 3.1. we decided what alternatives were available, as to what decisions could be made. In this question, these alternatives are chosen based on the program of requirements. In figure 7.1 the first results of these decisions can be seen. They are prescriptive and accounted for in paragraph 5.4. To answer part *3.3. Do the proposed design decisions match with the program of requirements?* the design was mapped onto the program of requirements. Here it shows that on four requirements the design does not satisfy. These have to do with two design decisions and are the results of a trade-off that is plead for.

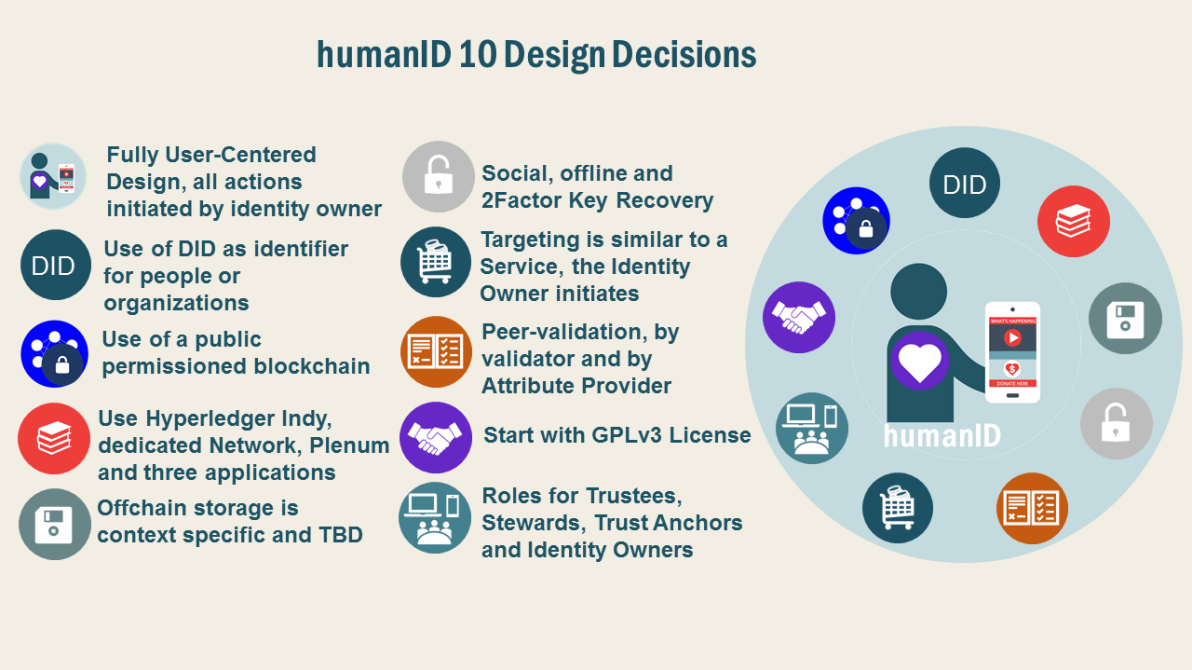



Figure 7.1: Design Decisions version 1

Making sure that the design decisions could actually result into a working system, requires a demonstration. Which the following sub-question concerns itself with:

*4. How can the design decisions be used in the an illustrative Cash Transfer Project?*

This demonstration doubles as a model validation. In this demonstration a fictive woman named Alice is taken through the processes of registration, identification, requesting a service and maintaining her identity. These processes are visualized in BPMN models and walked-through step by step. From these models several classes can be identified that are represented in a UML Class diagram, which illustrates that the design decisions can also be developed. Several realizations during this process are used to improve the design decisions, while the models and diagram form a research outcome that could be used by developers to actually build the system.

This model validation is complemented by an expert validation. Which answers the last sub-question:

*5. What is the value of the design decisions in a humanitarian context?*

Five experts were interviewed, who have backgrounds in digital humanitarian assistance, blockchain or identity management. A generic interview protocol was completed with specific questions based on the experts background. This validation had two goals: assessing the design decisions and discussing

other alternatives. In general the system was assessed positively yet some suggestions were made. Significant changes were on deciding to leave out peer-validation and using some of the centrality provided by a permissioned chain to create a more sustainable way of retrieving access to accounts.

Also two new cryptography concepts, hierarchical deterministic key pairs and multi-signature signing, are added to the decisions. The results were written down as improvements per design decision and as overall feedback. In figure 7.2 the second version of the design decisions is presented. A more general added value of the system was also discussed. A clear added value can be seen in the delivery of an interoperable tool. There is also added value in creating the opportunity to have a digital sustainable identity and to control it as an individual. The user-centred design protects the privacy of identity owners and minimizes the necessary data for service providers. The most significant added value of the design decisions might be that it brings together the humanitarian organizations and steers them away from their information silos. In the end, it is the process design and the implementation that will determine how this system is implemented and what its final form will be. At the least, these design decisions give flexibility and opportunities to be changed and be perfected into something that is usable.

## 7.2. Scientific Contribution

This research contributes to the scientific knowledgebase by providing the design of a blockchain based identity system which emanated from three sets of design principles and a systems engineering perspective. It was novel to combine self-sovereign identity (SSI) principles, privacy-by-design (PbD) principles and humanitarian information management principles (HIMP). This resulted into a shared set of principles that not only embodied a fairly ideological concept of self-sovereign identities, but combined it with the necessities of humanitarian practices and protection of data subjects. A rigorous academic approach ensured that traceability of these principles throughout the deliverables was possible. The innovative system design is put forward in an program of requirements holds originality in that it is ambiguous to the use of blockchain, the BPMN and UML diagrams that demonstrate the workings and finally into a set of design decisions. If we compare humanID to the NLRC system, differences can be found in the ideological approach while incorporating a process view for future implementation and use of the system. In relation to Blockstack, Sovrin and uPort, there is clear humanitarian touch stemming from the HIMP and the functional purpose of CTP. Designing the system as such that it can become foundational is also inventive as the majority of these systems are either functional or foundational, let alone that a transition is possible. These findings can be used by the scientific community to design, analyze or evaluate identity systems or other blockchain based systems.

## 7.3. Societal Contribution

This research contributes to society in a number of ways. In the short run, it contributes to the research and development efforts of publicly funded organizations such as the NLRC and 510. In the middle term, it will assist in developing several pilots that can already have an impact on people in need, by providing them with digital identities and enabling them for eligibility in CTPs. In the long term, it can assist the humanitarian sector and people around the world in acquiring digital identities, retaining dignity and optimizing humanitarian assistance at large. A full foundational system could contribute even more, especially in nations where digital identity systems of any sort are missing.

## 7.4. Limitations

This research has used a variety of methods, which result into limitations towards the generalization of the results. In the following paragraphs these limitations are disccussed.

### Design Science Research and Literature Review

This research was approached with a design science research strategy which is known for balancing scientific outcome and technical artifact. A researcher must divide time between both objectives, where the standard critique of the strategy is too much focus on the specific artifact, thus hindering generalization. This is noticed in three aspects. First, also in this research more time could have been spent on investigating current humanitarian information management systems, how they work, if collaboration is possible and how secure they are. As this research started from the perspective

**humanID**

| # | DECISIONS | IMPLICATIONS |
|---|---|---|
| 1 | Use blockchain technology | • Use strong asymmetric encryption<br>• Enables self-sovereign identity<br>• Accommodates growth<br>• Encode trust in the system |
| 2 | Use a public permissioned blockchain | • Open to all to register<br>• Creates a buy-in for stakeholders<br>• More scalable than permissionless<br>• A trust-framework is needed outside the system |
| 3 | Use DIDs and a fully User-Centered Design | • All contact is initiated by the identity owner<br>• Identity owner controls all private data<br>• Identity owners can have multiple identities based on the digital relationship because they are pairwise pseudonymous<br>• Attribute providers become the center of gravity<br>• A Decentralized Public Key Infrastructure is used<br>• Multiple validation for one credential is possible<br>• DIDs may be used for other systems<br>• Hierarchical Deterministic Key Pairs enable multi-show unlinkability<br>• Fraud detecting algorithms should be used to counter corruption with multiple identities using self-attested attributes only |
| 4 | Use Hyperledger Indy, HumanID, Plenum and four applications | • A blockchain designed for only one use-case<br>• Different consensus mechanism can be plugged in<br>• An Identity Owner Application to register and maintain an identity<br>• An Identity Application to approve registrations and provide credentials<br>• A Service Application to provide services only accessible by humanitarian organizations<br>• An Admin Application for Trustees and Stewards to appoint other roles and direct nodes |
| 5 | Use the GPLv3 License | • Does allow for commercial use as long as it is opened up which creates a business model as proposed by Hyperledger Indy and Sovrin |
| 6 | Use Hyperledger roles and matching interfaces | • Roles for Trustees, Stewards, Trust Anchors (Identity, Attribute and Service Providers), Identity Owners, Custodian<br>• Interfaces for Identity Owners: Feedback, User, Custodian, Validator<br>• Interfaces for Trust Anchors: Registration, Validation and Services<br>• Interfaces for Stewards and Trustees: Admin interfaces<br>• Feedback via FAQ, Chatbots and face-to-face |
| 7 | Offchain storage is to be determined by context | • Options are local devices, paper-based, smartcards, secure cloud storage, Highly Secure Modules<br>• Private keys are stored on the device or paper based<br>• Identity attributes could be stored on a device or on paper via QR codes<br>• Agents back-up data |
| 8 | Social and off-line key recovery, two-factor authentication and centralized account protection | • An option based on social recovery<br>• An option based on offline back-up<br>• Two-factor authentication as a permanent way to access an account<br>• Multi-signature signing to block an account and create a new account<br>• Hierarchical Deterministic Key Pairs to block an account |
| 9 | Targeting is seen as a service not as a separate activity | • Service provider role reserved for humanitarian organizations in functional purpose phase<br>• Service providers can retrieve a map to see registration coverage without revealing any private information or specific location<br>• Inclusion algorithm is send to the identity owner, only an inclusion result is send back<br>• Service providers must keep a list of organizations they trust to validate credentials<br>• Inclusion scores can only be stored temporarily<br>• Trustees and Stewards must open up the role of service provider to create a foundational system |
| 10 | Validation by attribute provider and by appointed validator | • No peer validation as it is difficult to value and opens up private information<br>• Validation by Attribute Providers<br>• Validation by appointed Validators for predefined periods only by using key rotation |

Figure 7.2: Second Version of Design Decisions Summary

of protective CTPs, which had limited academic literature available, this became out of scope. The search approach for literature described in appendix A, yielded only fifteen academic articles with an only regional coverage of CTP case studies. This makes generalization difficult. In other words the general knowledge gap was only based on a limited amount of CTP case studies and not on available technologies. Second, by validating the results of the literature review in semi-structured interviews, the risk of solving non-existent problems was mitigated but the risk of bias still remains. The semi-structured interviews that were used to extract information for the system analysis, have the drawback that they are time-intensive which resulted in a limited number of interviews. If more interviews were conducted, then the generalizations could have had more value. On the other hand, one might ask oneself how much additional knowledge is gained with each subsequent interview. Semi-structured interviews only return stated information, while revealed data would give more insight into how the current systems are actually used [163]. Third, this system was designed to generalize, to reach global scale and was drawn upon a wide set of design principles and validated concepts. It is the context specificity that puts this system to a real test, one illustrative demonstration has been given and this limits whether it can be a generic system used in various contexts. Generalization here comes much more from outside than from within and this is difficult to design for. The program of requirements however, was set up in a way that it could serve both central and distributed systems, that it can be made context specific as long as it fulfills the core functions and in this way the system can be generalized but different trade-offs can be made which might result in to a different set of design decisions. Unfortunately, a field-deployment to validate some of the assumptions was unfeasible for this research time-frame.

### Institutional Analysis

In the institutional analysis the theory of Williamson [160] was used to analyze the institutional environment. Yet, since this thesis deals with a complex socio-technical system, presenting a holistic view of institutions seemed out of scope. There is simply too much to consider so certain boundaries have to be set. This demarcates the solution space and creates a clear overview, whilst touching upon the main topics. Not making such a selection would result in more ambiguous results. It was aimed for to set this institutional analysis apart from the technical analysis, but this was impractical. For example, in the technical analysis a great many technologies are described but it was deemed unfeasible to discuss each set of standards, laws or regulations that applied to these technologies. Also, there was little focus on the GDPR, which is an important regulation. However, by using privacy-by-design principles and self-sovereign identity principles, dataprotection was accounted for. A risk assessment could determine if this system is GDPR compliant and what might have to change.

### Stakeholder Analysis and Desk Studies

The stakeholder analysis was set up by a desk-study. Desk-studies come with their own flaws, such as the reliability of sources that can be hard to observe and the up-to-datedness of information. These, however, can be accounted for. Within the humanitarian sector there is a lot of ”Monitoring & Evaluation” done by the organizations themselves. Using this information might be biased as it was produced on the inside, although many organizations try to outsource this activity to create an objective view. With regards to the use of new technologies there is limited information and it is difficult to check how reliable it is. For example on blockchain and related technologies a lot is written in blogposts such as Medium[1], Coindesk[2] and Hackernoon[3]. These blogs are often written by people who have invested interests in the technology so they are hardly unbiased and objective. Nevertheless, this information in some cases had to be used since there were no other sources available. The academic cycle for new technologies takes too long to have state-of-the-art reviews of technology available at scale, only conference proceedings can be found as other information might have been quickly outdated. Nonetheless, as there was a wide array of information used and many different sources were consulted, the risk of too much bias was mitigated and a profound understanding of the subject was established.

Since it was unattainable to speak with every stakeholder, a large set of assumptions were made as presented in appendix C. This limits the validity of the power-interest grid that was used in this analysis and ultimately whose interests were directly included into the program of requirements. During the

[1] https://medium.com/
[2] https://www.coindesk.com/
[3] https://hackernoon.com/

expert validation it became clear that national authorities in an affected area should have been given a more central role, but also that a wide support-frame for such a system is necessary to present a reliable alternative identity system.

### TIP Lenses

In general, this research was looked at through Technical, Institutional and Process (TIP) lenses, although the decision was made to only set-up a technical-institutional design. The design was made with the knowledge that a process approach would have to follow and thereby the design leaves room for negotiations and creates a buy-in. Including the process approach earlier could have lead to better exchanges of information upon which the design decisions were made.

### Program of Requirements and Participatory Research

The program of requirements was set up by drawing information from three resources: the desk-study, the semi-structured interviews and the participatory research. Participatory research was a methodological challenge because it embodied a similar research project that is also described in this analysis. The NLRC is developing its own system, which was participated in but also used to generate alternatives. This at times meant a conflict of interest. It was difficult not to steer into certain directions during the design sessions, but take on the role of fly-on-the-wall. This approach sometimes crippled the conceptual thinking that was needed for designing humanID, because in the more applied project of the NLRC design decisions were made around practical limitations and not theoretical ones. As every design project starts differently as described by Peffers et al. [124], NLRC's started around the code and from thereon it was backward-engineered to a system design. To be active in two research approaches, in different phases at the same time, resulted into confusion at times and might therefore have hindered this research. Lastly, it is difficult to pinpoint which idea started where if participatory research is conducted in parallel with developing a system design. In mapping the NLRC system and humanID to the program of requirements, it became clear that humanID does differ in significant areas thus the risk of copying the NLRC system is avoided.

### Generation of Alternatives and Comparative Analysis

Generation of alternatives can be done in a multitude of ways, this research has picked one that limited its view to four alternative systems. This created a tunnel vision that might have resulted in not considering viable other solutions for the system or for system components. Including these four systems also leads to a path-dependency, it might be true that other relevant technologies would better suit this purpose but have not been included since they were not mentioned by these four systems. Another drawback was that Sovrin and the NLRC system are both still conceptual. This might have resulted into parts of the system being theoretically sound but practically challenging. Since humanID has a lot of similarities with Sovrin, their launch this August will also prove part of the capabilities that humanID could have.

### model validation and Expert Validation

Validation in this thesis was done using a walk-through of the system and expert validation. The walk-through in BPMN and UML models, presented the story of Alice. This story has its own limitations as Alice has a smart-phone and internet connectivity, both assumptions are uncertain to hold in a humanitarian context. The story purposely depicts only part of what should be possible, hence some functionalities are not thoroughly assessed. This could mean that other components could also influence the design decisions. Expert validation created positive feedback and suggested improvement, yet the number of experts interviewed and their backgrounds may have limited this validation. The goal was to improve upon the design decisions, which was attained. Yet, more comprehensive feedback could have been given if an expert session had been organized instead of separate interviews or if experts would have been available with a background in humanitarian assistance and identity systems. On the other hand, some experts should be approached with in-depth knowledge on open source licensing as this was slightly overlooked. All in all, more experts should be interviewed to decrease subjectivity and further improve these design decisions. This was not possible due to time restrictions.

## 7.5. Future Research

From the limitations of the current study the following recommendations for future research are given:

### What are end-user demands for a digital identity system?

During this research it was not possible to do field research into what end-users would demand of this system, what they would need from it and how they might perceive it. The user-centered approach has not been tested so far, while it should, especially because users differ and contexts are diverse. The approach could be similar to the design science approach conducted in this research but instead of designing a model, an instance is designed and validated in the field. For example four scenarios could be sketched based on mode of registration and age, plus field tests should be conducted in a relevant geographical area:

- Self-registration for people over thirty years
- Self-registration for people under thirty years
- Registration terminal for people over thirty years
- Registration terminal for people under thirty years

Ideally these tests are conducted as part of an existing CTP or CTP that is going to be set up. This experiment not only tests the front-end but it could also test the back-end of the system at a small scale Several design iterations could be made as a result of the these tests. This would also yield results on how to test user preferences at a global scale, they might be difficult to generalize but it is interesting to see a cross-cultural perception of the same application.

### How to create a humanitarian open source license?

According to humanitarian principles it is unfavourable if organizations would financially benefit from further developing this system, in the way that it should not harm people if these organizations go bankrupt or otherwise cannot satisfy their financial commitments. Yet, each open source license available allows for commercial use. It would therefore be of value to see whether a specific humanitarian open source license could be produced. Such is not only relevant for this system but for all other humanitarian software projects. A master thesis student in software engineering, or systems engineering, might favor this research project and could use this specific project as a case study. An open source license could be developed and then generalized for similar projects in the humanitarian sector or outside. A result could be a new humanitarian open source license or the realization that there are already enough licenses out there and it is better to use one of the existing licenses.

### How to design a process management approach to implement humanID?

This research question has only been hinted at throughout this research as it was considered out of scope. The goal of such research could be to determine who should be involved, how to keep these organizations in the process and how to transform the conceptual design for humanID to a final design. Decisions to be made there are who are Stewards and Trustees, what is the standard data set upon which inclusion criteria can be formed and when to switch to a foundational purpose. Process management research could use a design approach aiming to realize a process design that can be demonstrated using humanID. First an overview of the system could be given, which focuses more on the stakeholder analysis than is done in this research. Second, a program of requirements is made and third, different process designs in the humanitarian sector or on a global scale can be analyzed, for example the development of the Cluster Approach. Based on this a system design can be created for example including multi-issue agenda setting, protecting the core values of each stakeholder and creating decisions round with clear endings and negotiation rules [44]. With a specific approach in a case study for humanID, organizations that are affiliated with large scale CTPs such as the British Red Cross can be included but also organizations involved with the Hyperledger Indy project. Generalizations could be made for process designs for global IT systems.

### What is the financial feasibility of a global humanitarian identity system?

This research has started with the idea that resources for humanitarian assistance are limited but demands are ever increasing. Since there is an overlap in setting up this system and maintaining the existing infrastructure, combined costs will at first increase significantly. Hyperledger Indy does allow for a business model and humanitarian organizations, plus other service providers might save money as administrative processes are optimized. The answer to how much of these efficiency gains flow back

into the system is yet unknown, leaving the question who is going to pay how much for it unresolved. Answers require a mixed methods research approach, where quantitative research and qualitative research are combined, for example in a social cost-benefit analysis for a specific geographical area. A lot of assumptions have to be made here and data is likely limited, but at the moment no substantiated estimates can be given at all.

#### Are the theories of Elinor Ostrom on self-governance applicable to blockchain based identity systems?

Elinor Ostrom became famous for her research on self-governance of natural resources and the tragedy of the commons. A criticism of self-governance is that scalability is difficult, but with public blockchains this might become worthwhile. Davidson et al. [41] states that blockchains could be recognized as a technology for making new economies. It would be interesting to find out if some of the theories of Ostrom could be applied to local communities keeping their information up-to-date at all times, arranging for validation and potentially further developing based on the open source code of the system. This would require less centrality, clear out some of the monopoly positions of humanitarian organizations and could strengthen local relations. All while preventing tragedies, such as fraud and corruption.

## 7.6. Reflection

### 7.6.1. Choices made within the project

During this research several choices were made that deserve reflection as they have significantly influenced the outcome.

#### Protective CTPs

There are several remarks on the use of CTPs in general. For this research, we assumed that CTPs are effective and there is a lot of academic and non-academic research to back this up. However, not in all research CTPs are found to add value or be a better solution than in-kind aid. Therefore, even if the design decisions are transformed into a final design and the foreseen benefits are yielded, it is still important to evaluate CTPs. In chapter 1 the direction of protective CTPs was chosen, which meant that the environment in which CTPs take place are chaotic, dynamic and result into information asymmetries. Also, protective CTPs are carried out by humanitarian organizations in collaboration or in accordance with local/national governments. CTPs that focus on promotion or prevention are more often carried out by the governments. Hence, if this system design was focused on promotion or prevention, the role of humanitarian organizations would have diminished and the role of authorities would have been superior. This might have led to a more centralized or federated design, private blockchain, centralized key recovery and attribute providers appointed by the government. Nevertheless, the design presented in this thesis does allow for governments to join. In the beginning only as identity or attribute providers and once opened up, also as service providers. USAID [152] state that digital identity systems also gather data which "facilitate various institutional process improvements, such as data-driven decision making, increased efficiency, or greater transparency and accountability. These process improvements, in turn, enable the system to contribute to functional goals" [p.19]. The design decisions presented can contribute to a wider area of improvements for the humanitarian sector, for example a lot less resources have to be put into administrative processes. The system could be integrated with specific last-mile solutions, and humanitarian organizations can selectively decide on where to promote the system based on the geographic information of identity owners. In general, using a system that increases collaboration might break information silos and increase partnerships outside of CTPs.

#### Technical reflections

On a technical level a lot of the complexity of blockchain technology has been left out. For example, the size of the blocks in a blockchain, the energy needed to run this system, how to generate the first block, how nodes can discover the network and how the consensus mechanism works in detail. It was assumed that since other systems utilize these technologies or part of them, they will work here as well and can be merged. In line with this, the BPMN models and UML class diagrams have not yet been developed and from implementing this a lot of questions will arise, similar to what was encountered in the participatory research. Theoretical technical solutions might not always be favored over practical implementations. For example, at this moment zero-knowledge proofs are theoretically possible on a blockchain but are not included in the design because they have not been put out at scale, but they

do offer a significant privacy-enhancement if possible at scale. Another limitation is that of blockchain technology which at a technical level is only an innovation at the data layer in this design. Of course stemming from this several institutional challenges could be solved, but opposed to the financial use-cases there is little radical technical innovation. Another technical topic that deserves reflection is that of key recovery, it was already mentioned by Dunphy and Petitcolas [55] that key loss might result in a new set of vulnerable people. Some experts also mentioned this and it is therefore necessary to state that this system should not one-to-one replace what is currently out there. Humanitarian organizations should keep helping people without digital identities until this system has sufficient coverage in a certain geographical area and even then the most vulnerable, with or without digital identities should be taken care off. Further technical considerations can be found in the use of cryptographic protection. For now the blockchain seems like a more than sufficient solution, but most cryptographic schemes have been broken at one point in time. In the near future, quantum computing might be one of the technologies that could crack some of the cryptography in blockchain [48]. Efforts are underway to create quantum-proof cryptography, for example the Estonian government uses Keyless Signature Infrastructure (KSI) which are protected against quantum algorithms [158]. Lastly, this system does not fully cover the possibility to ”game” the system by creating multiple identities. This has been an issue in digital identity systems for a long time. Recently organizations try to tackle it with the use of biometrics, but this brings about it own risks. Some centrality, authorized by nation states, is the only feasible solution for now but goes against the principles of self-sovereignty.

### Institutional Reflections

At an institutional level, it is important to state that ’encoding trust’ is not the same as ’trusting the system’. An example was presented by Frederik and Bregman [61] in a podcast with a critical note on blockchain technology, that explained an experiment where contracts for housing were made fully transparent i.e. ensuring trust as everybody could read it. The problem was not transparency, but understanding since people were not trained in reading and understanding such language or agreements. Using hundreds of DIDs that are not easily transformed to human-meaningful information and could result in the same problem, particularly for people in distress with high illiteracy rates and a limited digital literacy. Another limitation stemming from the institutional analysis was to not focus on GDPR and in specific on the right to be forgotten which implies that identities can be deleted. Blockchain is associated with permanency of data, although no private data is stored on the blockchain but pointers to identities via the DIDs are permanently stored. These can be dereferenced, so it is impossible to find out who they belong to but they cannot be fully deleted. Future technologies might be able to correlate them which could result in violating the GDPR.

### Maintenance of Identities and Mandate

A related issue that this design has not taken into account is what happens if someone dies. If identities are controlled by identity owners, than who informs the network that this person has deceased, so misuse of the identity is prevented. An essential component in this system is the use of up-to-date credentials and identity attributes, which would require the system to be part of everyday behavior or as mentioned in the expert interviews ”it should have a continuous value proposition”. This requires a community engagement approach and a foundational purpose, which is constricted by the design, aimed to be primarily functional in the first phases. The decided manner allows the system to be rolled out on the need of CTPs and develop an installed based before opening up and allowing for a foundational purpose. Consequently, in the first phases humanitarian organizations will sustain a large share of their monopoly on validation and services, and have to put in extra effort to keep this system up-to-date. Compared to the current situation, the advantage is that humanitarian organizations can better coordinate their efforts, saving time and money, but at the cost of a bottom-up solution. Humanitarian organizations will have to guide people in thinking along the lines of digital identity as something not only necessary during or after a disaster, but it will only be useful if there are other services provided than just CTPs. Even if this is technically and socially achievable, it remains to be questioned if this is in line with the humanitarian mandate. It might not be anyone’s mandate to provide the first global digital identity system, but competing with well-organized technical institutes such as Microsoft (U-prove) and IBM (Identity Mixer) might not be a fair fight. Moreover, during stable times, humanitarian organizations only have limited formal or informal power and national authorities could perceive the system as competing with their own. Clear and calculated implementation procedures and process approaches are therefore decisive for the success of this system.

#### Process Approach

In a process approach agreements on who is responsible for maintaining, developing and running (Stewards) the system should be made. One could propose, since it is open source licensed, that in several countries instances of the system are realized and several key elements are forked back to the generic system so interoperability is possible. Yet, even if these agreements can be made, there is a limited number of blockchain developers available worldwide who can build and maintain it. Throughout this research a standard data input for this system was mentioned which emanates from the diversity in inclusion criteria currently used throughout the sector. If each identity owner would be required to have a different set of credentials interoperability would be limited, which standard data input and thus standard inclusion criteria resolves. Agreement on what data to include should be integrated in this process approach before launch. Agreement will be very difficult but is not impossible. In 2015, all UN member states agreed upon 169 objectives and created the Sustainable Development Goals, which was made possible by a premeditated process management approach [50]. It took time, a dedicated vision pushed by persisting people, agendas incorporating more than just one topic and breaking traditional power-structures but they did find sufficient common ground [50].

#### Western Bias

A final reflection is that the proposed system is based on expert interviews, semi-structured interviews, academic knowledge and gray literature. All almost exclusively originating from within western culture. This may have resulted in bias in this research, a different cultural paradigm may have lead to a different outcome. Moreover, the research has insufficiently taken the end-user perspective into account. Nevertheless, the used sources build on rigorous research into CTPs and their effectiveness. A lot can still be gained during the first phases of the process approach and front-end design that is yet to be done, but the design might turn out to fall short on certain structural aspects that would have come up would end-users have been integrated in an earlier stage.

### 7.6.2. Personal Reflection

This research is the grand finale of the two-year master program in Complex Systems Engineering and Management (CoSEM) at Delft University of Technology. This program has the purpose to teach design skills for solving complex socio-technical issues within a specific track, Information & Communication Technologies being one of them. Throughout the CoSEM program many opportunities surfaced to merge personal interests with the curriculum, either in elective courses or project work. This has also resulted in graduating under the supervision of the NLRC and this specific research topic. The combination of blockchain, a very novel technology that is little understood, with the complexities of providing humanitarian aid, could be seen as an archetypal case for a socially aware CoSEM student. Performing six months of research in an environment with plenty of intrinsically motivated people, skilled professionals who could have worked for organizations with better terms of employment but stick with their professions for the love of doing good and the doors that open for humanitarian researchers, made these months truly worthwhile. This experience not only brought together all the skills and knowledge taught in these two years, it also gave sense and purpose to the relevance of programs such as CoSEM. In an ever more complex world, there is a clear need of structure and tackling the problems instead of the symptoms. Where one looks at a technical and institutional design with the knowledge that it will change once used, that users will try to game a system and implementation might be the biggest challenge. In general, looking back at this research process I am satisfied with the result. There has been a critical assessment of intermediary results, it was executed with academic rigour and I enjoyed the journey. Retrieving in-depth knowledge on blockchain and the humanitarian sectors were two goals that are achieved. Managing the project proved to be more of a challenge than I had expected in the beginning, but kept me down to earth and informed me there is much to be learned.

## 7.7. Recommendations to 510 and the NLRC

As this research is performed under the supervision of 510 and the NLRC, we would like to make several recommendations. In general the set of future research questions in paragraph 7.5 can be seen as recommendations and are in line with 510's development efforts. Another general recommendation that stems from the participatory research practice is process related. The project is incrementally being developed in which the system design follows from the code, instead of the other way around. While it

is clear what the ideology for this system is, it remains unclear as to how this ideology is embedded into the system. A structured approach with a program of requirements developed in-house and discussed with development partners, that guides the technical development would greatly benefit the project. Ensuring traceability within the system design and thus the code, would create advanced insights into where the project is headed to.

### Technical Recommendations

1. The NLRC system is built on a public permissionless blockchain with the underlying bitcoin blockchain. This decision should be re-evaluated based on this research. With this also comes the use of a particular network, consensus protocol and the roles.

2. The system must make use of DIDs instead of Merkle Trees. DIDs offer much more opportunities with regard to protecting privacy, giving control to the identity owner and interoperability. This would be in line with the HIMP.

3. The NLRC and 510 should increase their efforts in finding a secure offchain data storage that can be used in a distributed network by people with and without digital devices. The solution must be scalable as the network grows, follow safe and secure IT practices, allow identity owners to store back-ups and be context specific.

4. The solutions offered for key recovery come up short in a humanitarian context. This might create a new group of extremely vulnerable people. If there is some centrality in the system, it could be utilized for account recovery and protection. These possibilities must be further investigated and integrated in the system design.

5. Leave peer validation out of scope for the time being. There is little direct value and it constrains the system to be permissionless.

6. The system must somehow connect to last-mile solutions. We recommend to inquire on issuing credentials that demonstrate that identity owners are entitled to a certain amount of money. These credentials entitle identity owners to a one-time claim for cash with service providers that hand-out cash. This protects the privacy of identity owners as third-parties would only need to receive the credential and check that it is handed out by a service provider they trust, upon which they can give them cash.

7. The current system is not fully user-centric, i.e. a humanitarian service provider has an automatic connection with the identity owners. Targeting is seen as a separate activity, instead of being one of the many services. A fully user-centred design would be recommended.

### Institutional Recommendations

From a social perspective, 510 and the NLRC, are very aware of the formal and informal rules, cultures and ethics, that affect their humanitarian assistance programs. From a technical perspective, involving digital identity systems, blockchain and distributed data storage, there are several recommendations to make:

1. The GDPR has come in to affect and the system that is being developed must be critically assessed on this novel regulation.

2. During the semi-structured interviews it was stated that national/local regulation was not always taken into account, it is recommended to develop a framework that allows for a compliance assessment with national regulation.

3. ISO/TC 307 is becoming a noteworthy blockchain standard and could positively influence inter-operability of blockchain based applications, monitoring these developments and incorporating the standards could benefit their efforts

### Process Recommendations

Several of the future research questions concern the process management approach that should follow up on the design presented in this research. Concise recommendations are the following:

1. Hyperledger Indy is developed by Sovrin and the Hyperledger Foundation, they have a significant following and are involved in the wider context of blockchain development. We recommend 510 and the NLRC to get involved with them as they are focusing on a similar use case and have impressive resources

2. To start a process management approach an ideal program of requirements could be developed and broken down into parts that will be tested per pilot over a period of years, then a buy-in for collaboration per pilot could be sought after within and outside of the Red Cross Movement, clearly communicating what is to be expected and what is not. To manage expectations the program of requirements should be accompanied by succinct BPMN and UML Class diagrams, with a clear division of roles based on the descriptions of a blockchain ecosystem, digital identity ecosystem and CTP ecosystem.

# A

# Literature Review

To increase understanding of the processes and challenges in CTPs an academic literature review was conducted. The selection process is shown in figure A.1.

There were several criteria for including studies into this review. First, as the research into CTPs has significantly increased as of 2004 (after the tsunami in the Indian Ocean), this was used a lower boundary for publication dates. Second, only articles written in English were selected. Third, articles were scanned on the use of CTP as one of their main interventions in order to extract challenges directly related to CTPs and not to other interventions. Fourth, the CTPs had to be used in a humanitarian context. Fifth, design elements had to be extracted in case studies in order to relate challenges to specific design options.

Applying these criteria to search results from SCOPUS, SUMMON and ScienceDirect led to 3 academic journals. Through backward snowballing in the academic journals and gray literature that was found, applying the same criteria, a final result of 16 studies were included. As many organizations executing CTPs evaluate their own programs, this literature will serve as domain specific information later in this thesis.

Each literature review has its limitations, such as cultural bias by the researcher, access to literature and the available time. More specific, there was a lack of previous studies, resulting in a small sample size and less critical judgments on what to include. For example some of the studies only included 40 households, which makes it hard to generalize their findings. Through repeating part of the literature search and cross-checking the final selection with peers and Red Cross experts, this limitation was partly mitigated. Another limitation is that CTPs are highly context dependent, making them hard to compare and difficult to interpret. This was partly mitigated by classifying with design options, relating specific challenges to generic ones and cross-checking with Red Cross experts.

The results of the literature review are presented in tables A.1, A.2 and A.3.

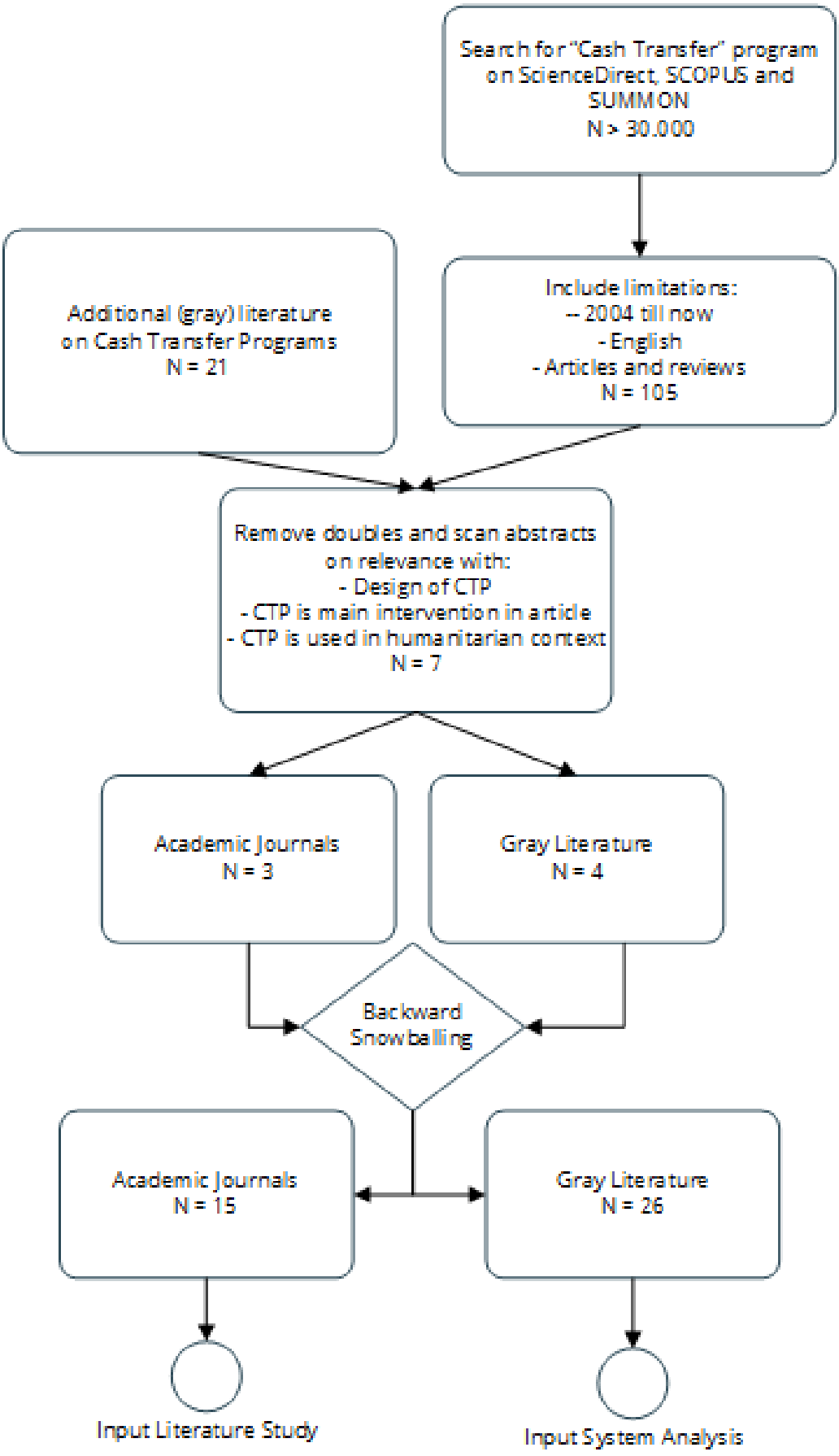



Figure A.1: Literature Review Selection Process

Table A.1: Overview of selected literature

| Authors | Year | Journal | Study design | CTP Type | CTP Objectives | CTP Size | Transfer Mechanisms | Targeting Methods | Time Frame | Transfer Amount | Monitoring & Evaluation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Aker | (2017) | The World Bank Economic Review | Case Study, Eastern DRC, emergency response | UCT, Voucher | Increase purchasing power of food and non-food items | 474 HH | Local credit system (no fees), Vouchers on fairs | Community based selection | 3 times in 7 months | $130 total | Focus groups<br>Household surveys<br>Market data |
| Ali & Gelsdorf | (2012) | Global Food Security | Case Study, Somalia, lessons learned | UCT<br>Voucher<br>Cash-for-Work | Cope with famine | 1.700.000 pers | Local Credit System (Hawlala) | Categorical selection<br>Community based selection | one-time | $75-125 (UCT)<br>$51-65(Vouchers) | Beneficiary feedback<br>External regulation<br>Independent Field Monitors<br>Market data<br>Surveys (monthly & quarterly) |
| Bailey & Walsh | (2007) | The Journal of Humanitarian Assistance | Case Study, DRC, non-acute emergency response | CCT | Non-food needs assessment, understand intra-household decision making | 40 HH | Cash | Lottery<br>Self-selection | one-time | $63 | Beneficiary feedback (self-reporting)<br>Beneficiary feedback (interviews)<br>Field Monitoring |
| Bedran-Martins & Lemos | (2017) | World Development Perspectives | Case Study, Brasil, emergency response | CCT | Cope with drought, reducing poverty | 221 HH | Cash | Categorical selection | monthly, long-term | $50 (average) | n/a |
| Brooy | (2007) | Journal of Human Security | Quant./Qual economic review, emergency response, effect local economy | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Davies & Davey | (2007) | Development Policy Review | Case study, Malawi, emergency response, effect on economy | UCT | Developing transfer mechanisms, provide aid, research impact on local economy | 10.000 HH | Mobile banks<br>Smart cards | n/a | monthly, 5 months | $12 (average) | Field monitoring<br>Focus groups<br>Surveys (monthly) |
| Doocy, Tappis & Lyles | (2016) | Journal of International Humanitarian Action | Case Study, Syria, exploration for expansion | UCT<br>Vouchers | Cope with internal conflict | 34 HH | Local Credit System (Hawlala) | Categorical selection | n/a | n/a | n/a |
| Fenn et al. | (2015) | Public Health Nutrition | Case Study, Niger, emergency response, effect on nutrition | UCT | Cope with malnutrition | 412 HH | Cash | Categorical selection<br>Vulnerability assessments | monthly, 6 months | $44-59 | Focus groups<br>Key informant interviews<br>Surveys (pre- & post-intervention) |
| Jelle et al. | (2017) | BMC Public Health | Case Study, Somalia, emergency response, effect on malnutrition | UCT | Cope with malnutrition, compare with in-kind aid | n/a | Mobile banks | Vulnerability assessment | monthly, 5 months | $84 | Focus groups<br>Health checks (monthly)<br>Key informant interviews<br>Surveys (pre- & post-intervention) |
| Kebede | (2006) | Development Policy Review | Case Study, Ethiopia, emergency response, comparison with food aid | UCT<br>Cash-for-Work | Reduce poverty, cope with food insecurity to prevent asset depletion | 128.260 pers. | Cash | Categorical selection<br>Community based selection | monthly, 7 months per year | $13 (average) | Focus groups<br>Key informant interviews<br>Market data<br>Survey (baseline) |
| Kelaher & Dollery | (2008) | International Review of Public Administration | Case Study, Indonesia, comparison with food aid | UCT<br>CCT<br>Vouchers<br>Cash-for-Work | Increase purchasing power, develop transfer mechanisms, test market conditions | 15122 pers. | Cash<br>Voucher | Categorical selection | monthly, 3 months | $13 | Beneficiary feedback (interviews)<br>Market data<br>Monitoring (merchants) |
| Langendorf et al. | (2014) | PLoS Medicine | Case Study, Niger, emergency response, effect on food security | UCT | Cope with malnutrition, compare with in-kind aid | 5.395 pers. | Cash | Categorical selection | monthly, 5 months | $59 | Beneficiary feedback (interviews)<br>Focus groups<br>Health checks (monthly)<br>Survey (monthly) |
| Lee | (2012) | Columbia Socail Work Review | Case Study, Somalia, emergency response, review CTP | UCT | Cope with food insecurity, drought, internal conflict and political instability | 13.830 HH | Cash | n/a | one-time | $50 | n/a |
| Mattinen & Ogden | (2006) | Disasters | Case Study, Somalia, emergency response, review CTP | Cash-for-Work | Increase purchasing power, increase access to water, enable restocking | 4029 HH | Local credit system (Xawalaad)<br>Vouchers | Categorical selection<br>Community based selection<br>Vulnerability assessment | 1 or >, 16 months | $30 (10-12 days)<br>$56 (20 days) | Focus groups<br>Key informant interviews<br>Surveys (post-intervention)<br>Work monitoring |
| Pega et al. | (2015) | Cochrane Database of Systematic Reviews | Systematic Review | UCT | Increase health outcomes | (1): 1200 HH<br>(2): 5395 pers. | Bank<br>Cash<br>Card<br>Mobile Banks | Categorical selection | monthly, 5 months | $45-59 | Beneficiary feedback (monthly, interviews)<br>Focus groups<br>Health checks (monthly)<br>Survey (pre- & post-intervention) |

Table A.2: Challenges derived from literature

| Authors | Year | Challenges |
|---|---|---|
| Aker | (2017) | 1. In-kind aid is safer if cash is easier to steal for donor and for beneficiary<br>2. UCTs could end up in the purchase of temptation goods<br>3. Local markets could not provide satisfactory supply<br>4. Hard to locate households for evaluation in camps as they continue traveling<br>5. Difficult to acquire full data on expenses<br>6. Voucher-beneficiaries bought staple goods to resell on local markets<br>7. Providing cash and complementary in-kind aid does not mean beneficiaries will buy the provided in-kind aid<br>8. UCTs were cheaper than vouchers<br>9. On average it took a beneficiary 90 to 105 minutes in line and 240 minutes to travel and pick it up |
| Ali & Gelsdorf | (2012) | 1. Months went by of negotiating before cash response was started<br>2. All forms of aid were at risk, so complementary programs were uncertain too<br>3. Difficulties in targeting the most vulnerable<br>4. Difficulties in monitoring interventions<br>5. Aid diversion by all parties (terrorist, authorities etc), crippling donor confidence<br>6. Access and security were limited<br>7. INGO's had to depend on local NGO's, which led to difficulties for M&E<br>8. M&E framework cannot fully detect fraud or diversion<br>9. Self-selection by local authorities sometimes lead to exclusion of vulnerable people<br>11. A good number of humanitarian aid workers have to be trained in CTP<br>12. Problems with handling donor contracts and unnecessary complexity<br>13. Significant coordination issues due to lack of clear problem owner<br>14. Interactions with Hawlala agents are still informal and trust-based, no contracts<br>15. Different organizations rarely share information with each other |
| Bailey & Walsh | (2007) | 1. Cash could potentially create local inflation<br>2. "Use of cash can incur security threats for beneficiary and staff"<br>3. Cash assistance could disbenefit women as they often do not control money flows in the household<br>4. Targeting method resulted in selection of people that live close to major markets, hence not ultimately poor<br>5. Self-selection results in entrepreneurial participants<br>6. For complementary in-kind aid it was hard to track and evaluate impact<br>7. Hard to define what is a good purchase and what is a bad purchase<br>8. Gender design is important for CTP<br>9. Markets should be available or brought to the recipients of cash/vouchers |
| Bedran-Martins & Lemos | (2017) | 1. Struggle with politicians only wanting to solve the symptoms so they can stay in position<br>2. High levels of vulnerability remain after participation<br>3. Farmers often receive their emergency benefits too late<br>4. Cash transfers reinforce the position of poor people in this political relationship |
| Brooy | (2007) | 1. Inflationary risk is considerable according to critics<br>2. Competitive and responsive markets are integral to the implementation of a CTP"<br>3. Assumption is that local markets are monetized in that the "preferred medium of exchange is currency"<br>4. Scale of CTPs so far has been minuscule (amount of cash and size), however the "larger the scale the greater the potential for local inflation"<br>5. Need for complementary programs to impact the supply side, "better evaluation of HH incomes in conjunction with market assessments should be undertaken"<br>6. Quality data is essential for assessments, targeting, evaluation etc. |
| Davies & Davey | (2007) | 1. Sources of income are hard to determine, making vulnerability based on income difficult to determine<br>2. There are a lot of difficulties to track income from the CTP, multiplier effects have to be taken into account to say something about the local economy<br>3. Classification of people is difficult; people hold multiple jobs, have multiple partners, seasonal spending<br>4. Possibility of identification through children who are able to pay their school fees after receiving cash |
| Doocy, Tappis & Lyles | (2016) | 1. Lack of a regulated cash transfer system within the country to move funds<br>2. Current movement of funds through informal value transfer networks, paying attention to fiduciary risks and accountability<br>3. Success is highly determined by context<br>4. There was insufficient supply of food, markets need to function<br>5. High number of people borrowing money or receiving credit<br>6. Cash assistance was preferred<br>7. Recipients feared prices would go up if vouchers were provided<br>9. NGO acceptance is limited by donor and organizational capabilities<br>10. Local councils expressed preference for a community approach instead of household approach<br>12. "Scaling up cash-based responses in a volatile environment may present new risks"<br>14. There has to be "clarity on legal and financial compliance mechanisms" (in some cases cash assistance might not be permitted)<br>15. Organizations should be flexible in their transfer mechanism approach<br>16. Physically carrying cash over the border is dangerous |
| Fenn et al. | (2015) | 1. Lots of seasonal dependencies (amount of transfer, migration during program etc)<br>2. "Without control group, it is not possible to attribute changes to the cash alone"<br>3. Although cash handed to women, culturally men bought staple goods so ended up with the majority of the cash<br>4. Social desirable answers on questionnaire |
| Jelle et al. | (2017) | 1. Lack of humanitarian access<br>2. Camp-based programs can face evictions of beneficiaries<br>3. Highly dependent on the willingness of donors to support CTP<br>4. Data for evaluation need to be consequently/uniformly submitted to have valid results, e.g. you need to educate people |
| Kebede | (2006) | 1. Collaboration depends on previous experience with CTP<br>2. Because of two programs, one with a working requirement and one without, it was unclear for some households what to do<br>3. Retargeting was necessary due to overlapping effects of multiple programs<br>4. Errors in targeting lead to insufficient funds for extremely poor households, subsequently households started redistributing funds themselves<br>5. Evaluation is also dependent on other data sources (markets, food prices etc)<br>6. If you do a national program, yet market prices may differ per region, you have to take this into account for the transfer amount<br>7. CTP drove up the local prices and due to errors in targeting, the poorest people were even worse off<br>8. Due to irregularity and inconsistency of the payments, beneficiaries were unable to plan ahead driving up prices even more<br>9. Unable to change the wage rate because it would create inconsistencies between the programs |
| Kelaher & Dollery | (2008) | 1. "In emergency aid, the level of information is often limited and pressure for immediate response great"<br>2. "Targeting can be expensive and socially divisive"<br>3. Cash-based targeting is different from in-kind food aid targeting and requires a more integrated and coordinated approach<br>4. "Community-based targeting in complex emergencies generally results in almost universal coverage"<br>5. CTP can influence "already committed in-kind food donors"<br>6. Potential of cash disincentivizing work<br>7. Scale is needed to drive down costs and increase efficiency<br>8. Assessment criteria should be defined at the start of a CTP, and "implemented straight away to avoid inclusions errors and disincentives to training and education"<br>9. "CTP pilots in emergency situations have usually been small-scale with deficiencies in market data and systematic quantitative evidence"<br>10. "Whatever form aid transfers take, it is the predictability of the transfers which is important to eligible beneficiaries" |
| Langendorf et al. | (2014) | 1. Complementary programs had a better effect on child health than CTP or in-kind food aid alone<br>2. Beneficiaries express preference for cash in some cases<br>3. Nutritious food for young children might not be available on the market<br>4. Cash transfers need additional means to what an agency normally delivers |
| Lee | (2012) | 1. Reluctance to CTP is rooted in paternalism, institutional change is needed<br>2. Effective program design is very versatile and hard to organize for<br>3. "Accounting for fluctuations in the exchange rate, resulted in devaluation in local currency"<br>4. Local government was not happy<br>5. "Decrease of effectiveness due to a lag in follow-up interventions" |
| Mattinen & Ogden | (2006) | 1. "Initial concerns over security and inappropriate use of cash were largely proved to be exaggerated"<br>2. "Targeting would be easier if the project had a work component"<br>3. Financing the project is difficult and limits the scope<br>4. A lack of transparency can frustrate the process and invoke disruptions within the communities<br>5. There was no banking system so USD were transferred via Nairobi to Somalia, "local traders then converted cash into Somali shillings"<br>6. Most money was used for debt-repayment<br>7. "Targeting, in general, is a challenge, targeting of cash could be perceived as more difficult since cash is of value to everyone"<br>8. "Objectives and timing need to be viewed in the context of seasonal calendars to understand better the likely impact of a cash injection"<br>9. "The amount should be set in relation to all project goals, this requires in-depth understanding of socio-economic situation of the households, needs, and priorities"<br>10. Exchange rates varied during the project<br>11. "Participatory techniques should be employed in monitoring and the results should be systematically discussed with and validated by beneficiaries"<br>12. "Market surveys should be conducted systematically, and an exhaustive market analysis prior to the intervention is essential" |
| Pega et al. | (2015) | 1. Meta-analysis was difficult due to different CTP designs<br>2. Targeting the poorest is difficult<br>3. A functioning market is needed for a CTP<br>4. Beneficiaries might be forced to repay debts if they receive cash<br>5. CTPs require deep local knowledge to effectively target the right beneficiaries<br>6. There is a chance local inflation arises |

Table A.3: Interpretation of challenges related to design options

| Authors | Year | CTP Objectives | Transfer Mechanisms | Targeting Methods | Time Frame | Transfer Amount | Monitoring & Evaluation |
|---|---|---|---|---|---|---|---|
| Aker | (2017) | Diversion: cash could be spent unsocial, for debts or on temptation goods<br>Diversion: conditional food can be resold<br>Functional markets: supply should be present | Cash: distribution points require travel and waiting time<br>Security: only cash when safety (recipient and organization) is guaranteed | | | | Location: beneficiaries change location<br>Traceability: difficult to trace expenses |
| Ali & Gelsdorf | (2012) | Complementarity: can increase uncertainty<br>Coordination: is complex due to context but vita<br>Coordination: aid workers have to be trained<br>Diversion: leads to decreased donor confidence | Cash: Hawlala is informal and trust-based<br>Security: access and security were limited | General: Targeting the poorest is time-intensive, expensive, complex and access dependent<br>Self-selection: can lead to exclusion of vulnerable people | | Funding: determines amounts and start of the program<br>Funding: contracts with donors have to b negotiated and can add complexity | Traceability: different organizations and complementary programs make it non-transparent<br>Uncertainty: will remain as monitoring & evaluation is limited |
| Bailey & Walsh | (2007) | Functional markets: supply should be present | Cash: can lead to local inflation<br>Cash: can lead to gender inequality<br>Security: only cash when safety (recipient and organization) is guaranteed | Geographical targeting: does not necessarily lead to identifying the most vu<br>Self-selection: leads to entrepreneurial be | | | Traceability: different organizations and complementary programs make it non-transparent |
| Bedran-Martins & Lemos | (2017) | Coordination: is complex due to context, but vital | | | Timeliness: delayed transfers can be deadly | | |
| Brooy | (2007) | Complementarity: CTP have to be integrated with existing program<br>Functional markets: supply should be present<br>Functional markets: responsive and monetized<br>Scale: the larger the scale, the higher the chanc inflation | Cash: can lead to local inflation | General: targeting highly dependent on quality data | | | Data Quality: regular evaluations needed to ensure quality data |
| Davies & Davey | (2007) | | | Categorical selection: difficult as people hold multiple jobs, multiple par<br>General: Targeting the poorest is time-intensive, expensive, complex and access dependent | | | Uncertainty: will remain, as multiplier effects exist |
| Doocy, Tappis & Lyles | (2016) | Coordination: is complex due to context but vital<br>Diversion: cash could be spent unsocial, for debts or on temptation goods<br>Functional markets: supply should be present<br>Legal: CTP have to be allowed in the country of intervention | Cash: no local credit system working<br>Cash: hawlala is informal and trust-based<br>Cash: can lead to local inflation<br>General: flexibility might be needed if context changes<br>Security: only cash when safety (recipient and organization) is guaranteed | Coordination: different preferences for targeting methods | | Scale: scaling up may present new risks | |
| Fenn et al. | (2015) | | Cash: can lead to gender inequality | | | Flexibility: seasonality influences market prices | Methods: socially desirable anwers influence evaluation<br>Methods: you need a control group to establish the effect of a CTP |
| Jelle et al. | (2017) | Coordination: aid workers have to be trained in CTP | | General: Targeting the poorest is time-intensive, expensive, complex and access dependent | | Funding: willingness determines amounts and start of the program | Data Quality: uniform and consequent data collection highly influences evaluation<br>Location: beneficiaries change location |
| Kebede | (2006) | Complementarity: different programs can cause uncertainty | | General: retargeting should be possible<br>General: targeting errors can lead to the poorest being worse off | Timeliness: irregularity of the payments results in increased prices to cover risks | Geographical: (non)-food prices might differ per region | Data Quality: evaluation is also dependent on quality of other data sources |
| Kelaher & Dollery | (2008) | Complementarity: CTP have to be integrated with existing program<br>Scale: is needed to drive down coststand increa | | Eligibility criteria: decided upon in advance and made transparent<br>General: targeting can be socially divisive<br>General: CTP targeting is different from in-kind aid targeting | Timeliness: predictability of payments is crucial for beneficiaries | | Data Quality: evaluation is also dependent on quality of other data sources<br>Scale: CTP pilots often small scale, hence hard to generalize |
| Langendorf et al. | (2014) | Complementarity: CTP have to be integrated with existing program<br>Coordination: CTP need additional means comp<br>Functional markets: supply should be present | | | | | |
| Lee | (2012) | Coordination: institutional change is needed to improve CTP | | Cash-for-work: might make targeting easier as richer people will not want to work for the cash | | Flexibility: fluctuations in exchange rate<br>Funding: willingness determines amounts and start of the program | Follow-up: decrease of effectiveness of CTP due to lack of follow-up |
| Mattinen & Ogden | (2006) | Diversion: cash could be spent unsocial, for debts or on temptation goods<br>Security: only cash when safety (recipient and organization) is guaranteed<br>Transparency: a lack thereof can disrupt the CT | Cash: no local credit system working<br>Cash: hawlala is informal and trust-based<br>Cash: can lead to local inflation<br>General: flexibility might be needed if context changes | General: Targeting the poorest is time-intensive, expensive, complex and access dependent | Timeliness: predictability of payments is crucial for beneficiaries | Flexibility: seasonality influences market prices<br>Flexibility: fluctuations in exchange rate<br>Funding: willingness determines amounts and start of the program | Follow-up: evaluation should be validated by beneficiaries<br>Data Quality: uniform and consequent data collection highly influences evaluation |
| Pega et al. | (2015) | Coordination: is complex due to context but vital<br>Diversion: cash could be spent unsocial, for debts or on temptation goods<br>Functional markets: supply should be present | Cash: can lead to local inflation | General: Targeting the poorest is time-intensive, expensive, complex and access dependent | | | Methods: hard to do meta-analysis due to different study designs, bias and indirect-ness of intervention |

# B

# Semi-Structured Interviews

Interviews have been conducted in a semi-structured way. Semi-structured interviews are based on a set of predefined questions, but they are open and can be put forward in a flexible order [93, p. 57]. They are particularly useful when investigating complex systems, as they offer less restrictions on potential answers than structured interviews do [93, p. 57]. It can be a disadvantage to conduct these qualitative interviews as they require a lot of time and resources, also it can be hard to generalize the results as you need a significant number of interviewees to do so. Finally, interviewing potential users of a system or people involved with targeting and registration is normally not sufficient, as stated data might be different than revealed data [163]. This would require a field deployment, which was not possible.

## B.1. Interview Protocol

The *goal* of these interviews was threefold. First, several interviews were conducted to validate the literature review. Second, interviews were conducted to extract tacit knowledge about the system of interest. Third, to further develop the design, a program of requirements is needed. During interviews, certain questions addressed the elicitation of requirements.

The *response group* was selected as follows. First, within the NLRC a selection of people was made that had affiliations with CTPs, where a mix was needed between field and policy experience. Second, on LinkedIn a query was made on "Cash Transfer Programming". Twenty-seven people received the following LinkedIn invitation which was bound by 250 character limit:

> "Dear [...], I am linking you, concerning my thesis research in the field of blockchain use in humanitarian Cash Transfer Programs, more specific the process of targeting and registering beneficiaries. I'd like to ask you some questions, potentially via a skype meeting? Thanks in advance!"

Once accepted they received a follow-up message which elaborated on the research and a skype meeting was set up. In two cases, due to low internet connectivity a questionnaire was send, which consisted of the same questions yet slightly adapted to filling them in on a digital device. A final overview of all people interviewed can be found in table B.1. Interviewees approached via the Red Cross network, received a similar invitation and follow up message.

To synergize two research projects within the NRLC, the interviews were conducted in collaboration with Tara Stahli from the Graduate Institute of International and Development Studies, in Geneva. Each interview started with the following introduction, in order to set a baseline understanding of what our research was about.

> "**Introduction** Tara is a student in International Affairs at The Graduate Institute of International and Development Studies in Geneva, and Lars is a student in Systems Engineering at Delft University of Technology. We are in the phase of our research that we like to validate some of our ideas and discuss some future directions. **Our research is about** It was born out of the limits with Cash Transfer Programming (CTP) with regard to scale,

timeliness, costs, dignity and data protection. More specific, we focus on the process of targeting and registration of beneficiaries in protective CTPs. In this process, we identified the following challenges: complex local situations (access, connectivity etc), targeting errors can be disastrous, available data is limited, collaboration and coordination is vital and the quality of targeting determines how good monitoring can take place. **Our proposed solution** In one sentence: a (global) digital identity management system. For the purpose of this interview we would like to leave some details open on purpose but to give you a bit of an outline, here are some of the functions we expect it to have:

- Interoperable between all humanitarian organizations doing registration and targeting in a specific area, this would reduce costs/time among the organizations
- Safe and privacy secure data sharing, trust between different organizations would not be an issue (for this questionnaire please assume this to be the case) as you could instantly see if someone misuses the data
- Like the internet, there is not a single owner of the system or of the data
- The system can be integrated with last-mile solutions for payments (digital, cash, cryptocurrencies, banks etc), and focuses on fast transactions

We hope that by now we have given you some sense of what we are aiming for, if not, do not be worried. Your answers on our questions will speak for itself and shall be extremely valuable to us altogether."

Table B.1: List of Interviews

| Name | Organisation | Function | Date | Setting | Aim |
|---|---|---|---|---|---|
| Angelika Kessler | Netherlands Red Cross | FES Advisor, Cash expert | 07-03-18 | Face-to-face | Validate Literature Review |
| Jordane Hesse | Luxembourg Red Cross | Emergency Cash Transfer Delegate | 07-03-18 | Skype | Validate Literature Review |
| Arjen Crince | Netherlands Red Cross | Information Manager | 11-04-18 | Face-to-face | System analysis, design requirements |
| Simon Tembo | Malawian Red Cross | Identity Validator/Community Mapper | 11-04-18 | Whatsapp Call | System analysis, design requirements |
| Wunderful | Malawian Red Cross | Identity Validator/Community Mapper | 11-04-18 | Whatsapp Call | System analysis, design requirements |
| Aneel Ahmed | Concern Worldwide | PM Rapid Fund Program Pakistan | 12-04-18 | Skype | System analysis, design requirements |
| Ajayi Ayobamidele | UN OCHA | Cash Coordinator Nigeria | 13-04-18 | Skype | System analysis, design requirements |
| Kenza Ben Azouz | Mercy Corps | Cash Platform Manager Nigeria | 17-04-18 | Skype | System analysis, design requirements |
| Paula Bil Gaizan | Something Meaningful Consulting | CTP Advisor, Director at Sempo | 18-04-18 | Skype | System analysis, design requirements |
| Rebecca Vischedijk | Netherlands Red Cross | CTP Advisor | 18-04-18 | Face-to-face | System analysis, design requirements |

## B.2. Questions

After the introduction described above, the interviewee was asked for consent on recording the interviewee. Subsequently,the list of questions (see table B.2) was asked in a semi-structured fashion. Once the interview had ended, the interviewee was kindly thanked for his/her time and notified that this interview will be used for the following purpose: quotes to support the storyline of this research, amendments to a stakeholder analysis, technical analysis and institutional analysis, finally to elicit requirements for a future identity management system. Each interviewee will receive a summary of the interview, upon request the audio files can be made available. Each interviewee has two weeks to approve or disprove this transcript, if this was not done it is assumed that the transcript is approved.

Table B.2: Interview Questions

| | Questions and Purpose | | Expected | |
|---|---|---|---|---|
| **#** | **Question** | **Aim** | **Answer format** | **Time** |
| 1 | Could you please briefly state your experience with Cash Transfer Programs? | To get an understanding whether someone has practical and/or theoretical experience with CTPs | Open answer about regions, number of CTPs, role, Prevention/Protection/Promotion | 2 min |
| 2 | Could you please briefly state your experience with Targeting and Registration of beneficiaries? | To get an understanding whether someone has targeted and registered themselves or designed the program | Open answer about targeting and registration | 2 min |
| 3 | Was there any type of digital identity system involved? | To see if they already used some digital tools to enhance efficiency | List of digital systems | 1-2 min |
| 4 | In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | To find out what it implies for a beneficiary to have more control over his or her own digital identity, but at the same time be confronted with technology he/she might not be familiar with, which can generate confusion (even if perceived to be 'user-friendly' | Open answer, no direction | 5-7 min |
| 5 | What do you believe will be pivotal factors for the usability (from a beneficiary perspective) of this proposed identity management system? | To find out what (non)-functional application requirements there would be for this system | Open answer, no direction | 5-7 min |
| 6 | Who do you collaborate with when it comes down to targeting and registration? | To get an understanding of who is involved in targeting and registration according to the interviewee | List of organizations/authorities | 3 min |
| 7 | How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | To understand how dependent they are on their environment and who they see as leading stakeholders | Open answer, potential barriers | 5 min |
| 8 | What would you require of the system for it to convince your stakeholders to use it? | To find out stakeholder requirements (self-registration, open/closed, speed etc) | Open answer, potential requirements | 5 min |
| 9 | Inclusiveness with any given new technology is vital. Speaking from your personal or organisational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | To understand if there is a specific segment of beneficiaries that would be more prone to decline the new system, i.e. for whom it would be less usable | Open answer, no direction | 2 min |
| 10 | What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? (i.e. consent of sharing personal data, knowing what will happen with this data, understanding where and how it is stored) | To find out if beneficiaries are willing to place trust in a decentralized network rather than a known and tangible central institution and/or what may this loss of control trigger in the beneficiary | Open answer, no direction | 5 min |
| 11 | What kind of laws and regulations would apply to such a system in your current environment? | To find out which regulation should be taken in into account when designing the system | Open answer, national/local laws, data protection regulation | 3 min |
| 12 | How would you describe the organizational culture when it comes down to targeting and registration? | To understand what norms there are in their respective organizations | Open answer, safety and privacy | 5 min |
| 13 | Are there any questions you have for us? | | | |

# B.3. Interviews

Table B.3: Interview Angelika Kessler

Angelika Kessler is a Food and Economic Security Program Advisor for the Netherlands Red Cross Society (NLRC). She is one of the few people within the NLRC trained in emergency cash response. She has experience with CTPs in Mali, Nigeria and CAR. These were mainly unconditional cash programs. This interview was recorded on the 7th of March 2018, in a face-to-face meeting at Leeghwaterplein 27, The Hauge.

*So how does a CTP work in practice, from initiation to implementation within the RC?*It goes a lot like it does on paper. The initiation is triggered by a disasters or a forecast of a disaster. Subsequently, we contact the donor to ask for money. The donor required a project description stating the number of beneficiaries we want to reach, the amount of money needed and which specific area. This can take up from one month to a year. With forecast based programs you try to do part of this beforehand, this reduces the time needed for a proposal. This is the ideal situation but in practice forecast based programs have not been fully realized yet. Another solution is the shock response, in which you have a fund that is readily available. This fund is dedicated to a specific type or reoccuring disaster. From hereon the design is finalized and we can further set out the CTP.

*What would be the objective of a CTP with in the RC?*The use of cash within the RC is to speed up the process of providing aid and help people deal with the effects of disasters. Especially with pre-registering beneficiaries the process can be quicker. What type of cash is partly decided by the donor, in general institutional donors are more likely to use unconditional cash. In some cases individual donors provide conditional cash, by sending money for their relatives directly to the merchants. The merchants then let the beneficiaries buy only pre-specified items. these individual donations are actually a significant money stream towards Wester Africa.

*What are the transfer mechanisms used by the RC?*It highly depends on the context. For example in Senegal you could use bank accounts, but in other areas people have no accounts. Mobile money becomes more popular, as they are more secure than cash. However, the mobile networks are not always working well, so the use of hard cash is most common. When it comes down to roles, ECHO determines that distribution of cash should be done by another partner than the one implementing the program. Monitoring and evaluation should also be done by another party. This has created a market for monitoring and evaluation companies for hire. *Do you some use informal payment networks?*I have not seen this myself, but did read bout it.

*So preferably you set up a list of beneficiaries beforehand, at the moment you said there is an ongoing effort to set up a list for the whole of Western Africa, how does this process work?*You either go to the authorities first and then go down to the village chief. Or if you do not trust the authorities you directly go to the village chief. You then target and identify people using volunteers, the community and authorities. It is very important to have the communities participate, they need to be sensitized for CTPs, in order to establish social acceptance. Based on criteria set beforehand and criteria set with the community or village chief you can identify the people that are eligible. This also helps with social acceptance. For identification we use a list with a photo, biometrics, ID card (if available) and phone number (in case of mobile money). You need enough data to establish that people who receive aid, do that in their own name.

*What are the main disadvantages of the current approach, what can be improved upon?*The tools are all there, the application is known but the learning process is long. It just takes time, to collaborate with third parties and teach your volunteers. Combined with British RC, a program is developed on how to be cash-ready. Which software, how to do biometric photos etc etc. You need to work with the environment, low connectivity, no internet, evacuations. This is difficult. Forecast based emergency aid, makes live much easier. In 5 to 10 years we might have a good working forecasting.

*So am I correct that there are a lot of complementary programs and organizations that work in the same affected area? How does this work?*Via a coordination process. This is not easy, and usually there are gaps and overlaps. Here also, if you prepare on beforehand, you might be able to make sure that there are no gaps or overlaps. Timeliness is a pivotal factor, the earlier the response the more efficient it will be. Another pivotal factor is complementary programs, they have to be coordinated to. As collaboration is difficult, for example on beneficiary lists, this could be improved upon. Beneficiary lists are personal data and protected by data regulation so you should not exchange that. On the other you should, as it enables more people to be helped by the time and costs saved.

*I read a lot of people are unidentified. Is this a problem in the field*Yes, this is a problem. Even if they have a passport it could mean nothing. Some passports/IDs are clearly fake, people went to the village chief and asked for a new passport. They are now 10 years younger. Biometric data therefor helps a lot. But you need to train people on how to take biometric data. Then you also need to coordinate this, as a bank might have other regulation about biometric data than the humanitarian organization. Example; RC asks for 2 fingerprints, the bank asks for 10. Then it will take more time at the bank where the cash is deposed in their bankacccount, they will have to wait more etc. Another challenge is that there are villages where 50% of people have the same surname, some have the same first name, the same fathers name but only a different name for their mother. Identification becomes an obstacle then. You make a spelling error and it becomes an other person.

*All this data, is it safely stored?*Not always that safely, it is stored on a computer and that computer has a passport. That's it. People change from their mission, is the data than deleted from someones personal computer? Or is it only stored on the project computer? There is definitely exchange which should not happen.

*In general, what is your vision for these projects? 80% is the goal of humanitarian aid spend? What do you think is feasible, and what is necessary?*We are going through a fashion phase. Many things can go easier than with in-kind, while we do in-kind distribution we usually harm the market. On the other hand when we only do cash, and there is a product missing than we do something wrong as well. We should combine them. So when the fashion phase is over, we can think again and balance how much CTP is needed and how we need to accompany CTPs with in-kind aid.

Table B.4: Interview Jordane Hesse

Jordane Hesse is an Emergency Cash Delegate, currently affiliated with the Luxembourg Red Cross. After a short introduction on the research project, I explain to Jordane that the goal of this interview is to validate some of the results of the literature review.

*What is your experience with CTPs?* In Nepal I did two projects. The first was an emergency response where we distributed 150$ to about 40.000 households and the second was a seasonal program where we distributed 100$ to 5300 households. All distribution was done via cash-in-envelope, which was a very convenient option. There was a well established local market, where the traders were also personally involved with the mergency. We found that the affected people are very resourceful in re-establishing their local markets and communities.
In Haiti, I contributed to a livelihood program with cash. The decision for cash was made because we could not determine wat goods to give. Most beneficiaries in the program were farmers, decisions on which tools and what seeds were dependent on how their farms were located. The set-up of the program took too long, which was a disappointment as we missed the planting season because of it. Payments were done through a remittance company, which was contracted on IFRC conditions. This was partly the reason for the delay.
I also assisted in a cash program in Madagascar, in which donations came from the European Union. Here we used mobile money for distributions, which each participant witdrew for physical cash within two days.

*In these programs, what kind of steps do you take?* We use the cash toolkit of the IFRC (RCMcash.org). This is our bible, I know it by heart. I helped developing it with the IFRC and American RC. There are five main steps, the IFRC picked all the best practices from the field and translated these into templates and sub-step. I also draw some information from the CalP toolkit. They roughly have the same steps, and in their sub-steps they refer to best practices within the entire humanitarian sector.

*How does targeting and registration go in practice? What approach do you take?* This is very complicated and one of my main challenges. We always try to work inside the available cluster, where we divide the work between organizations and try to map who works were as to avoid duplicate efforts. Once an organizations is designated to one area, you have to find out where the worst damages have occurred. Depending on the available time you can have a detailed or more generic set of of inclusion criteria. Then local volunteers go into the field to target beneficiaries, there is a risk here as local biases exist.

*So in your case, who determines these vulnerability criteria?* Most of the time they are the same. Elderly and disabled people, pregnant women, families with more than 3 or 4 children or single women with children. These are like the top four categories we target. In some cases the donor may exert influence on these criteria, but as an IFRC employee you also have a mandate to educate your donor. Not everything is possible, as from your office it is very hard to see what is possible in the field.

*What I was wondering, what are problems you come across with targeting and registration?* Inaccessible areas, lack of time, weather conditions and the coordination within a group of volunteers. *How about missing ID's?* I did not face this issue at large, as we regularly work together with local authorities and such that can provide some sort of lists. One example is that we grouped together community chiefs, priests, local journalists and schoolteachers, to let them discuss who is to be included and who not. This form of triangulation aims to mitigate corruption, but this can still happen.

*What kind of transfer mechanisms have you been using?* So in Nepal, cash-in-envelope which worked very well. It came natural to beneficiaries on how to use and protect their cash, and as safety was not an issue, it was the ideal solution. However, when you are not in a safe country it becomes difficult. You need remittance companies, banks and mobile money. In Madagascar we used mobile money because people were used to it, unfortunately this means you have share data with a mobile provider and oblige people to register with this provider. I find this unfair. In Haiti we used a remittance company, where we also needed to share data with. Remittance companies provide flexibility as they have mobile distribution points, but you pay for everything. It is a difficult trade-off, but in the end you make it because you want to distribute the cash.

*How do you determine the amount?* Normally we do a gap analysis, where we try to find out what people have lost and aim to (partly) correct this loss.

*Based on the targeting and registration mechanisms, what do you think are the biggest improvements to be made there?* There is no ideal targeting method, it just does not exist. So for me the triangulation is a good one and find the best people to rely on. I understand it opens the door for corruption, this is unfortunately how it is. *Could it be improved if there is one interface or one system that all organizations in the system share?* Right now we use more and more tablets, to register data and access data. This helps us, especially compared to paper-based systems. But sharing with other organizations, I have never seen it really. Because everyone has its own methods and workfield. *So how do you monitor these CTPs?* You can monitor from the beneficiary side, the market side or the third-party side.

Table B.5: Interview Arjen Crince

| Questions | Answers |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | Red Cross run cash based assistance program in Nigeria in a situation of armed conflict. Was involved in setting up and delivering physical cash to beneficiaries |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | Was not directly involved in targeting and registration.Volunteers went to those houses that were,pre-identified and pre-selected by the community leader/local chief as being most affected/most vulnerable and by means of questionnaire gathered personal information of those families. Contrary to the beneficiary registration, cash distribution happened more centralized, i.e, people had to sometimes travel to receive physical cash, which apparently posed an obstacle, as up to 90%of the people did not show up (but money was handed out to trusted people who picked it up for them). How did validation take place of those beneficiaries who did not have an ID? In general, "you just have to trust them" (peer-to-peer trust system). One of the issues was the feedback loop, i.e. validation was not sufficient, not enough interaction with volunteers who gathered information (eg. beneficiary registered 35 people in their household and during cash distribution they mentioned a number of males and females within their household that did not add up to the initially mentioned number.) But validation/ cross-check could not always be done, as it slows down the overall process of cash distribution, which then raises security issues. |
| Was there any type of digital identity system involved? | People were registered by taking pictures of their face, filling in Koboforms and providing identification number (if available). Those without means of identification (ID), were provided a Red Cross identification card. Kobo tool was used only by trained volunteers who aided the beneficiary in registration. One of the issues was language, i.e. kobo forms were in English only and volunteers had to translate questions themselves into local language, which implied non-unified language and potentially differing answers from beneficiaries. |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | Usability: Believes in concept but sees practical obstacles: Humanitarian organizations themselves,i.e. people within organization will have to change their mindset, not actually volunteers themselves, but for example branch secretary (will loose some of their role and will stop change), Internet connection (more troubles in armed conflict than with areas of natural disaster which can be better prepared and can better track movement of people), self-registration (urban vs. rural, young vs. old). |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | The government needs to be taken into account; the government can make it or break it, (apart from countries where there is hardly an government-presence, i.e. Yemen). Government may take advantage of those receiving aid, eg. In form of taxing beneficiaries who have received aid money. Beneficiary perspective: If money is involved (now or in the future) then "all would register, that would not be the issue, but keeping it up to date is the most difficult part (...) when a baby is born, or when someone gets lost or dies how to keep it up to date? (...)if you can't log in, you can't de-register" (Signing in regularly may be difficult for individuals). Registration acceptance will differ per country, per racial group and will also depend on the government. Beneficiary hesitance when providing personal data? Not that he heard of, because i.a. it was linked to cash and the message came from local volunteer (who was backed up by local community leaders) in local language. Acceptance high (up to 100%) if proceeded in this way. Issue: Assumes that potential doubts are not voiced due to fear of community leader. Did receive complaints that people perceived themselves as being eligible for aid but were left out because they were not the favorables of community leaders. |
| Who do you collaborate with when it comes down to targeting and registration? | Bank, local agents from bank (Money flow: money travelled from Geneva to London to Abudja,then to local branch of a bank and then local bank gave it to local agent who drove to point of cash distribution). Hardly any interaction with other International organizations (IOs) due to the scarcity of IOs in the area at the time. Joint approach of IFRC and ICRC (first time ever collaboration between the two in one area on the same project). |
| How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | Local volunteers would love technology; but some people knew little to nothing about technology and were also afraid of it (until they got to know it better). Access to data and access to internet, limited to some areas. Beneficiaries: "They don't care as they understand it. Whether they keep a paper (which they will loose to 90%) or if they have something digital (they will need a PW or similar and a paper to write it down) does not really make a difference". Norm to store paper-based document (e.g. ID)? People in the villages usually not," they do not understand the concept of keeping data up to date. If you register them once, they would do that, if you would say you have to log in every month (...) unless there is somebody to help them with it, they will never do it." |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organizational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | The elderly people would struggle most, i.e. elderly people in villages without any connection. |
| What would you require of the system for it to convince your stakeholders to use it? | |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | "They don't think about it. They don't understand the concept and they don't understand the value of data. But I guess it's the same here; what people put on Facebook they don't understand". Lars: What would you need to convince them to keep their data up to date? It's not about convincing them, they don't grasp the concept, how to keep it up to date is to send someone there to help them keep it up to date. But they need to get something for it, i.e. an incentive." By not grasping the concept is in the rural areas. In the cities the volunteers can be educated to perform the tasks and grasp the concept. |
| What kind of laws and regulations would apply to such a system in your current environment? | None were taken into account; unaware of national laws but tried to keep to Dutch standard on data, responsibility and data laws on a theoretical level. On a practical level, information had to be stored on a few computers (which ideally would not be done). If you want to bring aid, you want to focus on bringing aid, and not loose time by focusing on first getting to know the laws. But there were talks to local community and governor before aid was distributed; but in those talks the data responsibility were not brought up. None of the people registered (in this particular case) would probably ever come across their information on any website, so they would never complain, i.e. they would not know how/where to complain; they do not know what to do about it. Should feedback be incorporated into the system? Feedback should be separated from the system itself, i.e. they should be able to call a number and complain about it or going to seek feedback actively in person (people may be afraid to complain publicly) How about data sharing with banks? Only paper-based data was shared (only name and amount of money distributed) |
| How would you describe the organizational culture when it comes down to targeting and registration? | No consent was asked upfront to further use data (ignorance rather than deliberate choice); i.e. it was not done in a systematic approach, not explained well enough to the volunteers in the field. Beneficiaries were told that data was only used for their specific project. Data was not re-used as far as he knows. If you would implement another cash transfer program, would volunteers go into the field and register beneficiaries the same way as previously again? Yes, also because the beneficiaries would change, of course. Only those were registered and were identified as beneficiaries. –>Again, issue of 'up-to-datedness', especially when using data to build queries. |
| Further comments: | Obstacles: People can take advantage of blind, old, vulnerable people.<br>There needs to be a possibility to register people, i.e. if they have to travel<br>to an area with internet connection, this could be a problem.<br>"Staying updated": What if during a situation of armed conflict there<br>is no access to internet for over a year and a child is born during this time,<br>how can information be updated, registered? (Lars–>We need to consider if<br>self-registration is the full way to go, or is there still a need to go into<br>the field? –>It is very context based<br>Does not believe it to be realistic that a whole villages moves to another<br>village to update their online data. (In essence only needs to be done when<br>there is a change in data?)<br>Within a community there must be an incentive for people to keep their data up<br>to date, but this incentive is not sure yet. |

Table B.6: Interview Simon Tembo and Wunderful

| Questions | Answers |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | Based on the criteria of flooding; the local Red Cross is given a list of areas under the flood extense zone (issues of flooding). Beneficiaries were already selected by the government beforehand; the Red Cross Staff then visits these communities (geo-locating with help of volunteers who guide them to the affected households) in order to 'verify' that these households indeed meet the criteria provided by the government and at the same time to be better prepared for future flooding (eg. to make sure these beneficiaries are evacuated). |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | Not involved in the registration of beneficiary. They are given a list of beneficiaries provided by the government (government selects beneficiaries according to the flood extense zone). The list is provided to the Malawian Red Cross by the government; The people on the list have an identifier to identify themselves. Those who do not have one are identified by another means (not aware to interviewee?); people without official ID are not excluded. |
| Was there any type of digital identitysystem involved? | Lists are provided in excel and exchanged via email, the lists are then printed and taken with them into the field for validation |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | Question not asked due to nature of conversation |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | Question not asked due to nature of conversation |
| Who do you collaborate with when it comes down to targeting and registration? | Working with government entities; disaster risk management and social cash transfer. No collaboration with other International organisations. Collaboration with volunteers (who guide the Red Cross staff to the affected people). |
| How would your stakeholders (local authorities, volunteers, headquarters of your organisation, donors) respond if you introduce this system? | Question not asked due to nature of conversation |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organisational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | Is there one group of people that gets left out often? Some people may lack only a few percent to qualify. No specific group that is being left out, but eg. Elderly and women have an advantage, i.e. they have a higher possibility of being on the list of beneficiaries as they are for example not well/fit enough to work. |
| What would you require of the system for it to convince your stakeholders to use it? | Question not asked due to nature of conversation |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | Are people to happy to give information? So far no hesitancy of the people (the people know that they are Red CrossStaff) |
| What kind of laws and regulations would apply to such a system in your current environment? | Question not asked due to nature of conversation |
| How would you describe the organizational culture when it comes down to targeting and registration? | Question not asked due to nature of conversation |
| Further comments: | There were some beneficiaries complaining to be left out |

Table B.7: Interview Aneel Ahmed

| Questions | Answers |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | Nine years of experience in cash programming in a number of disaster-prone areas in Pakistan (mainly flood and drought response) with a number of international organizations (Concern Worldwide, Pakistan Red Crescent Society), Catholic Relief Services, Premier Urgence International and Government Departments). |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | Unique IDs were provided to those beneficiaries who don't have identity cards. This approach allowed us to reach the most vulnerable communities who already lost almost all assets in disasters, at the time of cash distribution, details of such program participants were shared with Mobile money transfer companies for smooth distribution. The codes were distributed to beneficiaries on a paper (which were kept safe by the beneficiaries). |
| Was there any type of digital identity-system involved? | No digital devices used for registration, data was collected on paper and transferred to a centralized database (excel sheet) which was stored on a computer. |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | {Question was re-phrased slightly} A lot of time is spent on identifying and registering people (20-40 days); through a digital system time can be saved. What would people need to self-register on a digital device? Educated people can register themselves easily, but majority of people in affected areas lack education. Risk in terms of favoritism if they cannot self-register and are dependent on foreign help. |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | Question not asked due to nature of conversation |
| Who do you collaborate with when it comes down to targeting and registration? | Collaboration with other international organizations (drought-clusters) in targeting and registration; data was shared among them via excel sheet stored on a computer. Collaboration also with banks and mobile phone providers in cash transfer, as well as with a number of district departments. Who has the formal power? The district administration. |
| How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | Currently there is no digital database on government level; predominantly paper-based database (if any at all). |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organizational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | Educated vs Non-educated |
| What would you require of the system for it to convince your stakeholders to use it? | Question not asked due to nature of conversation |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | Are there issues with consent? Do you ask if there data is allowed to be used? Vulnerabilities is a big concern. Not hesitant to provide personal information. Community meetings are conducted prior to the registration process; the procedure is explained to the community in advance (scope, criteria, information on organization, modalities of transfers), happy to share information in these situations. In recurring situations of cash based assistance, are (the same) beneficiaries re-registered or can data be re-used? Usually the same data is used, i.e. it is re-verified. |
| What kind of laws and regulations would apply to such a system in your current environment? | No answer was provided |
| How would you describe the organizational culture when it comes down to targeting and registration? | How is personal data being handled? "We tell them [beneficiaries] that data will only be used for the humanitarian sector and that we do not share this data with any other persons, also not the government, we usually only share the data with the line (district) department." People do not have a concern with this [if they are told that their data is being used only for the humanitarian sector and for this specific project]. |
| Further comments: | Access is a big issue, eg. Long travel time to banks<br>Limited mobile access (issue in transferring money); eg. Maybe only 5 of 100 people would have access to a mobile phone<br>Most people do not have identity cards. How did you deal with that? Thumb impression was required (challenge because the then taken thumb impression, did not match that one on the identity card).<br>Time can be saved through the means of digital tools in registration |

Table B.8: Interview Ajayi Ayobamidele

| Questions | Answers |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | CTP started in Nigeria in 2013 for flood-affected communities, however the coordination of cash coordination was destructed mainly due to Boko Haram movement; 2014-2015 humanitarian committee thus shifted its attention from flood to armed conflict. 2015-2016; issues of cash was reactivated (once the humanitarian sector was able to gain access to Boko Haram "captured" areas in the North Eastern part of the country), national-level cash response activated in 2016 (most of the involved staff was on short term assignments, hence cash coordiantion was not strong and cash working group was not 'unified'. Currently, cash distribution is used extensively in the North-East in the sectors of food security, education section, early recovery, shelter, health. |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | Question not asked due to nature of conversation |
| Was there any type of digital identity system involved? | Different organizations come up with different means to register and target beneficiaries (internally displaced persons) mostly through biometric data registration (introduced in 2017 due to issues of double registration, IDPs who register with different organizations). How did beneficiaries react to this new technology? No negative reaction, there was a lot of sensitization to explain the process for being biometric registration and also to understand the benefits o the registration. With the support of community leaders and leaders of IDPs the partners were able to do the registration using biometric mechanism. Partners were able to clearly identify the beneficiaries for humanitarian intervention. Beneficiaries were not hesitant to provide data? No they were not hesitant, as there was sensitization at the beginning, and the community leaders really helped to communicate information to beneficiaries |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | Question not asked due to nature of conversation |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | Organizations responding in the same regions shared data among each other by means of MOU (memorandum of understanding), so if a new system is introduced, the humanitarian committee will be a little 'hesitant (?)', unless the new system can be integrated into the already existing mechanism that is currently being used for registration, monitoring and reporting. |
| Who do you collaborate with when it comes down to targeting and registration? | No cluster-approach. It is mainly a 'sector-approach'; 33 local donate areas.,26 organizations (UN, local NGOs, Red Cross movement). As per September 2017 13.4 million dollars has been dispersed through cash programming; 200.000 people reached. In terms of progression, every month trend analysis are conducted to examine progress (in terms of use of cash); based on trend analysis number of beneficiaries increased 82.000 to 200'000 households (April to December 2017). Cash disbursement grew from 6 million dollars to 13 million dollars during that time. Trend analysis of local government areas (same time period); coverage area moved from 13 to 33, 290 million dollars is to be expected to be dispersed in 2018. |
| How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | Question not asked due to nature of conversation |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organizational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | We cannot rule out that everyone gets included; re-registration has to happen if some people leave the country and return again. Issue of people who have to re-register? Yes, of course, especially those who are moving back to habitual place of residence, they have to be registered in the new location. |
| What would you require of the system for it to convince your stakeholders to use it? | Question not asked due to nature of conversation |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | See question 3 |
| What kind of laws and regulations would apply to such a system in your current environment? | Interviewee does not have much information on Data protection regulations. But mentions that telecommunications existing laws of privacy/identity of people using the service of telecommunication services (KYC) are sometimes referred to; if people do not have an ID card? Not be able to register without passport. Are there a lot of people how do not have a passport/ID card? Yes of course. Are they excluded from CTP? They are allowed to use their national ID card or are issued a SCOPE card (i.e. pre-paid cards) (International passport = travel document, National ID Card = identification as a national of Nigeria). |
| How would you describe the organizational culture when it comes down to targeting and registration? | Question not asked due to nature of conversation |
| Further comments: | How to scale up CTP, timeliness of response, data protection, issue of targeting and registration, key challenges including access, connectivity, coordination, sharing of data among different partners, issue of trust between and among different organizations when it comes to data sharing, digital payment/payment mechanism. Biggest challenges when scaling up: Security, Access (related to security), markets (no markets in some locations, no financial service providers), people's perception of cash (cash might bring about dependency), quality of intervention, issue is the capacity of partners to implement cash (usually low capacity), issue of multi-purpose cash grants (cash for purposes across specific sector), problem of cash coordination (which agency should coordinate cash?) A lot of movement of people due to conflict, i.e. issues of tracking people |

Table B.9: Interview Anonymous

| Questions | Answers |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | I have experience with CTP in xxxx where a lot of the people were refugees and unbanked. In xxxx there was a platform where they could actually distribute credit cards, people could then go to the ATM or the store to retrieve/spend their money. Then I moved on to xxxx, where we use a cash platform for the distribution of food and cash vouchers. I had no experience with this, but it kind of comes on its own with the available technology. Our organisation decided to move away from XXXX, so a new platform system had to be brought into place. My role here was very operational in the beginning, by creating the tender criteria and now it is more about rolling it out. All of this of course involves a lot of discussions about data protection. |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | Right now I am actually in the field, in xxxx I was also in the field. The workflow here is as follows. We have a team of 6 to 15 enumerators, that are staff or hired. We go house by house, register potential beneficiaries and ask if we can look in and around the house. We register the information in our tablet and scanner, which goes straight into the humanitarian information management system (XYXY) system. *Could you briefly state how the response was of the beneficiaries when you came with the new system?* This is a very new system, we have only been piloting with it since 2 weeks. But, we work in the field where we have been present for three years now, so people trust our organization. We ask for their consent and inform them about what it means to give consent. We also ask for feedback, but since it is not truly anonymized feedback it can be difficult to get a full picture of the satisfaction. But overall we have a very good relationship with the communities. I think though we can empower them even more when it comes down to giving out their data. |
| Was there any type of digital identity-system involved? | As stated there is a nation-wide humanitarian information system used by our organization: XYXY. Alongside XYXY, our organization has its own cash platform. In this platform all the beneficiary data is stored and all of the humanitarian programs are stored in there. When tendering for the cash platform we realized these systems should be integrated. The cash platform is not owned by our organization, but we do own the information that has been put in to it. Then there is also a third party, who delivers biometric scanners (non-profit). They deliver their own biometric scanner, that is very robust and field work proof. Their services are the only ones that comply with GDPR so far, that I know of. *So where do you store this data?* This all stored in XYXY, where we have the advanced plan for extra data security. Then this data is accessed via encrypted channels through the cash platform were only the minimum viable data for the cash transfer is requested (so name, age, etc, biometric-generated identified – GUID "Global Unique Identifier" – and no fingerprint image). So when the cash platform is hacked it is impossible to recreate the biometric identity. Deciding who is included happens in XYXY, where all humanitarian program beneficiaries in xxxx are registered in. As we registered potential beneficiaries we execute the inclusion criteria in XYXY and receive a final list of included beneficiaries. These beneficiaries are given a NFC card by our organization, which at the moment are only being used for cash transfer. However, they have multiple wallets and could be used for other purposes. On each card a picture of the card holder and a next-in-kin is showed, the card also holds both of their biometric data sets. |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | *Rephrase the question: Do you think a future system using self-registration would be feasible?* We have not thought about it in that way, we are not innovating in that part at the moment. This something that might be better suitable for a specialized company. |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | Criteria that were found to be of importance to our team and external organizations were user-friendliness, ease of transaction, beneficiary data protection etc. |
| Who do you collaborate with when it comes down to targeting and registration? | *Would it be possible for them to use these cards for other programs outside of your organization?* This has not been decided yet, we do not see this happening very soon. As stated before collaboration is often difficult for a variety of reasons. One, most of the actors are simply not working in the same location with the exception of big IDP camps. Second there is the aspect of trust, not all humanitarian organizations are open for collaboration. In my opinion, for this to happen it would require a move from headquarters who might not be actively working on this as they have other strategic issues to attend to. Third, awareness for data responsibility still needs to grow, as not every organization is working on the same level. So organizations might have to work on their own data regulation before collaborating. Once again, this is my personal statement. |
| How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | I think they have different priorities. There are definitely upsides with regards to time and costs, but it will be hard to get a push from above which is needed to roll out such a system. So they would have to have a need. |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organizational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | So one of the criteria for the system we now have, was that it would be flexible. So for every beneficiary, if they refuse or are unable to provide biometrics (for example they have no hands, have henna on their fingers etc), they can still be registered to receive a card. In the system it will then be designated that in further contact, the beneficiary will never have to share his/her biometrics but will automatically be asked for a pin code instead. These pin codes can be released to the beneficiaries upon request, there is one person that has access to these pin codes which are stored inside the cash platform. So we try to be as inclusive as possible. |
| What would you require of the system for it to share your data for other stakeholders to use it? | They would have to be as professional and understanding of data protection as we are. |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | *Do you think that from your perspective they fully understand what is meant by informed consent?* ? No I do not think they really know in the area we operate, but there are areas in xxxx were they do fully understand. It would be difficult, maybe even unrealistic, to expect them to have fully informed consent. Even by the processes, it would be hard to do this. However, in xxxx they were very weary of their data. Especially, providing it to UN bodies as they thought it might have further consequences for request for asylum. Lets say in general, we tell we will not share the data to any other organization and then it comes down to trust. Once again, these are all my personal statements. |
| What kind of laws and regulations would apply to such a system in your current environment? | These are parts of the criteria, but this is something I do not have a lot of expertise on. We work together with people with expertise to cover this part. What I do know is that the GDPR covers most of the national regulations, as it is very extensive. |
| How would you describe the organizational culture when it comes down to targeting and registration? | I would say our organization is very strong in data protection and regulation. We actively seek collaboration with other organizations, we run security assessments, so yes this is definitely something that we find important. |
| Further comments: | *What would we the biggest challenges for this system for the next 5 to 10 years?* Practical issues have to be fixed today, as it could damage the reputation of our organization and the programs. The biggest challenge would be on how to be accessible for feedback, especially when we are talking about locations that have very limited access. So we would need an even more expansive hotline, where people can always call to in any language that is spoken in xxxx. We would need a clear communication strategy at hand and make sure that each person providing feedback is notified.<br>*How would you deal with updating information?* This is great with XYXY, we can very easily update information through their forms. Also it depends on what kind of information needs to be updated, if it is information that could change the monthly cash transfer then it should be updated. But this of course depends on the criteria set by a humanitarian organization. They have tried to collaborate on this, but so far there has not been a uniform take on it. If something happens to one of the card holders, then they would have to report it to their community leaders or to our organization. The forms can than be changed, and a new card is issued or modify the account via the cash platform.<br>At one point we were thinking of using the IOM data, as it is quality data, but then we heard from other NGO's they were not satisfied with it so we decided not to. |

Table B.10: Interview Rebecca Visschedijk

| Questions | Answers |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | I have experience with a CTP in Nigeria. The operation was designed to provide support to the Nigerian Red Cross Society (NRCS) in its response to the protracted humanitarian crisis in the North East of Nigeria where some 4 million people are experiencing acute food insecurity and 1.9 million people have been displaced by the conflict and need immediate humanitarian assistance So with Boko Haram? Officialy within the Red Cross we refer to them as armed opposition group, but made no inference to their position to comply with our humanitarian principles. Then I was in St. Maarten where we had a cash-voucher program, where people were handed out paper vouchers with a barcode which they could retrieve food with in a supermarket. |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | I was involved in the registration. I arrived as a third round in the response, so my task was data cleaning of people that had been identified and registered in Nigeria. On St. Maarten the criteria for targeting were already set, I had a very minor part in the targeting. The community councils were trained and they then identified the people who were elligble according to our criteria. The lists were then given to us, upon which we went out to validate these people. In this phase new people were identified as well, so in that way I did some targeting tasks. *So how you do validate?* You can ask questions, gut feeling (you can not say you are not eligible based on that feeling, but it helps in the process), validation methods within the affected area (so community councils, government lists, passports if available etc), post with their address on it, but also RC identification numbers if people do not have formal identification. It depends on the criteria you set. In Nigeria, we took two or three months to really set up a process within the community. Make it a democratic process and set rules for inclusion, set up a feedback process, monitor that the community council reflects the community etc. This was also noticeable in the approach. In St. Maarten where there was no community approach, there was a lot of uncertainty which resulted in chaotic situations at the distribution points. While in Nigeria, which was less secure and in the middle of armed conflict, the distribution went smoothly. *What type of feedback systems did you have?* A hotline, which could be called, it was not always operational. And because we were within the community, we retrieved a lot of feedback through our relationship with the communities. *How important is this community approach and could you use a different one?* It is important for acceptance in the communities. You could not do that but then you need to highly invest in your communication. *Could you foresee a method where a humanitarian organization would not have to go into the field for validation*? No, also I do not know of other organizations doing this in a different way. |
| Was there any type of digital identity-system involved? | We used KOBO and tablets, this gets uploaded to a UN server from which you download it into an excel database. Not necessarily that safe, some elements of what is stored on the UN server were accessible via a URL. |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | *How were beneficiaries responding to you asking for PII?* This was an eyeopener for me. In Nigeria, where there is a low literacy rate and people are limited in their data literacy. For example, people could not write so they just gave a fingerprint because they could not do an autograph. So yes we asked for consent, but I do not believe they truly understood what consent meant. *What would be the pivotal factors?* People need to understand, communication is key! The idea I have is that you can talk a lot to people but in the end they only understood the Red Cross is here, I get money if I give them information. Also training, and it should be as straight forward as possible and easy-to-use. |
| Who do you collaborate with when it comes down to targeting and registration? | *Did you collaborate with other organizations doing CTPs in Nigeria?* Well we tried to, but in our geographical area there were not so many NGO's. Therefore the distance was not worth the effort. *Who did you collaborate with*? A service provider for financial services (a Nigerian bank), volunteers, ICRC, RC Nigeria, IFRC, local RC branches and municipalities and community councils. *Of these stakeholders who holds the most power?* It really depends on the knowledge people have in the field, however ownership and end decisions lie with the National Red Cross Society, thus Nigerian RC. If I could have chosen, I would have made a different decision than KOBO. This decision came from the Nigerian RC. |
| How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | Again, it really depends on the decision makers. At a RC operation it would probably be most important that the IFRC and national society believe in the system. People brought in from outside will probably go with whatever there is. Even a branch of the Nigerian RC can have quite a say in this, so they should also believe in it. *So it could not be that an IFRC can say, from now on we use this system?* No this is not how the RC movement works. Maybe a UN could say this is how we work, and others might follow. So the IFRC can make recommendations, but the decision is made locally. |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organizational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | It depends on the country and how used people are to technology. In Nigeria a fully digital system would not work, so then you would need volunteers for last-mile solutions. Otherwise a big group of people would be excluded. |
| What would you require of the system for it to share your data for other stakeholders to use it? | You would need more standardized data input and each organization looks for specific data. Also organizations would then need to trust the ones owning the database. |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | |
| What kind of laws and regulations would apply to such a system in your current environment? | Personally no, I expect the designers of the CTP program (thus the earlier rotations) to have taken this into account. |
| How would you describe the organizational culture when it comes down to targeting and registration? | In the field, within an international humanitarian operations, I have experienced that people from western countries are more familiar with data responsibility. It is getting better though, more people are thinking about it. Yet, for example if people have a hard time in getting the system running then data protection is not on their mind. |

Table B.11: Interview Paula Gil Baizan

| **Questions** | **Answers** |
|---|---|
| Could you please briefly state your experience with Cash Transfer Programs? | I am doing an evaluation for UNRA for their safety net; they are running a massive cash program (similar to a social protection system). They have massive problems with targeting, i.e. quality and availability of data is a big issue (Trust of information that is coming into the system). Nobody is able to solve this problem at the moment. Having an ID card does not solve the problem of targeting. Data that is being collected to generate an ID is not the same data used for a sophisticated targeting system. Example: To get my passport they asked me a bunch of questions: biometrics, personal identifying to me, etc. but Nobody asked me if I have two children under five, or if I am a single mum, or my credit card debts is so high that I cannot cope every month, etc. I just have an ID. It depends on the cash program, but generally yes, it is very rare to do a blanket distribution of cash. You usually need to know that they need it, i.e. you need to ask them more questions, such as their ability to cope with the risks that they have. There's a difference between finding the people and knowing if these people are who they say they are. For example, MasterCard, ID2020, Accenture & WFP are already working on an interoperable identity, but nobody is tackling the question: Okay now that we have found you, how do we know that we have to give you stuff? To use technology to fix that would be needed. |
| Could you please briefly state your experience with targeting and registration of beneficiaries? | n/a |
| Was there any type of digital identity-system involved? | n/a |
| In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance? | Beneficiaries are people. How hard was it for you to move to contactless payment? It took me a little while, but I managed. Eg, if you go to Nairobi now, there are things happening that I don't even understand. The humanitarian crisis (remote, poor places, in the depth of a war) is never going to change; there are always going to be humanitarian actors operating there, but that is a niche, that is not the bulk of the humanitarian field. The bulk of the money of humanitarian work is in those places where you cannot tell the difference between development and humanitarian; people are above or below the poverty line due to a shock or other causes. And in those places, people have mobile phones. |
| From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? | In reality it is usually driven by time. Being poor and being in crisis takes a lot of your time and your attention. If you make it taxing, every new technology there is always the need to train people, but there is difference between the way you would have to train me and the way you train people in crisis. People in crisis are very resourceful; if you give them something to allow them to build on their capability to adapt, then they will use it. Give people something that is useful for them, if you build something that is only useful for the NGO then you will be passing on the cost of use to the beneficiary and then the beneficiary will not want to use it. If you have a product that is no longer focused on giving people things, but that is focused on creating the right environment for the people to take decisions you are at a better place for the next 10 years than if you only focus on one bit of their experience. |
| Who do you collaborate with when it comes down to targeting and registration? | n/a |
| How would your stakeholders (local authorities, volunteers, headquarters of your organization, donors) respond if you introduce this system? | n/a |
| Inclusiveness with any given new technology is vital. Speaking from your personal or organizational experience, do you think there may be a segment of the beneficiaries that would struggle most with this new form of registration? | n/a |
| What would you require of the system for it to share your data for other stakeholders to use it? | n/a |
| What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? | n/a |
| What kind of laws and regulations would apply to such a system in your current environment? | n/a |
| How would you describe the organizational culture when it comes down to targeting and registration? | n/a |
| Further comments: | I think [our proposed solution with identity managed on a distributed ledger ] is fantastic and many NGO's would love to use it, but I see it as my personal crusade to say that this is not going to fix the targeting error. NGO's have value because they have experienced people that know what to look for (in targeting people) - NGO's will continue to survive if they continue to capitalize on their validator role. That validator can go back into the system and insert subjective information, but that is not reducing the inclusion/Exclusion error as the information is still input by a human.<br>There are other forms of targeting: Community based targeting works really well; for example in Kenya: proxy means testing and community based targeting; beneficiary can self-register and this information gets validated by others (i.e. people get paid to validate information such ash "what is access to electricity?", "is there access to water?"", so you can correlate some of this information to the individual) –> Removing the human would be groundbreaking<br>*Do you think in 5-10 years the human will be out of the loop in the validation process?* The human can either be out or only in, when the human is actually needed, i.e. depending on the context. If enough data points are available (social media, community based targeting, etc.) you will not need the human to verify information of others, but people can self-register. And if you think of progression/better technology penetration then yes (and it will put NGOs out of work really). *There will be an upheaval in the NGO world, as you put them out of work, no?* Well not really, they are already going out of business. Example: Congolese government turns to private sector to raise money rather than to NGO's. If you look at the ways donors are pushing NGO's to operate is to push them to a place where they only have the human when is needed, not as a default. The change is happening, regardless of what is happening in the technology sphere.<br>There is something beyond of what you are trying to do: for your idea I can already name five competitors. |

# C

# Stakeholder Overview

Table C.1: Overview of National/Local Stakeholders

| Stakeholder | Examples | Vision for Targeting and Registration | Key Interests | (Potential) Role | Formal Power | Informal Power | Source |
|---|---|---|---|---|---|---|---|
| National/Local Humanitarian Organizations | National Red Cross Societies,Local NGO's or Humanitarian Organizations | Targeting and registration are essential tools for the efficient and just distribution of cash based assistance and needs to scale up, in order to prevent and alleviate more human suffering | Coordinate locally and carry out disaster response and disaster preparedness | Initiator, local coordinator, CTP focal point, supply of human capacity, targeting beneficiaries, informal registrar of identities | If legally registered in the affected area, they have some judicial power | Significant as the national authorities in which the humanitarian assistance is needed are unable or unwilling to assist their citizens themselves | NGO.org[1] |
| National Authorities | National governments, ministries, specific departments | Targeting and registration may be essential tools for the efficient and just distribution of cash based assistance which prevents and alleviates human suffering | Welfare of their people | Law maker, barrier, data supplier, supply of human capacity, formal registrar of identities, coordinator of existing Social Safety Net | Significant, but depending on the context | Significant, but depending on the context | Assumption that national authorities are pro CTP and have capacity to support |
| Local Authorities | Federal authorities, provincial authorities, municipalities | Targeting and registration may be essential tools for the efficient and just distribution of cash based assistance which prevents and alleviates human suffering | Welfare of their people | Law maker, barrier, data supplier, supply of human capacity, formal registrar of identities, coordinator of existing Social Safety Net | Significant, but depending on the context | Significant, but depending on the context | Assumption that local authorities are pro CTP and have capacity to support |
| ICRC | n/a | Targeting and registration are essential tools for the efficient and just distribution of cash based assistance and needs to scale up, in order to prevent and alleviate more human suffering | Coordinate and initiate disaster response and disaster preparedness | Initiating CTP, CTP Design, Set-Up of Operational Programme, Coordinate and supply human capacity, Coordinate Funding, Coordinate with External Environment, Coordination through Cash Working Groups, informal registrar of identities | Significant by Humanitarian Law | Significant as national states in which humanitarian assistance is needed are often unable or unwilling to assist their citizens themselves | ICRC[2] |
| UNHCR | Shelter provider, protection, camp coordination, camp management | Registration is an essential tool for protection, for the management of operations and for the achievement of durable solutions | To lead and coordinate international action for the world-wide protection of refugees and the resolution of refugee problems | Coordinator of registration, Camp Management, data supplier, supply of human capacity, initiator of complementary programs, informal registrar of identities, Targeting beneficiaries | Limited | Significant in a refugee camp | UNHCR[3] |
| WFP | Responsible for Food Security and/or Logistics | Targeting and registering food insecure communities is the central element of all WFP food aid operations | To eradicate global hunger, poverty and to meet emergency needs | Initiator of complementary programs, informal registrar of identities, targeting beneficiaries | Limited | Significant in food aid | WFP[4] |
| UNDP | Early Recovery | SDG 16.9: Legal Identity for all, including birth registration by 2030 | To achieve the eradication of poverty, and the reduction of inequalities and exclusion | Initiator of complementary programs, informal registrar of identities, targeting beneficiaries | Limited | Significant in early recovery and longer term projects around identity | UNDP[5] [6] |
| OCHA | n/a | Targeting and registration are essential tools for the efficient and just distribution of humanitarian aid, in order to prevent and alleviate more human suffering | To mobilize and coordinate effective and principled humanitarian action in partnership with national and international actors | Emergency Relief Coordinator, Initiator of Cluster Approach | Limited | Significant due to UN resolution | OCHA[7] |
| Military Forces | National Defense, Local Militia, Police Forces | Targeting and registration may be essential tools for the efficient and just distribution of cash based assistance which prevents and alleviates human suffering | Executing orders from their national/local authorities | Peacekeepers, supply of human capacity, security of CTP | Significant, a monopoly on violence, but depending on the context | Medium, but depending on the context | Assumption that military forces are pro CTP |
| Beneficiaries | n/a | Targeting and registration are essential tools for me to receive humanitarian assistance | Personal Welfare | Suppliers of data, receiving cash, local knowledge, feedback | Very limited | Limited | Assuming people want to be registered for help |
| Community Representatives | Local trust anchors, chiefs, counsel members | Targeting and registration are essential tools for my community to receive humanitarian assistance | Community Welfare | Suppliers of data, supply of human capacity, local knowledge, inclusion criteria, feedback | Very limited | Significant | International organizations collaborate with communities for support and local knowledge |
| Merchants | Shop owners, goods distributors | Targeting and registration are essential tools for my customers to receive humanitarian assistance and create demand for my products | To be profitable | Suppliers of data, local knowledge, collaborators with CTP | Very limited | Limited | Assumption that they are able to meet demand |
| Service Providers | Cash distributors, mobile operators, remittance companies, banks | Targeting and registration are essential tools for my services to deliver humanitarian assistance for which I receive payment | To be profitable | Suppliers of data, local knowledge, collaborators with CTP, supply of human capacity, | Very limited | Limited | Assumption that they are available in the affected area |

Table C.2: Overview of International Stakeholders

| Stakeholder | Examples | Vision for Targeting and Registration | Key Interests | (Potential) Role | Formal Power | Informal Power | Source |
|---|---|---|---|---|---|---|---|
| International Humanitarian Organization | Oxfam Novib, Islamic Relief, Save The Children, Cordaid, Christian Aid, IFRC | Targeting and registration are essential tools for the efficient and just distribution of cash based assistance and needs to scale up, in order to prevent and alleviate more human suffering | Coordinate and initiate disaster response and disaster preparedness | Initiating CTP, CTP Design, Set-Up of Operational Programme, Coordinate and supply human capacity, Coordinate Funding, Coordinate with External Environment, Coordination through Cash Working Groups | Limited by national law | Significant as national states in which humanitarian assistance is needed are often unable or unwilling to assist their citizens themselves | Humanitarian Coalition[8] |
| International Authorities | European Union, USA, Nation States | Targeting and registration are essential tools for the efficient and just distribution of the funding we provide humanitarian organizations, which prevents and alleviates human suffering | To realize their strategic ideas by funding projects | Providing high value (multi-annual) funds | Significant with their relations to the affected areas | Significant through UN and other aggregate organizations | Assumption that international authorities will support and fund out of humanitarian principles and for their strategic agendas |
| Development Partners | CalP, HPN, ODI, The World Bank, ReliefWeb | Targeting and registration are essential tools for the efficient and just distribution of cash based assistance, and requires research to develop and improve | To increase the scale and quality of CTPs as a tool for humanitarian assistance | Research on targeting and registration, provide some funds, supply of human capacity for coordination | Limited | Limited, some with regards to spreading knowledge | CalP[9], ODI[10] |
| Institutional Donors | UKAID (DFID), USAID, ECHO Ministries | Targeting and registration are essential tools for the efficient and just distribution of the funding we provide humanitarian organizations, which prevents and alleviates human suffering, and enables feedback on our funding | To realize their strategic ideas by funding projects | Providing high value (multi-annual) funds, research on targeting and registration | Significant | Significant, looking at funding and knowledge | Dochas[11] Mango.org [12] ECHO[13] |
| Individual Donors | n/a | Targeting and registration are essential tools for the efficient and just distribution of the funding I provide humanitarian organizations, which prevents and alleviates human suffering, and enables feedback on my donation | To show altruistic behavior | Providing low value (periodic) funds | None | Very limited | Assumption that individual donors want to do good |
| Private Organizations | Corporates, social enterprises | Targeting and registration provide options for us to show (Corporate) Social Responsibility, through which humanitarian organizations can prevent and alleviate human suffering | To be profitable or to achieve a social good | Supply of human capacity (e.g. data scientists), supply of materials | None | Very limited | Assumption that private organizations have a social status and engage in Corporate Social Responsibility, yet they need to remain profitable |

# D

# Overview of Alternative Systems

Table D.1: Alternative systems

| Name | Website | Open source | Sector | Concept | Stage | Blockchain | Type |
|---|---|---|---|---|---|---|---|
| AID:tech | https://aid.technology/ | No | Finance | Financial inclusion, transparency of international aid delivery | Pilot | Ethereum | Private |
| BanQu | http://www.banquapp.com/ | No | Finance/identity | Financial inclusion, transparency of international aid delivery, building digital identities | Pilot | Ethereum | Private |
| BlockBonds | https://blockbonds.io/ | No | Finance | Mobile borderless banking application | Live | Multichain | Private |
| BlockStack | https://blockstack.org/ | Yes (GPL v3) | Data storage | Digital identities for digital purposes | Live | Bitcoin | Permissionless |
| Building Blocks | http://innovation.wfp.org/project/building-blocks | No | Finance/identity | Cash for food aid | Pilot | Ehtereum | Private |
| Civic | https://www.civic.com/ | No | Identity | Secure identity platform based around biometrics | Live | Ehtereum | Private |
| Dock.io | https://dock.io/ | Parts | Identity | Secure identity platform and sharing | Live | Ethereum | Permissioned |
| Helperbit | https://app.helperbit.com/ | No | Finance | Peer-to-peer donations | Live | Bitcoin | Public |
| IBM Identity mixer | https://www.zurich.ibm.com/identity_mixer/ | Yes (Apache 2.0) | Identity | Attribute Based Credentials for online identification and verification | Live | Agnostic | Agnostic |
| IDbox | https://www.idbox.io/ | No | Identity | Hardware and software for creating secure digital identities without electricity, internet or smartphones | Conceptual | Ethereum | Private |
| IFPS | https://ipfs.io/ | Yes (MIT) | Data storage | Peer-to-peer hypermedia protocol to make Data storage faster, safer and more open | Live | Agnostic | Agnostic |
| IRMA | https://privacybydesign.foundation/irma-uitleg/ | Yes,(Apache 2.0) | Identity | Attribute Based Credentials for online identification and verification | Live | Agnostic | Agnostic |
| Microsoft U-prove | https://www.microsoft.com/en-us/research/project/u-prove/ | Yes (BSD) | Identity | Privacy protected user centered common public-key infrastructure | Live | Agnostic | Agnostic |
| NLRC | https://tykn.tech/ | Not yet | Finance/identity | Cash Transfer Projects, building digital identities | Conceptual | RSK | Permissioned |
| Proof of Individuality | http://proofofindividuality.online/ | No | Identity | Demonstrate someone has one account within the system, person to person verification | None | Ethereum | Private |
| Sempo | https://sempo.ai/ | No | Finance/identity | Empowers NGOs to rapidly and efficiently deliver cash assistance directly to victims | Live | Ethereum | Private |
| ShoCard | https://shocard.com/ | No | Finance/identity | Identity verification system that works the way consumers and businesses need it to for security, privacy, and always-on fraud protection | Live | Bitcoin | Private |
| Sovrin | https://sovrin.org/ | Yes (Apache2) | Identity | Permanent digital identities that do not require a central authority | Conceptual | Hyperledger Indy | Permissioned |
| uPort | https://www.uport.me/ | Yes (Apache2) | Identity | Open identity system for a decentralized web | Live | Ethereum | Permissionless |
| Yoti | https://www.yoti.com/ | No | Identity | Attribute Based Credentials for online identification and verification | Live | Hashgraph | Private |
| Zerocash | http://zerocash-project.org/index.html | No | Finance | Protocol that provides a privacy-preserving version of Bitcoin | Conceptual | Bitcoin | Permissionless |

# E

# Expert Validation

For this research expert interviews were used to partly retrieve new knowledge since the use of blockchain and digital identity systems is a new concept [109], and to validate the system design presented in chapter 5. Experts were chosen based on there experience within the fields of digital identity management and blockchain, to validate the technical concepts. Other experts were chosen to validate the social side of this system design, the humanitarian aspect. Unfortunately, there were no experts available with knowledge of both sides. This is a drawback of this expert validation, but due to time-constraints it was impossible to mitigate.

In the table E.1 the experts that were interviewed are listed.

| Name | Organization | Background | Validation |
|---|---|---|---|
| Djuri Baars | Blockchain Lead at Rabobank | Self-sovereign identities and Blockchain | Technical, Blockchain Architecture |
| Arnold Daniels | Co-founder at Legalthings | RegTech and Blockchain | Technical, Blockchain Architecture |
| Sander Dijkhuis | Product Owner at Cleverbase | Trust Service Providers, Digital Certification | Technical, Identity System |
| Vincent Graf | ICT Innovation Officer at ICRC | Digital Humanitarian Aid | Humanitarian Practices |
| Maarten van der Veen | Visionary Lead at 510 | Digital Humanitarian Aid | Humanitarian Practices |

Table E.1: Overview of Expert Interviews

For each interview the audio transcript is available and specific questions based on their background were asked. A general outline of the expert interview protocol can be seen below.

## E.1. Interview Protocol

Experts approached via email were contacted using the message underneath, experts contacted via Linkedin received a more informal and shorte invitation.

> *Dear Reader,*
>
> *My name is Lars Stevens and I am graduating from TU Delft, Complex Systems Engineering & Management. In collaboration with the Netherlands Red Cross and its data team 510, I have been working on systems design to tackle some of the challenges in Cash Transfer Projects. More specifically challenges with registration, identification and targeting, with regards to the expected scaling-up cash transfer projects.*
>
> *In my research I have conducted a systems analysis from a technical, institutional and stakeholder point of view upon which I decided to scope my system around the following matters:*
>
> - *Digital Identity Life-cycle -> registration, identification, usage and maintenance*
> - *Privacy-by-design principles*

- *Layered blockchain architectures*
- *Humanitarian information management principles*

*I have merged these concepts together with stakeholder views into a program of requirements and I designed a conceptual model of the system. As one of my last phases in this research I would really like to speak to you about the workings of this system and your views on its place in the humanitarian sector.*

*If you are interested to help me out, please let me know and I will send you some more information and set up a meeting (skype or face-to-face). Thanks in advance for your time and efforts.*

*Kind regards, Lars Stevens*

After receiving their agreement and setting up an appointment, a document was send to each expert. This enabled each expert to develop some contextual understanding and gave background information on the following aspects of this study:

- Problem Definition
- Research Question
- Overview of System Analysis
- Program of Requirements
- Design Decisions

Some of these interviews were recorded in Dutch and transcribed in English, while others were conducted in English. There was no conscious choice here but the fact that initial conversation took off in Dutch.

## E.2. Interview Questions

The following general set-up was used to ask questions.

1. Introduction
   (a) Introduction interviewee and organization
   (b) Introduction interviewer and organizations
   (c) Introduction research background and goal of the interview
   (d) Ask for consent on recording the interview and start recording the interview
   (e) Declare expectations of the interview and how this interview is used
2. Assesment of Design Decisions (not in chronological order)
   (a) The use of DIDS and other sorts of identifiers
   (b) Public permissioned vs Public permissionless
   (c) Blockchain Architecture
   (d) Open source license
   (e) Roles and Interfaces
   (f) Off-chain storage
   (g) Key Loss
3. Presentation of Models (only if expert understood BPMN and/or UML)
4. Any questions from the interviewee?
5. Closing the Interview

## E.3. Summaries of the Interviews

In this section per expert interviewee a summary of the most important notions is given. This is done in the order of when each interview was conducted.

### E.3.1. Arnold Daniels, Legalthings

This interview took place in Amsterdam, from 10:00-11:30 on Thursday 14-06-2018. The research is introduced and then the protocol is worked through.

AD: I am not a fan of Ethereum at all because costs of gas are to expensive if you use multiple smart contracts. You could use Ehtereum as a private network, but then you need at least a 1000 nodes for a private network.

AD: The choice for a public permissioned ledger seems logical. The problem with Sovrin in my eyes, is that if you lose your access your identity is gone. LS: There are some recovery methods: offline and social. AD: The problem is that these offline backups can also be stolen and with trusted peers, are they findable. Other options could be sought after in biometrics or pass-phrases.

AD: Your private key is pretty much not usable from a shared medium, so private key should be stored on their device. Ls: Would it be possible if the private key for people who do not have a device, is printed and then used as a login on a registration terminal? AD: Yes that could be, but why would you that? You could also use the two-factors of a biometric with a pass-phrase to log-in.

LS: what do you think of Hyperledger Indy? AD: Yes is fine, the DID you could use on every ledger. You need enough nodes, like with every chain. IF you chose a public chain you would not need to set up your own network, and you have more security or transparency. If would not be feasible if all the nodes are centralized. You could also roll it out on a public permissionless chain like Waves[1] or NEM[2].

LS: The idea of Hyperledger Indy that seemed fitting for this research is the division of roles. What do you think about this? AD: You could also do this on a public permissionless chain, you work with PKI's, where the certificates are public and thus humanitarian nodes could give a credential to other nodes and then you can follow the trust-chain. This is what I think is a weakness in Hyperledger Indy because some nodes are assigned, which does leave room for fraud and corruption. LS: So would you say a permissionless could work better? AD: Yes this could work better.

LS: is it possible to switch to another blockchain? AD: No not that I know of, but you could create blockchains that support multiple ways of signing. So you could have an account on for example a side-chain, and use this to sign on another side-chain.

AD: An Identity Wallet is useful if you want to use it across multiple chains, but if you do not use it across chains than you might not need the wallet.

AD: In the system you should have list of trusted organizations, so the Red Cross might say they trust Oxfam but not an Animal Rescue Service. They could even say that at the moment we trust Oxfam, but from this date we only trust them for 60%. Based on this trust scores could be calculated when providing a service, based on who signed which credential of the identity owner.

AD: The thing I do not really envision is how peer-validation could be used in this system, because then you would have to make public who has signed your peer-credentials. That does interfere with how privacy-proof the system is.

LS: Would it be possible to send out a connection request based on the geo-location of people on the blockchain? AD: Yes that would be possible, but it is not in line with the self-sovereign identity concept. Then you would open up the location data and contact data on a public chain. That is not the route to take. You would have to have the identity owner to reach out first, who could have gotten the news for the program via other sources.

AD: Humanitarian organizations are very big, so they need to assign credentials to validators in the field who can perform validation in the name of the Red Cross.

LS: Why I chose for Hyperledger Indy, is because they are more scalable. What do you think of this? AD: The number of nodes that writes to the blockchain is always restricted, that is why you have the consensus algorithm. I am not 100% but from my understanding the Hyperledger Fabric or Hyperledger Indy is not necessarily super scalable, but it might be more scalable than blockchain.

LS: What do you think of the use of DIDs? AD: Good, but do you really need it? What data-formats are there? Do you need it when using a Wallet? Using standards if often good, and for now it does

[1] https://wavesplatform.com/
[2] https://nem.io/

look good. But again, does it really solve the problem? LS: I thought the DID is the format that allows you to have pairwise pseudonymous connections and are able to revoke it? AD: That is also possible with other standards.

LS: uPort uses IPFS for storage, what do you think of that? AD: A bad choice, IPFS is made for a permanent internet. But permanent is permanent, that does not comply with the GDPR. An alternatives is that nodes store it themselves off-chain, but that would not really work in this design. LS: So where would you store the private data in this design? AD: Not. It would impact the user experience because you would have to enter them every-time, but if credentials are given and stored you will not need to enter them for those credentials. You could always generate this data yourself. You would only need the format. You could store it on the device, you could print it or store it in a QR, that would increase the convenience.

### E.3.2. Sander Dijkhuis, Cleverbase

This interview took place in The Hague, from 10:00-11:30 on Friday 15-06-2018. The research is introduced and then the protocol is worked through.

LS: What does your system use for identifiers? SD: We use the UUID format, which is a unique identifier string. You can calculate a UUID on your own system and be pretty sure that there is no other string like it out there. We just use UUIDs to identify our users within internal systems and within certificates we issue, but the format is not relevant to the outside world. For external relying parties, we offer contextually meaningful identifying attributes instead. LS: What attributes do you request? SD: During the registration of a natural person we validate the email address and data from the user's identity document. We link these qualified attributes to our internal identifier. We can also qualify additional attributes. Depending on the organization that relies upon our identification and on the end user's permission, we present different attributes. So the Tax Office might want your company registration number while a social security office might want your BSN. LS: Would you need a central authority to give out these UUIDs? SD: No that is not necessary.

LS: What do you think of the DIDs? SD: I think it is good that you can use a uniform identifier format independent of service provider or attribute provider. I think you could also introduce some inefficiencies by the requirement to share this data on a blockchain.

SD: Around the validator and observer nodes you need a framework to make sure that these nodes are to be trusted. And you would need a way to blacklist nodes if they perform poorly.

SD: What I find difficult to see is how it is different than just setting up a PKI. LS: The difference is that instead of storing the root-keys centrally, you store them decentral, so that it is why it is called a DPKI.

LS: Where do you store private data with Cleverbase? SD: What you have to when you are a Trusted Service Provider is to store the private key of the end-user in a very safe place. You could do this on a smart-card, or as we do, use server signing. In our case this is a system involving a Highly Secure Module (HSM), that is certified to be FIPS 140-2 Level 3 compliant. The public keys are stored in the certificate, which is the credential that we issue. You can make the private key storage very secure. HSMs at this level of security have tamper-detection and tamper-response circuitry, and are designed so that private keys cannot be traced they are used during cryptographic operations. From some HSMs, all secrets are wiped as soon as screws in the enclosure are accessed or when vibration is detected.

LS: Where do you store the identity attributes? SD: They are currently stored in a private and secure database managed by us. LS: So in this system where would you store this? SD: I am not sure how we would store the data specific to your project; in our current solution, personal data is stored in a secure cloud storage. Users can rely upon our certifications such as ISO 27001, which involve regular audits. LS: Could you store it on the phone? SD: Yes, you could, but then people are not known for making good back-ups of their phones. LS: In Sovrin they use these agents that make back-ups that could also be a solution.

LS: How does key loss with Cleverbase? SD: Then we revoke the credential and people would have to get a new account by re-registering. We can then crosscheck in the database and give them the same account but with new credentials.

SD: Relying on biometrics for authentication is complex. There is a lot of research about gathering and about faking these biometrics.

SD: I still find it fascinating whether you would need a DPKI for your project, or you could just as well use a regular PKI.

### E.3.3. Vincent Graf, ICRC

This interview took place in the Hague and Geneva, via skype, from 16:00-17:30 on Monday 18-06-2018.

VG: In the humanitarian context key recovery will remain a problem. Especially since now, if people loose their access they will become the must vulnerable and before they can be assisted they will need a digital account again. We should continue to help all people, not only those that are registered via a digital identity system.

VG: In some communities, because of culture for example, some affected people are represented by other members of the communities which act as a kind of proxy. This can be true for 1 person or a household. This case must be taken into account when a system require individual registration and unique ID management.

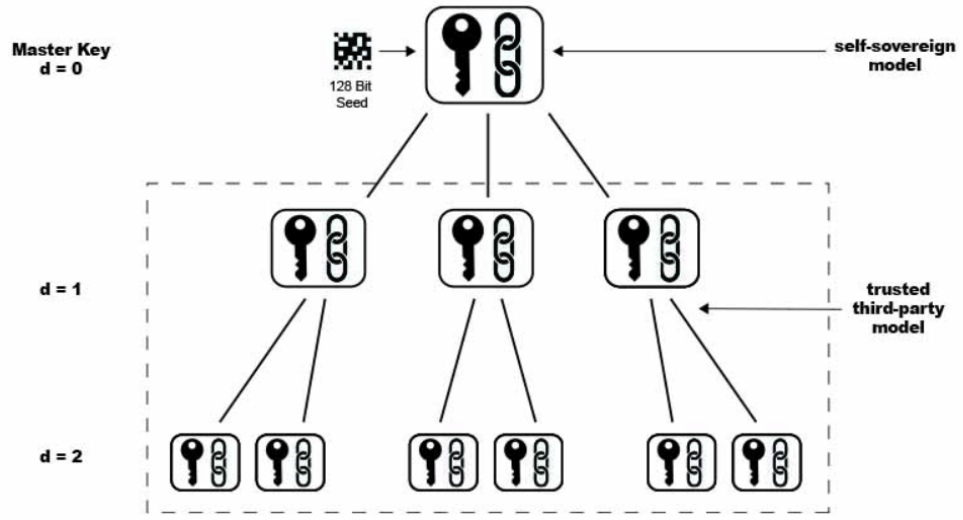
VG: I understand that open-sourcing these IT projects is done as many of these organizations are publicly funded. But this does not mean that everyone will just start to use it. In many cases it are still the nation states that hold most power, so they would need to be persuaded to become part of this system to really make it work. Not all nation states might want to participate, since it will reduce their central control on the provision of identities.

VG: I am wondering what the business model would be, how is it sustainable? LS: Good question, this is something that I have left out of scope but I would seek it at the service providers. For example mobile phone companies and banks all over the world require to comply with KYC regulation, they might want to pay for that or at least keep the system up-to-date. The same goes for humanitarian organizations, they will save money from registration and identification processes. How to monetize this into the system is to be further researched.

VG: I think the public permissioned chain and the characteristics coming with the Trustees-Stewards configuration, is the least-bad alternative to do this. Humanitarian Organizations, that will likely be Trustees or Stewards, may not be seen as totally impartial as they may be linked to one or another party to the conflict. I do not really see any other options though, but we do have to question if running such a system is part of their mandate.

LS: Do you think that a public permissioned blockchain better resembles or is more likely to be adapted by the humanitarian sector than a public permissionless chain? VG: I think it depends, the permissionless chain might be perceived well by organizations that have less to do with politics. While the permissioned chain might be a favorable choice for organizations that would like to have more power in this process. Maybe, the permissioned chain does suit the purpose better, I am not sure.

[htpb!]




**1.1 Self-Sovereign Model.** Placing the individual at the core root of the derivation (depth 0), where the user is the holder of the seed and master key is the self-sovereign identity model. Here the user has the greatest degree of control and responsibility in managing their identity client-side.

**1.2 Trusted Third-party Model.** Placing the individual at a depth of 1 or any subsequent derivation is the trusted third-party model. In some cases where an individual is not willing or capable of managing their own keys on their device.

Figure E.1: Hierarchical Deterministic Key Pairs from Robles and Appelcline [128]

### E.3.4. Djuri Baars, Rabobank

This interview took place in Utrecht, from 10:00-11:00 hours on Tuesday 19-06-2018. The research is introduced and then the protocol is worked through.

DB: With regards to blockchain we have created some 100 use-cases, where we respond to specific requests from the departments. None of the departments request blockchain, they request a solution for a problem. There are three main component in each of these use-cases: Identity, Value Transfers and Signing.

LS: What do you think of the use of DIDs? DB: It is a good specification, we do not use it at the moment but the standard is good and provides future opportunities. It offers the possibility to make identities interoperable between systems and therefore I see DIDs as an Identity Rolodex.

LS: Do you know if an organization needs a specific DID for communication with a person, but also the other way around, so are there two DIDs necessary for one way communication? DB: I am not sure. Ideally you want multi-show unlinkability. LS: Correct, so far only Idemix uses it. I have not seen an example on the blockchain. DB: You could use hierarchical deterministic key-pairs (see figure E.1). Which allow the user to create a master key, and create children and grandchildren keys that are one-way. They can not be traced back to the master key, resulting in unlinkability. It is quite a technical concept, but it could work. From my understanding this is something that uPort has or is trying to implement.

DB: A ZKP is about proving that what you did was done with integrity, so you do not reveal the proof. An example is that if there is a Where-is-Waldo-Map, I could point out where Waldo is. But then so can others. If I take a black piece of paper and only cut out Waldo's figure to put it on top of the where-is-waldo-map, then I can demonstrate that I have found Waldo on this map but none of the others can reproduce the proof based on my actions. LS: So are these also how zk-SNARKS work? DB: Yes, this is how they work. Regular ZKP are indeed very CPU intensive and zk-SNARKS still take a significant space on the blockchain. LS: Could you also do this off-chain? DB: The nice thing about zk-SNARKS is that they are non-interactive, so if you do this off-chain than you need to set up an extra connection as it must be interactive. This is possible, but requires extra efforts. With regards to GDPR, it would be better to put only the ZKP-proof onchain than any of the data.

LS: I have found this user-centered design for DIDs, would it be possible to send the inclusion algorithm to the identity owner so that the service provider would never have to receive the credentials, but only receives by whom the credentials are verified and what the inclusion score is? DB: Yes this is possible. But it would require a list of trusted parties for service providers that they need to maintain. This maintenance is necessary.

LS: What do you think of using a DPKI? DB: That could work just fine, but it would make some attribute providers even more important because of how they submit their credentials.

LS: What type of blockchain would you use? DB: If you are an self-sovereign purist you could only use the permissionless chain. Then you would have to accept that also organizations like ISIS could provide attestations. While if you use Sovrin and have a permissioned chain, you make it more complex and have a barrier-to-enter, but could work if you do not want organizations like ISIS to attest. If you use a public permissioned chain you give yourself an extra governance problem.

LS: The reasons for chosing for a permissioned ledger are that they better match with the current governance structure, scalability and does not require much resources for consensus, plus it enables the division of roles so that the system can be functional at first. What do you think of this? DB: I agree with the argumentation. My point is that blockchains that have similar purposes should work together or that only one should exist, this in general would decrease the amount of energy needed in permissionless chains. If you erect a whole blockchain for one use-case than you might not be working effective. Furthermore what is also interesting is that there is a business-model possible for a permissioned system, while these are much more difficult than for permissionless systems.

DB: With regards to key-loss, if you have some centrality, you could also arrange that if someone has lost their keys they could go to the humanID trustees and they will than revoke all credentials and make sure that nobody else can use your identity. You would run into some scaling issues here as well. LS: What is see are four options for key-covery: key-phrase, two-factor authentication, social recovery and a back-up. Do you see more? DB: If I hear this you use technical and non-technical solutions. With social recovery you would need some form of contract while with a key-phrase you just login differently. LS: You would likely need multiple solutions to make it available in all contexts. DB: Using biometrics for the two-factor authentication would bring other risks, because you likely store these centrally. This creates a new single point of failure.

LS: Where would you store the private key? DB: Ideally the identity owner should have it, yet in practice people often do not trust themselves with the private key so you would need a custodian. This would again introduce some centrality. You could work with this master-key concept, where the issuer of a credential holds the master key themselves and only hands-out child key sets. They could than revoke the access. You could also look at how BitGo[3] does this, with multi-signature signing. In BitGo you have three wallets: sender, BitGo and recovery. You need two to sign and the BitGo wallet always signs with you. But if you loose your key and let BitGo know BitGo closes of your sender wallet and together with the recovery wallet, it transfers all of your coins to a new wallet (see figure E.2). LS: This could also be used by people without devices, because you could print out this private key and then if they loose them, they could go to the organization that have provided them with the identity and revoke them in this way.

LS: What would be other ways to do an Identity Wallet? DB: IF you use blockchain you would have to use wallets somewhere, whether they are dedicated wallets or part of another application. You could, like how IRMA functions, load your credentials onto a Smartcard.

DB: With these systems you have to kind of shop for identity credentials

LS: Based on this design would you rather advice the humanitarian sector to join Sovrin/Hyperledger Indy or try to create something themselves? DB: Join Sovrin, it would be more efficient, less costly and there should be a minimum of different identity systems.

[3] https://www.bitgo.com/info/

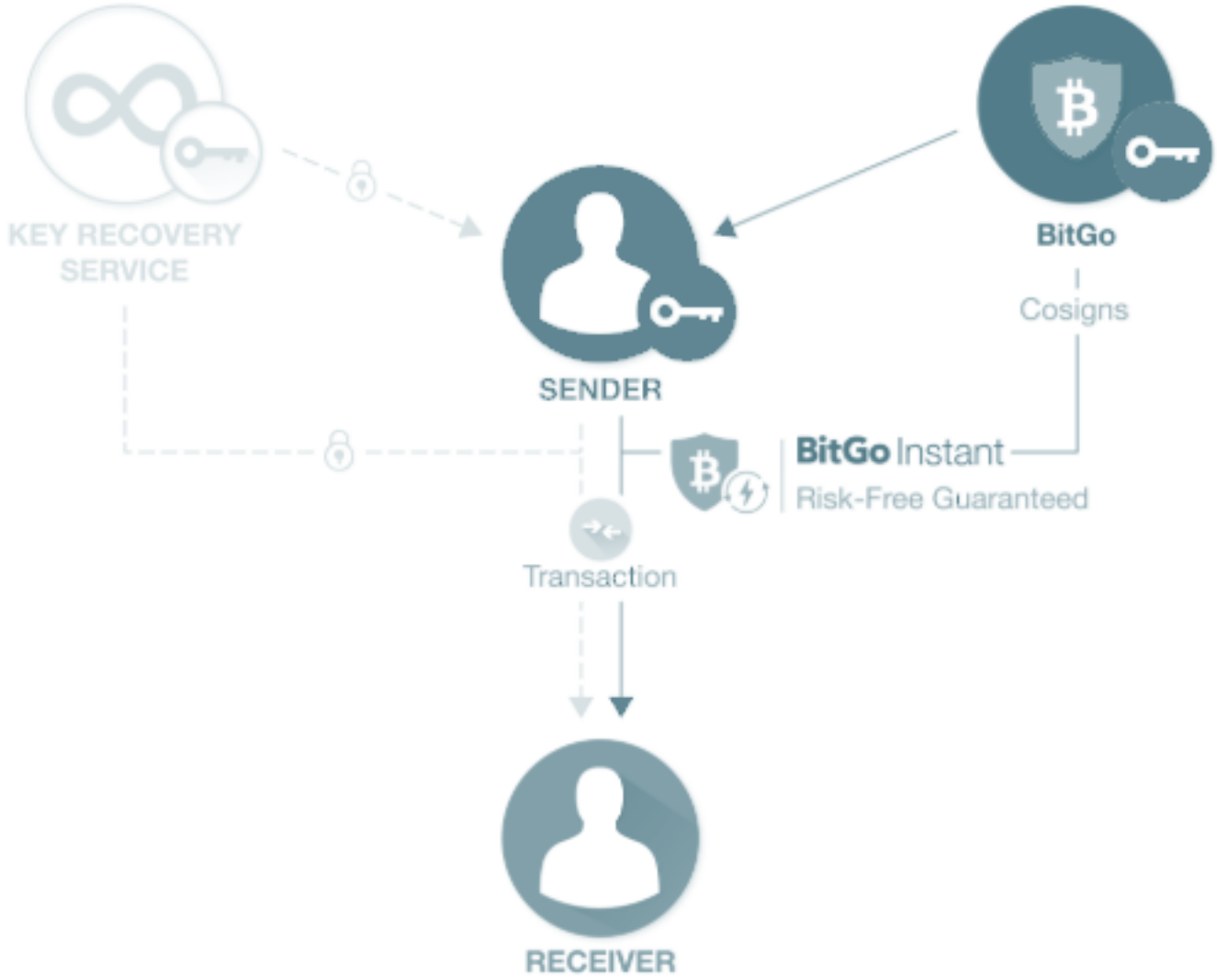



Figure E.2: Multi-signature signing in BitGo [26]

### E.3.5. Maarten van der Veen, NLRC

This interview took place in The Hague, from 13:00-14:00 hrs on Monday 18-06-2018. The research is introduced and then the protocol is worked through.

MV: Is it possible to have multiple identities? LS: Yes, this is possible. But based on the user-centered design it would not matter as long as people get validated. The credentials that are issued are only related to one identity. Yet, in some humanitarian cases it issuing credentials is not possible before the CTP is set-up. A humanitarian organization might have to include non-validated identities and risks including people twice or more. MV: You could decided to make fraud-detection algorithms, based on time-stamps and include CATPCHA-like measures to ensure it are people that assign. You could also try to have a certain phone-number only register one or two identities per phone.

MV: Is it possible to register as an authorized representative, lets say for children? LS: No this is not possible at the moment. This is a limitation of the system for now and should be added to the design requirements.

MV: You said that identities can now be registered in advance of a disaster or continuously, yet from disaster response experience and research it became apparent that people do not prepare for disaster. So the system must have a value even before a disaster strikes. There must be a continuous value proposition, fully integrated into the community. LS: You may first integrate this with KYC protocols for mobile phone companies, or other organizations.

MV: Biometrics are still to be frauded, each fingerprint is different and I can unlock my phone with many bodyprints (tongue etc). At the border they at least state that you need to use your right thumb. Iris-scans may be better. In general, including biometrics is not fraud-free.

MV: Which of the four systems you compared matches best? LS: Sovrin is best suited. NLRC in objectives. Also since the choice for a public permissioned chain was made, Sovrin was the ideal comparison. To be clear, humanID uses the same architecture but has a different system on top of this infrastructure than Sovrin has made.

LS: What do you think of the blockchain use? MV: Blockchain might enable some important aspects I see for such a system. First, it enables self-sovereignty. Two, stable systems in a digital environment are often distributed. Furthermore, the system should be scalable or extremely interoperable, and it should be portable. So when someone seeks refuge in another country it should be able to use the same digital identity.

MV: It is a rat-race, either there is one main digital system or there are multiple that should be interoperable. As a humanitarian organization we must question if we are the ones to create this identity system or that it would be more efficient to join one of the existing alternatives. These already have some installed base. It would be nonsense to create many, stand-alone digital identity systems or private ones.

MV: How many validator nodes would yo need? Is this feasible? LS: You would need many less than in public permissionless blockchains, and the consensus mechanism is easier to run. As it requires less energy and less time.

MV: So with public permissioned the identity owners in your system are in control of their identities but not of the system which is done by the Trustees and Stewards. Which is different in Bitcoin, that is run by users. LS: This is true, but in Bitcoin there is centralization of mining, that has created an entire industry. So it is a trade-off that has to be made, a permissioned chain better simulates the current humanitarian governance. MV: Would this deter user adoptability? LS: This is difficult to say. They would still see the same humanitarian organizations as they do now.

MV: To implement this system you would need a wide backing base. The mandate of the humanitarian organizations is very limited, governments request the help of humanitarian organizations, but before a disaster strikes the mandate is very limited. LS: So the system must be backed by a wide variety of actors to have the ability to implement it and create the mandate for it.

MV: The inclusion algorithm should also be send to the identity owner, so that the credentials are not even send to the service provider.

# Bibliography


[1] Licenses | Choose a License. URL https://choosealicense.com/licenses/.

[2] 510.Global. Internal Docs: Peer-to-peer cash transfers for early warning early action systems, 2017.

[3] 510.Global. CBA: CASH BASED ASSISTANCE THE FUTURE – 510 GLOBAL, 2018. URL https://www.510.global/the-future-of-cash-based-assistance-2/.

[4] Andreas Abraham. Self-Sovereign Identity. 2017. URL https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf.

[5] Jenny C Aker. Comparing Cash and Voucher Transfers in a Humanitarian Context : Evidence from the Democratic Republic of Congo. *The World Bank Economic Review*, 31(January):44–70, 2017. doi: 10.1093/wber/lhv055.

[6] Degan Ali and Kirsten Gelsdorf. Risk-averse to risk-willing: Learning from the 2011 Somalia cash response. *Global Food Security*, 1(1):57–63, 2012. ISSN 22119124. doi: 10.1016/j.gfs.2012.07.008. URL http://dx.doi.org/10.1016/j.gfs.2012.07.008.

[7] Muneeb Ali, Jude Nelson, Ryan Shea, and Michael J Freedman. Bootstrapping Trust in Distributed Systems with Blockchains. *USENIX;login:*, 41(3):52–58, 2016. URL https://www.usenix.org/publications/login/fall2016/bootstrapping-trust-distributed-systems-blockchains.

[8] Muneeb Ali, Ryan Shea, Jude Nelson, and Michael J Freedman. Blockstack Technical Whitepaper Blockstack: A New Internet for Decentralized Applications. 2017. URL https://icotokn.com/wp-content/uploads/2017/11/blockstack-whitepaper.pdf%0Ahttps://blockstack.org/whitepaper.pdf.

[9] C. Allen. The Path to Self-Sovereign Identity, 2016. URL http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[10] C. Arnold, T. Conway, and M. Greenslade. Cash Transfers. Technical report, Department for International Development, 2011.

[11] J.J. Atick, Z. Safdar, A. Gelb, E. Gasol Ramos, and S. Pahlavooni. Digital Identity toolkit: A guide for statkeholders in Africa. Technical report, World Bank Group, Washington, D.C., 2014.

[12] Djuri Baars. *Towards Self-Sovereign Identity using Blockchain Technology*. PhD thesis, Universtiy of Twente, 2016.

[13] S. Bailey. Humanitarian Cash Transfers in the Democratic Republic of the Congo: Evidence from UNICEF's ARCC II Programme. (April), 2017. URL https://www.air.org/sites/default/files/downloads/report/Humanitarian-Cash-Transfer-DRC-April-2017.pdf.

[14] Sarah Bailey and Steve Walsh. The Use of Cash in Emergency and Post-Emergency Non-Food Item Programs - A Case Study from the DRC. *Journal of Humanitarian Assistance*, 2007. URL http://sites.tufts.edu/jha/archives/49.

[15] Owen Barder, Chris Blattman, Lindy Cameron, Jan Egeland, Mohamed Elmi, Michael Faye, Jacquelline Fuller, Marcia Lopes, James Mwangi, Tara Nathan, Andrew Natsios, Toby Porter, Claus Sorensen, Jane Waterman, and Lauren Woodman. Doing cash differently: How cash transfers can transform humanitarian aid. Technical Report September, ODI, 2015. URL https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf.

[16] M. Barnett and T.G. Weiss. *Humanitarianism Contested: Where Angels Fear to Tread*. Routledge, New York, 2011. URL https://books.google.nl/books?id=pPGrAgAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false.

[17] Michael N. Barnett. Humanitarian Governance. *Annual Review of Political Science*, 16(1):379–398, 2013. ISSN 1094-2939. doi: 10.1146/annurev-polisci-012512-083711. URL http://www.annualreviews.org/doi/10.1146/annurev-polisci-012512-083711.

[18] Johannes M. Bauer. Platforms, systems competition, and innovation: Reassessing the foundations of communications policy. *Telecommunications Policy*, 38(8-9):662–673, 2014. ISSN 03085961. doi: 10.1016/j.telpol.2014.04.008. URL http://dx.doi.org/10.1016/j.telpol.2014.04.008.

[19] Roman Beck, Sven Weber, and Robert Wayne Gregory. Theory-generating design science research. *Information Systems Frontiers*, 15(4):637–651, 2013. ISSN 13873326. doi: 10.1007/s10796-012-9342-4.

[20] Ana Maria Bedran-Martins and Maria Carmen Lemos. Politics of drought under Bolsa Família program in Northeast Brazil. *World Development Perspectives*, 7-8(March):15–21, 2017. ISSN 24522929. doi: 10.1016/j.wdp.2017.10.003. URL https://doi.org/10.1016/j.wdp.2017.10.003.

[21] D. Bell. UML basics: The class diagram, 2004. URL https://www.ibm.com/developerworks/rational/library/content/RationalEdge/sep04/bell/index.html.

[22] Donald Bell. UML basics: The class diagram An introduction to structure diagrams in UML 2. Technical report, IBM, 2004.

[23] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System.

[24] Best Use of Resources Initiative. Cost Efficiency Analysis: Unconditional Cash Transfer Programs. Technical report, IRC, New York, 2015. URL https://www.rescue.org/sites/default/files/document/954/20151113cashcefficreportfinal.pdf.

[25] Alexander Betts and Louise Bloom. Humanitarian Innovation: The state of the art. 2014.

[26] BitGo. BitGo: Making Digital Currencies Usable for Business., 2018. URL https://www.bitgo.com/info/solutions#custody.

[27] Blockstack. Blockstack Core, 2018. URL https://github.com/blockstack/blockstack-core.

[28] Tony Bovaird. Marketing in Public Sector Organizations. In *Public Management and Governance*, chapter 6, pages 81–94. Routledge, New York, 2nd edition, 2009.

[29] Clare O Brien, Zoë Scott, Gabrielle Smith, Valentina Barca, Andrew Kardan, Rebecca Holmes, and Carol Watson. Shock-Responsive Social Protection Systems Research Synthesis Report. Technical Report January, Oxford Policy Management, Oxford, 2017.

[30] Julian La Brooy. A Weighted Welfare Analysis of Local Price Inflation. *Journal of Human Security*, 5(2):65–82, 2007.

[31] CaLP. Glossary of Cash Transfer Terminology Programming (CTP) Terminology, 2017. URL http://www.cashlearning.org/downloads/calp-updated-glossaryfinal-october-2017.pdf.

[32] K. Cameron. The Laws of Identity. 2005.

[33] B. Carson, G. Romanelli, P. Walsh, and A. Zhumaev. Blockchain beyond the hype: What is the strategic business value? *McKinsey Digital*, 6 2018. URL https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

[34] Ann Cavoukian. Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices. Technical report, 2009. URL https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf%5Cnwww.privacybydesign.ca.

[35] C. Churchman. Guest editorial: Wicked problems". *Management sciences*, 14(4):141–142, 1967.

[36] Paul Knox Clarke and Leah Campbell. Coordination in theory, coordination in practice: the case of the Clusters. *Disasters*, 2018. ISSN 03613666. doi: 10.1111/disa.12282. URL http://doi.wiley.com/10.1111/disa.12282.

[37] Ronald Coase. The Nature of the Firm. *Economics*, 4(16):386–405, 1937. ISSN 00130427. doi: 10.2307/2626876.

[38] Alexis Collomb and Klara Sok. Blockchain/Distributed Ledger Technology (DLT): What Impact on the Financial Sector? *Digiworld Economic Journal*, 103(103):93–111, 2016. ISSN 11578637.

[39] L. Cornish. New security concerns raised for RedRose digital payment systems, 2017. URL https://www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619.

[40] D. Tapscott and A. Tapscott. *Blockchain revolution*. Penguin Random House, New York, NY., 2016. ISBN 978-0-241-23785-4.

[41] Sinclair Davidson, Primavera De Filippi, and Jason Potts. Economics of Blockchain. *SSRN Electronic Journal*, 2016. ISSN 1556-5068. doi: 10.2139/ssrn.2744751.

[42] Simon Davies and J. Davey. Making the Most of It: A Regional Multiplier Approach to Estimating the Impact of Cash Transfers on the Market. *Development Policy Review*, 26(1):91–111, 2007.

[43] Hans de Bruijn and Paulien M. Herder. System and actor perspectives on sociotechnical systems. *IEEE Transactions on Systems, Man, and Cybernetics*, 39(5):981–992, 2009. ISSN 10834427. doi: 10.1109/TSMCA.2009.2025452.

[44] Hans de Bruijn, Ernst ten Heuvelhof, and Roel in 't Veld. *Process Management*. 2010.

[45] Deloitte. Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality. Technical report, Centre for the Edge, Deloitte, Melbourne, 2016. URL https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf.

[46] Deloitte. Key Characteristics of the Blockhcain, 2017. URL https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-key-characteristics-noexp.pdf.

[47] Peter J. Denning. A new social contract for research. *Communications of the ACM*, 40(2):132–134, 1997. ISSN 00010782. doi: 10.1145/253671.253755.

[48] Advait Deshpande, Katherine Stewart, Louise Lepetit, and Salil Gunashekar. Overview Report Distributed Ledger Technologies / Blockchain : Challenges , opportunities and the prospects for standards. *British Standards Institution*, page 82, 2017. doi: 10.7249/RR2223. URL https://www.rand.org/pubs/external_publications/EP67133.html.

[49] Development Initiatives. Global Humanitarian Assistance Report 2017. Technical report, Development Initiatives, Bristol, 2017. URL http://devinit.org/wp-content/uploads/2017/06/GHA-Report-2017-Full-report.pdf.

[50] Felix Dodds, David Donoghue, and Jimena Leiva Roesch. *Negotiating The Sustainable Development Goals*. 2016.

[51] Shannon Doocy, Hannah Tappis, and Emily Lyles. Are cash-based interventions a feasible approach for expanding humanitarian assistance in Syria ? *Journal of International Humanitarian Action*, pages 1–13, 2016. ISSN 2364-3412. doi: 10.1186/s41018-016-0015-7. URL http://dx.doi.org/10.1186/s41018-016-0015-7.

[52] Daniel Drescher. *Blockchain basics - a non-technical introduction in 25 steps*. Apress, 2017. ISBN 978-1-4842-2603-2. doi: 10.1007/978-1-4842-2604-9. URL https://console.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html.

[53] M. Drijvers. *Efficient Delegation of Idemix Credentials*. PhD thesis, Radboud University Nijmegen, 2014.

[54] Reed Drummond, Les Chasen, Christopher Allen, Ryan Grant, Brian Weller, Kiara Robles, and Shannon Appelcline. DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01. 2016.

[55] P. Dunphy and F.A.P. Petitcolas. A First Look at Identity Management Schemes. *IEEE Security and Privacy Magazine*, 2018.

[56] W. Easterly. *The White Mans Burden: Why the West's Efforts to Aid the Rest Have Done So Much Ill and So Little Good*. Penguin Books, London, UK, 2007. ISBN 978-0143038825.

[57] Espyder. An enterprise class GDPR compliance platform, 2018. URL https://espyder.net/.

[58] B. Fabres. Think Global, Act Global in the Mekong Delta? Environmental Change, Civil Society and NGOs. *Advances in Global Change Research*, 45(1):7–34, 2011. doi: 10.1007/978-94-007-0934-8.

[59] R. Ian. Faulconbridge and M. J. (Michael J.) Ryan. *Managing complex technical projects : a systems engineering approach*. Artech House, 2003. ISBN 1580537642. URL https://books.google.nl/books/about/Managing_Complex_Technical_Projects.html?id=nt0Yd5JtJWIC&redir_esc=y.

[60] Bridget Fenn, Garba Noura, Victoria Sibson, Carmel Dolan, and Jeremy Shoham. The role of unconditional cash transfers during a nutritional emergency in Maradi region, Niger: A pre-post intervention observational study. *Public Health Nutrition*, 18(2):343–351, 2015. ISSN 14752727. doi: 10.1017/S1368980014000378.

[61] Jesse Frederik and Rutger Bregman. De oplossing voor bijna niks: de blockchain, 2018. URL https://soundcloud.com/rudifreddieshow/de-oplossing-voor-bijna-niks-de-blockchain.

[62] Marito Garcia and Charity M. T. Moore. *The Cash Dividend*. The World Bank, Washington D.C., 2012. ISBN 978-0-8213-8897-6. doi: 10.1596/978-0-8213-8897-6. URL http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-8897-6.

[63] Alan Gelb and Caroline Decker. Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries. *Review of Policy Research*, 29(1):91–117, 2012.

[64] Daniel Gilman and Leith Baker. Humanitarianism in the Age of Cyberwarfare: Towards the Principled and Humanitarian Emergencies. 2014. URL http://reliefweb.int/sites/reliefweb.int/files/resources/HumanitarianismintheCyberwarfareAge-OCHAPolicyPaper11.pdf.

[65] S. Giodini, M. van der Veen, and L. Stevens. DRAFT Whitepaper Future of Cash Based Assistance. 2018.

[66] Google. Google Cloud Storage SLA, 2016. URL https://cloud.google.com/storage/sla.

[67] Paul A Grassi, Michael E Garcia, and James L Fenton. NIST Special Publication 800-63-3: Digital identity guidelines. Technical report, National Institute of Standards and Technology, 2017. URL http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[68] GSDRC. International Legal Frameworks for Humanitarian Advocacy. Technical report, GSDRC, University of Birmingham, Birmingham, UK, 2013.

[69] GSMA. Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid. Technical report, GSMA, London, 2017.

[70] Debarati Guha-Sapir and Olivia D'Aoust. Demographic and Health Consequences of Civil Conflict. Technical report, The World Bank, Washington, D.C., 2010. URL http://wdr2011.worldbank.org/sites/default/files/pdfs/WDRBackgroundPaper-SapirandD'Aoust.pdf?keepThis=true&TB_iframe=true&height=600&width=800.

[71] Elise Haak. *Towards a Governance Structure for the Data-Driven Prioritization of Humanitarian Aid A data ecosystem approach*. PhD thesis, Delft University of Technology, 2017.

[72] Mohammad Hajialikhani and Mohammad Jahanara. UniqueID: Decentralized Proof-of-Unique-Human, 2018. URL http://arxiv.org/abs/1806.07583.

[73] Teresa M. Harrison, Theresa A. Pardo, and Meghan Cook. Creating Open Government Ecosystems: A Research and Development Agenda. *Future Internet*, 4:900–928, 2012. doi: 10.3390/fi4040900.

[74] Paul Harvey. HPG Discussion Paper Cash and vouchers in emergencies. 2005.

[75] Paul Harvey and Sarah Bailey. Cash transfer programming in emergencies. Technical Report 11, ODI, London, 2011.

[76] HelpAge International. Cash transfers in emergencies: A practical field guide. Technical report, HelpAge International, Muang, Chiang Mai, 2010.

[77] Joakim Hertzeberg Ulstein. *Humanitarian Governance: Network, Agency and Power*. PhD thesis, University of Oslo, 2012. URL http://www.annualreviews.org/doi/10.1146/annurev-polisci-012512-083711.

[78] Ken Hess. Decisions, decisions. How do you choose an open source license?, 2014. URL https://www.zdnet.com/article/decisions-decisions-how-do-you-choose-an-open-source-license/.

[79] Alan Hevner and Samir Chatterjee. Design Research in Information Systems. In *Integrated Series in Information Systems 22*, volume 22, chapter 2, pages 9–23. Springer Science+Business Media, LLC 2010, 2010. ISBN 978-1-4419-5652-1. doi: 10.1007/978-1-4419-5653-8. URL http://link.springer.com/10.1007/978-1-4419-5653-8.

[80] A.R. Hevner, S.T. March, J. Park, and S. Ram. Design Science in Information Systems Research. *MIS Quarterly*, 28(1):75–105, 2004. ISSN 0276-7783. doi: 10.2307/25148869.

[81] Garrick Hileman and Michel Rauchs. Global Blockchain Benchmarking Study. Technical report, Cambridge Centre for Alternative Finance, Cambridge, UK, 2017. URL https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf.

[82] Humanitarian Coalition. What is the Humanitarian System? URL http://humanitariancoalition.ca/the-humanitarian-system.

[83] Humanitarian Response. What is the Cluster Approach? URL https://www.humanitarianresponse.info/en/about-clusters/what-is-the-cluster-approach.

[84] Hyperledger. Introduction — hyperledger-fabricdocs master documentation, 2017. URL http://hyperledger-fabric.readthedocs.io/en/release-1.1/blockchain.html.

[85] Hyperledger. DKMS (Decentralized Key Management System) Design and Architecture V3, 2018. URL https://github.com/hyperledger/indy-sdk/blob/master/doc/design/005-dkms/DKMSDesignandArchitectureV3.md.

[86] Hyperledger. Getting Started with Libindy, 2018. URL https://github.com/hyperledger/indy-sdk/blob/master/doc/getting-started/getting-started.md.

[87] ICRC. Basic rules of international humanitarian law in armed conflicts, 1988. URL https://www.icrc.org/eng/resources/documents/misc/basic-rules-ihl-311288.htm.

[88] IDS. Blockchain for development – hope or hype? 2017. URL https://opendocs.ids.ac.uk/opendocs/bitstream/handle/123456789/12945/RRB17.pdf?sequence=38.

[89] IFRC. National Societies directory, 2017. URL http://media.ifrc.org/ifrc/who-we-are/national-societies/national-societies-directory/.

[90] International Red Cross and Red Crescent Movement. Cash in Emergencies Toolkit, 2017. URL http://rcmcash.org/.

[91] Ori Jacobovitz. Blockchain for Identity Management. Technical Report December, Ben-Gurion University, Beer Sheva, 2016. URL https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf.

[92] Mohamed Jelle, Carlos S Grijalva-eternod, Hassan Haghparast-bidgoli, Sarah King, Cassy L Cox, Jolene Skordis-worrall, Joanna Morrison, Timothy Colbourn, Edward Fottrell, and Andrew J Seal. The REFANI-S study protocol : a non- randomised cluster controlled trial to assess the role of an unconditional cash transfer , a non-food item kit , and free piped water in reducing the risk of acute malnutrition among children aged 6 – 59 months living. *BMC Public Health*, 17:1–8, 2017. doi: 10.1186/s12889-017-4550-y.

[93] Paul Johannesson and Erik Perjons. *An Introduction to Design Science*. Springer International Publishing, Stockholm, 2014. ISBN 9783319106311. doi: 10.1007/978-3-319-10632-8.

[94] R Joosten. A Conceptual Analysis on Sovrin. Technical Report January, TNO, Groningen, 2018.

[95] A. Kaspersen and C. Lindsey-Curtet. The digital transformation of the humanitarian sector. URL http://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/.

[96] Emebet Kebede. Moving from emergency food aid to predictable cash transfers: Recent experience in Ethiopia. *Development Policy Review*, 24(5):579–599, 2006. ISSN 09506764. doi: 10.1111/j.1467-7679.2006.00349.x.

[97] David Kelaher and Brian Dollery. Cash and in-kind food aid transfers: The case of tsunami emergency aid in banda aceh. *International Review of Public Administration*, 13(2):117–128, 2008. ISSN 2331795. doi: 10.1080/12294659.2008.10805125.

[98] Vanessa Ko and Andrej Verity. Blockchain for the Humanitarian Sector: Future Opportunities. Technical report, 2016. URL https://www.academia.edu/30287787/Blockchain_For_The_Humanitarian_Sector_Future_Opportunities.

[99] P. Kohlhaas. Zug ID: Exploring the First Publicly Verified Blockchain Identity, 2017. URL https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702.

[100] Roy Lai. Understanding Interbank Real-Time Retail Payment Systems. In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1*, volume 1, chapter 12, pages 283–310. Elsevier Inc., Cambridge, USA, 1 edition, 2018. ISBN 978-0-12-810441-5. doi: 10.1016/B978-0-12-810441-5.00012-9. URL http://linkinghub.elsevier.com/retrieve/pii/B9780128104415000129.

[101] Roy Lai and David LEE Kuo Chuen. Blockchain – From Public to Private. In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, volume 2, chapter 7, pages 145–177. Elsevier Inc., Cambridge USA, 1 edition, 2018. ISBN 9780128122822. doi: 10.1016/B978-0-12-812282-2.00007-3. URL http://linkinghub.elsevier.com/retrieve/pii/B9780128122822000073.

[102] Céline Langendorf, Thomas Roederer, Saskia de Pee, Denise Brown, Stéphane Doyon, Abdoul Aziz Mamaty, Lynda W.M. Touré, Mahamane L. Manzo, and Rebecca F. Grais. Preventing Acute Malnutrition among Young Children in Crises: A Prospective Intervention Study in Niger. *PLoS Medicine*, 11(9), 2014. ISSN 15491676. doi: 10.1371/journal.pmed.1001714.

[103] Jason Law and Lovesh Harchadani. Scaling a BFT Consensus Protocol for Identity, 2016. URL https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/topics-and-advance-readings/scaling-a-bft-consensus-protocol-for-identity.md.

[104] Jennifer Lee. Cash Transfers in Emergencies. *Columbia Social Work Review*, 3:21–32, 2012. URL http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url,cookie,uid&db=sih&AN=89483465&site=ehost-live&scope=site.

[105] LucidChart. UML Class Diagram Tutorial. URL https://www.lucidchart.com/pages/uml-class-diagram.

[106] M.L. Markus, A. Majchrzak, and L. Gasser. A Design Theory for Systems That Support Emergent Knowledge Processes. *MIS Quarterly*, 26(3):179–212, 2002. URL http://www.jstor.org/stable/4132330.

[107] Juri Mattila. The blockchain phenomenon. 2016. URL http://blogs.reuters.com/felix-salmon/2013/04/09/the-disruptive-potential-of-native-advertising/.

[108] Hanna Mattinen and Kate Ogden. Cash-based interventions: Lessons from southern Somalia. *Disasters*, 30(3):297–315, 2006. ISSN 03613666. doi: 10.1111/j.0361-3666.2005.00322.x.

[109] M. Meuser and U. Nagel. The Expert Interview and Changes in Knowledge Production. In A. Bogner, B. Littig, and W. Menz, editors, *Interviewing Experts*, chapter 1, pages 17–47. ECPR, 2009.

[110] B. Nardi and V.L. O'Day. *Information Ecologies: Using Technology with Heart*. MIT Press, Cambridge, MA, USA, 1999.

[111] Douglass C North. Institutions, Institutional Change, and Economic Performance. *The Journal of Economic Perspective*, 5(1):97–112, 1991. ISSN 07388950. doi: 10.2307/2234910.

[112] NRC. Cash Transfers in Remote Emergency Programming. Technical Report August, Norwegian Refugee Council, Oslo, 2016.

[113] Carly Nyst, Paul Makin, Steve Pannifer, and Edgar Whitely. Digital Identity : Issue Analysis Executive Summary. Technical Report June, Consult Hyperion, Guildford, UK, 2016.

[114] Ekeni Obi. What is Rootstock(RSK)? The bitcoin sidechain no one is talking about., 2018. URL https://medium.com/@ekeneobi/what-is-rootstock-rsk-the-bitcoin-sidechain-no-one-is-talking-about-838c4b0a668f.

[115] OCHA. Best Practices in Humanitarian Information Management and Exchange. In *Symposium on Best Practices in Humanitarian Information Exchange*, number February, Geneva, 2002. United Nations Office for the Coordination of Humanitarian Affairs.

[116] P. Offerman, S. Blom, M. Schonherr, and U. Bub. Artifact Types in Information Systems Design Science – A Literature Review. In R. Winter, J. Leon Zhao, and S. Aier, editors, *DESRIST 2010*, pages 77–92, St. Gallen, Switzerland, 2010. Springer-Verlag.

[117] Svein Ølnes, Jolien Ubacht, and Marijn Janssen. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, (xxxx):1–10, 2017. ISSN 0740-624X. doi: 10.1016/j.giq.2017.09.007. URL www.elsevier.com/locate/govinf.

[118] OMG. Business Process Model and Notation (BPMN), Version 2.0. Technical report, Object Management Group, 2013. URL http://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMNhttp://www.omg.org/spec/BPMN.

[119] Oracle. Object-Oriented Programming Concepts, 2017. URL https://docs.oracle.com/javase/tutorial/java/concepts/index.html.

[120] Nouha Oualha, Melek Önen, and Yves Roudier. Secure P2P data storage and maintenance. *International Journal of Digital Multimedia Broadcasting*, 2010:1–11, 2010. ISSN 16877578. doi: 10.1155/2010/720251. URL https://www.hindawi.com/journals/ijdmb/2010/720251/.

[121] P2P Foundation. Zooko's Triangle, 2014. URL https://wiki.p2pfoundation.net/Zooko%27s_Triangle.

[122] B. Paynter. How Blockchain Could Transform The Way International Aid Is Distribute, 2017. URL https://www.fastcompany.com/40457354/how-blockchain-could-transform-the-way-international-aid-is-distributed?platform=hootsuite.

[123] M.E. Peck. Do You Need a Blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum*, pages 58–60, 10 2017.

[124] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 2007. ISSN 0742-1222. doi: 10.2753/MIS0742-1222240302.

[125] Frank Pega, Stefan Walter, S.Y. Liu, R. Pabayo, S.K. Lhachimi, and R. Saith. Unconditional cash transfers for reducing poverty and vulnerabilities: effect on use of health services and health outcomes in low- and middle-income countries. *Cochrane Database of Systematic Reviews 2014*,, (6):1–18, 2014. doi: 10.1002/14651858.CD011135.www.cochranelibrary.com.

[126] W.W. Powell. Neither Market Nor Hierarchy: Network Forms of Organization. *Research in Organizational Behavior*, 12:295–336, 1990.

[127] Red Cross Movement. M3_3_2_1 Targeting criteria, 2017. URL http://webviz.redcross.org/ctp/docs/en/1.toolkit/Module3ResponseAnalysis/M3_3Targeting/M3_3_2Identifytargetingcriteria&mechanisms/M3_3_2_1Targetingcriteria.docx.

[128] K. Robles and S. Appelcline. Hierarchical Deterministic Keys for Bootstrapping a Self-Sovereign Identity, 2016. URL https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/draft-documents/hierarchical-deterministic-keys-for-bootstrapping-a-self-sovereign-identity.md.

[129] Nate Rush. Making the uPort Smart Contracts Smarter – uPort – Medium, 2017. URL https://medium.com/uport/making-the-uport-smart-contracts-smarter-e1798d8c1cf9.

[130] J. Sachs. *The End of Poverty: How We Can Make It Happen in Our Lifetime*. Penguin Books, London, UK, 2005. ISBN 978-0143036586.

[131] P. Sandner. Comparison of Ethereum, Hyperledger Fabric and Corda, 2017. URL https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6.

[132] W. R. Scott. *Institutions and Organizations*. Sage Publications, Thousand Oaks, 1995. ISBN 1452242224.

[133] Kris Shrishak. *Enhancing the Privacy of Users in eID schemes through Cryptography*. PhD thesis, Delft University of Technology, 2016.

[134] Thomas J. Smedinghoff. Solving the legal challenges of trustworthy online identity. *Computer Law and Security Review*, 28(5):532–541, 2012. ISSN 02673649. doi: 10.1016/j.clsr.2012.07.001. URL http://dx.doi.org/10.1016/j.clsr.2012.07.001.

[135] Ian Sommerville. *Software Engineering: (Update) (8th Edition) (International Computer Science)*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2006. ISBN 0321313798.

[136] Sovrin Board of Trustees. Sovrin Provisional Trust Framework Sovrin Provisional Trust Framework. 2017. URL https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Provisional-Trust-Framework-2017-06-28.pdf.

[137] Sovrin Foundation. Sovrin ™ : A Protocol and Token for Self- Sovereign Identity and Decentralized Trust. 2018.

[138] Sovrin Foundation. Sovrin, 2018. URL https://github.com/sovrin-foundation/sovrin.

[139] M. Sporny and D. Longley. A Web-based Ledger Data Model and Format, 2016. URL https://www.w3.org/2016/04/blockchain-workshop/interest/sporny-longley.html.

[140] T. Stahli. *Managing Identity on the Blockchain - The Future of Beneficiary Registration in Humanitarian Cash Transfer Programmes?* PhD thesis, The Graduate Institute of International and Development Studies, 2018.

[141] L. Stevens. Interview with Angelika Kessler on 7-3-2018, 2018.

[142] The Digital Responder. The GDPR is a unique opportunity to get humanitarian data protection right, 2017. URL https://thedigitalresponder.wordpress.com/2017/12/30/the-gdpr-is-a-unique-opportunity-to-get-humanitarian-data-protection-right/.

[143] The World Bank Group. Managing Risk, Promoting Growth: Developing Systems for Social Protection in Africa—Africa Social Protection Strategy 2011–2021. Technical report, The World Bank, Washington, D.C., 2012.

[144] The World Bank Group. Digital identity: towards shared principles for public and private sector cooperation. Technical report, GSMA/The World Bank Group/Secure Identity Alliance, Washington, D.C., 2016.

[145] The World Bank Group. Technical Standards for Digital Identity: Draft for Discussion. Technical report, International Bank For Reconstruction and Development/The World Bank, Washington, D.C., 2017.

[146] The World Bank Group. Identification for Development (ID4D), 2017. URL http://www.worldbank.org/en/programs/id4d.

[147] TU Delft. Systeemmodellering 2, 2014.

[148] UC Berkeley School of Information. Attribute Based Credentials - Privacy Patterns. URL https://privacypatterns.org/patterns/attribute-based-credentials.

[149] UN OCHA. Global Humanitarian Overview 2017. Technical report, United Nations, New York City, 2016. URL https://reliefweb.int/sites/reliefweb.int/files/resources/GHO_2017_publication_corrections_digital.pdf.

[150] UNICEF. UNICEF announces collaboration with telecommunications giant in drive for 'Big Data' for social good. URL https://www.unicef.org/media/media_95005.html.

[151] UNOPS. RFI Blockchain-based International Assistance, 2017. URL https://drive.google.com/file/d/0B--8okvw4smiUkxGN1N2UEwtOUE/view.

[152] USAID. Identity in a Digital Age: Infrastructure for Inclusive Development. Technical report, USAID, Washington, D.C., 2017. URL https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf.

[153] Bartel Van De Walle and Tina Comes. On the Nature of Information Management in Complex and Natural Disasters. *Procedia Engineering*, 107:403–411, 2015. ISSN 18777058. doi: 10.1016/j.proeng.2015.06.098. URL http://dx.doi.org/10.1016/j.proeng.2015.06.098.

[154] Bartel Van De Walle, Gerd Van Den Eede, and W. Muhren. Mobile Response. In J. Löffler and M. Klann, editors, *LNCS*, number May, pages 12–21. Springer-Verlag, 2009. ISBN 978-3-642-00439-1. doi: 10.1007/978-3-642-00440-7. URL http://link.springer.com/10.1007/978-3-642-00440-7.

[155] Piet Verschuren and Rob Hartog. Evaluation in design-oriented research. *Quality and Quantity*, 39:733–762, 2005. doi: 10.1007/s11135-005-3150-6.

[156] W3C. Decentralized Identifiers (DIDs) v0.10, 2018. URL https://w3c-ccg.github.io/did-spec/.

[157] Mike J Walker. Hype Cycle for Emerging Technologies, 2017. Technical report, Gartner, Inc., 2017. URL http://www2.caict.ac.cn/zscp/qqzkgz/qqzkgz_zdzsq/201708/P020170831493337899927.pdf.

[158] Mark Walport. Distributed ledger technology: Beyond block chain. *Government Office for Science*, pages 1–88, 2015.

[159] Oliver E. Williamson. Transaction Cost Economics: How It Works; Where It is Headed. *De Economist*, 146(1):23–58, 1998. ISSN 0013063X. doi: 10.1023/a:1003263908567. URL http://dx.doi.org/10.1023/A:1003263908567.

[160] Oliver. E. Williamson. The New Institutional Economics: Taking Stock , Looking Ahead. *Journal of Economic Literature*, XXXVIII(September):595–613, 2000. ISSN 0022-0515. doi: 10.1257/jel.38.3.595.

[161] Kelce S Wilson and Larry Plonsker. Some Blockchain Architecture Design Choices. 2008. URL http://www.the-blockchain.com/docs/SomeBlockchainArchitectureDesignChoices-WilsonandPlonsker.pdf.

[162] Greg Wolfond. A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review*, 7(10):35–40, 2017. ISSN 1927-0321. doi: http://doi.org/10.22215/timreview/1112.

[163] Larry E. Wood. Semi-structured interviewing for user-centered design. *Interactions*, 4(2):48–61, 1997. ISSN 10725520. doi: 10.1145/245129.245134. URL http://portal.acm.org/citation.cfm?doid=245129.245134.

[164] Peter Yeoh. Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, 25(2):196–208, 2017. ISSN 1358-1988. doi: 10.1108/JFRC-08-2016-0068. URL http://www.emeraldinsight.com/doi/10.1108/JFRC-08-2016-0068.

# F

# Scientific Article

# Self-Sovereign Identity Systems for Humanitarian Interventions

## A Case Study on Protective Cash Transfer Programs

L. Stevens
Delft University of Technology
The Netherlands

*Situation:* Information management enables humanitarian organizations to make adequate interventions based on timely, appropriate and trustworthy information. A crucial type of information are identities, because they can be used to assess vulnerability and efficiently manage aid distribution. Vulnerability determines who receives aid first because resources are always limited. This information is increasingly being stored and processed in identity systems.
*Complication:* Most identity systems are centralized and produce analogue proofs of identity such as passports or ID cards. These systems are susceptible to privacy and data breaches. Centralization leads to single-points-of-failure and could lead to fraudulent behavior resulting in people lacking formal proofs of identity. In general there is limited interoperability between identity systems and limited collaboration between the owners of these systems.
*Approach:* To create an interoperable and shared digital identity system using a Design Science Research strategy and systems engineering approach. This system must be distributed, protect privacy and put the identity owner in control of his or her data. The foundation of the system consists of Humanitarian Information Management principles, Privacy-by-Design principles and Self-Sovereign Identity principles. This research creates a functional blockchain based system, that enables identities for the use-case of Cash Transfer Programs.
*Results:* We present a validated set of ten design decisions that represent the trade-offs that have been made and prescribe a blueprint for a technical design.
*Next steps:* Future research should be done on how such a system could be implemented and used. This would require a process design approach that has to be developed, Also, elaborate research into user experience and user interfaces should be conducted.

*Keywords:* Cash Transfer Programs, Self-Sovereign Identities, Blockchain, Design Science Research, Decentralized Identifiers

## 1. IDENTITY AND DATA SHARING WITHIN THE HUMANITARIAN SECTOR

Climate related disasters, geophysical catastrophes, armed conflicts and man-made environmental emergencies are becoming more frequent (Development Initiatives, 2017). The effects are often mutually reinforcing, severe, immediate and have a ripple effect (Pega et al., 2014). In 2010, approximately 500 million people lived in an uncertain and destructive environment (Guha-Sapir & D'Aoust, 2010). This was even before the Syrian conflict and Ebola crisis struck. In the Global Humanitarian Overview 2017, published by UN OCHA[1], an estimated 128.6 million people were in humanitarian need for which $22.2 billion is required for relief. Almost a 10-fold increase of what was needed in 1992 when the appeal for funding humanitarian needs was started (UN OCHA, 2016, p.5). All the while, the necessary resources to overcome or prevent the devastating outcomes of these disasters, remain limited. Therefore, NGOs, governments and humanitarian organizations are in search of more efficient and effective methods for intervention (Brien et al., 2017) and in the meantime, direct their resources to those who are most vulnerable.

Adequate interventions are enabled by timely, appropriate and trustworthy information. This makes information management (IM) a crucial activity. IM is empowered by using information technology (Van De Walle, Van Den Eede, & Muhren, 2009). *Information systems* (IS) merge information technology with work processes, and constitutes of six activities: "information capturing, transmitting, storing, retrieving, manipulating and displaying" (Van De Walle et al., 2009, p.13). Information systems gather data which "facilitate various institutional process improvements, such as data-driven decision making, increased efficiency, or greater transparency and accountability. These process improvements, in turn, enable the system to contribute to functional goals"(USAID, 2017, p.19). Humanitarian organizations are increasingly using information systems to increase efficiency and have joined the data revolution (Gonzalez Morales, Hsu,

[1]United Nations Office for the Coordination of Humanitarian Affairs

Poole, Rae, & Rutherford, 2014). Information systems are also used to optimize the designation of resources to vulnerable people. For example, to establish whether someone satisfies the vulnerability criteria, *identity systems* are consulted. Identity systems help in identifying and registering people, consisting of software, hardware and procedures (The World Bank Group, 2017b). In many nation states, providing identities is institutionalized by the government, in which identity attributes (e.g. biometrics, birth certificates, land-titles) are registered and issued as an analogue legal identity in the form of a passport or ID-card. These legal identities are considered a very strong proxy for trust and can be used to identify oneself at government departments, banks, telecommunication operators, insurance companies and the like (Gelb & Decker, 2012). Identities are a crucial part of information in many humanitarian operations, but the existing identity systems turn out flawed in such contexts:

- Information management by humanitarian organizations often takes place in dynamic, complex and chaotic environments, this frustrates coordination and collaboration in identity IM (Van De Walle & Comes, 2015);
- Investments in identity systems result in sector silos, which reduces interoperability and limited scalability (The World Bank Group, 2017b);
- 1.1 billion people have no official means to prove their identity, with the majority living in Africa and Asia (The World Bank Group, 2017a). Either because their existence is not acknowledged by the central institutions providing non-digital identities or because they are otherwise incapable of acquiring one, for example due to high costs, long travel distances or the lack of birth certificates.
- Most identity systems are centralized or federated (Smedinghoff, 2012; Wolfond, 2017; Dunphy & Petitcolas, 2018) this makes them susceptible to mass surveillance, individual surveillance and data breaches due to a single-point-of-failure (Nyst, Makin, Pannifer, & Whitely, 2016)

These obstacles should be mitigated to ensure secure, private and usable identity systems (Jacobovitz, 2016). A humanitarian identity system that tackles these challenges is yet to be designed. The final form of a system is a result of a process design in which participants interact and implement the system according to their (changing) preferences, which requires a technical and institutional design to be flexible. According to systems engineering practices, this design should not only constitute a technical perspective but also an institutional viewpoint and a process design to be successful.

## 2. DESIGN PRINCIPLES AND BLOCKCHAIN TECHNOLOGY

In this research we will present a technical and institutional design that is flexible as to best accommodate this future process design, but the actually design this process is left out of scope. The technical and institutional design shall be presented as a set of design decisions because they simulate trade-offs based on several collections of design principles or guidelines. First, we resort to Humanitarian Information Management Principles (HIMP), which aim for collaboration, inclusiveness and interoperability OCHA. Although HIMP are not always complied with in reality as a result of the turbulent humanitarian context Van De Walle and Comes, they can be used to embed sector-wide coordination in a design and potentially break up information silos. HIMP focuses on the data controllers and data processors, thus it can be complemented with a data subject perspective that is provided by the Privacy-by-Design (PbD) principles written down by Cavoukian (2009). PbD embeds data protection for the data subject into a design. Unfortunately, both HIMP and PbD do not deal with the issue of centralization. There is a good reason for that: there was no fruitful way to do it when they were developed. Centralization was necessary to grant the trustworthy value that official identities hold, but this has its downsides. With the conception of blockchain technology this could be the past. To grasp this, one first needs to understand what a blockchain is.

A blockchain is a digitally distributed ledger, which is almost immutable, append-only and borderless. In essence, blockchain is simply a way to structure data. All data on a blockchain is digitized which eliminates the need for paper and manual documentation (Deloitte, 2017). So instead of relying on an analogue, hard-copy identity like a passport, one can rely on a digital identity. Specific information is stored in a block of data which is cryptographically sealed, chronologically stored with a permanent time-stamp and thus providing a trace of data transactions (Deloitte, 2017). These blocks should not contain any personal details but could contain references to securely and locally stored private information. Each node in the network holds a copy of the ledger, hence the term "distributed", of the data which is automatically updated when everyone in the network agrees on an updated version of the ledger (Deloitte, 2017). Blockchain facilitates the formation of self-sovereign identities. Self-sovereignty is about data subjects owning and controlling their own identity, this is possible in a distributed system with no single authority (Baars, 2016). Since this technology does not require one or multiple central authorities to provide a trustworthy data record but rather relies on consensus and strong cryptographic properties, it could tackle challenges concerning the power of central institution, security and privacy. Allen (2016), in a seminal blogpost, proposes a set of Self-Sovereign Identity (SSI) principles.

Table 1
*Overview of Principles based on Allen (2016), Cavoukian (2009) and OCHA (2002)*

| Principles | Source | Rationale |
|---|---|---|
| Existence | SSI | Users must have an independent existence |
| Control | SSI, PbD | Users must control their identities |
| Access | SSI | Users must have access to their own data |
| Transparency | SSI, PbD | Systems and algorithms must be transparent |
| Persistence | SSI, HIMP | Identities must be long-lived |
| Portability | SSI | Information and services about identity must be transportable |
| Interoperability | SSI, HIMP | Identities should be as widely usable as possible |
| Consent | SSI | Users must agree to the use of their identity |
| Minimalization | SSI, HIMP | Disclosure of claims must be minimized |
| Minimization | SSI, HIMP | Only relevant data is collected |
| Protection | SSI, PbD | The rights of users must be protected |
| Proactive; Preventative | PbD | Design for it in advance, prevent incidents from happening |
| Privacy by Default | PbD | Privacy must be embedded in the design as the default |
| Humanity | HIMP, PbD | System must do no harm |
| Accessibility | HIMP | Each humanitarian actor must have access |
| Inclusiveness | HIMP | System must stimulate collaboration and partnership |
| Accountability | HIMP | System must evaluate the reliability and credibility of the data |
| Objectivity | HIMP | A variety of data sources must be used |
| Timeliness | HIMP | Data must be collected, analyzed and disseminated efficiently |

The three sets of principles, can be combined into one comprehensive list, as can be seen in table 2. To use this trio as a guideline is new. Consequently, we do not know what such a system would look like. Therefore a case study on a specific type of humanitarian assistance, Cash Transfer Programs (CTPs), is conducted. The remainder of this article is build up as follows. In the next paragraph this case study is introduced and the research design is discussed. In paragraph 4, the role identity plays in CTPs and the results are presented. In paragraph 5 we will discuss these results and conclude this study.

## 3. DESIGN SCIENCE RESEARCH FOR CASH TRANSFER PROGRAMS

Cash Transfer Programs (CTPs) are humanitarian interventions that can be implemented as an alternative or in parallel to in-kind assistance. CTPs are increasingly popular (Barder et al., 2015) and can be defined as: "..programs that provide non-contributory cash grants to selected beneficiaries to satisfy minimum consumption needs" (Garcia & Moore, 2012, p. 18). A CTP can have a *protective* aim, where they assure that people continue to live on a basic level of welfare and do not endure permanent losses as the result of a disaster. A CTP can also *prevent* people from falling into poverty in the first place or *promote* people out of poverty (Garcia & Moore, 2012). All three types of CTPs should, when conducted, be organized by national or local governments, yet usually only the latter two are. During disasters CTPs are carried out with permission of the authorities, but they are themselves incapable or unwilling to do so (Pega et al., 2014; Arnold, Conway, & Greenslade, 2011; Garcia & Moore, 2012). This gives the humanitarian organizations a mandate to use digital identity systems in protective CTPs, which is why this research focuses on protective CTPs.

The set of design decisions is the final result of a Design Science Research (DSR) strategy and systems engineering approach. The strategy lays out the phases of this research, while the systems engineering defines the mind-set. The DSR strategy is often used in IS research and applied to wicked problems (Johannesson & Perjons, 2014). For a wicked problem there are no off-the-shelf solutions and requirements are unknown or unstable (Churchman, 1967). Hence, DSR strategy is a good fit. The same goes for systems engineering which is often used for complex socio-technical issues. Balancing the difficult to understand blockchain technology with the tangled humanitarian governance structures and challenging environments, requires a systems engineering perspective that meticulously demarcates the solution space. In line with DSR theory by Johannesson and Perjons (2014) a research design was set-up. The first step was a system analysis consisting of a technical, institutional and stakeholder viewpoints. Desk research and a literature review provided the input for this analysis and the results were validated using semi-structured interviews. A decision was made to focus on three sets of principles. The second step was to develop a program of requirements based on these principles. In the third step a comparative analysis of four blockchain based identity systems was conducted and mapped against the program of requirements. This generated alternatives for the design and made clear where trade-offs had to be made, resulting in ten design decisions. In figure 1 it is visualized how the principles are embedded in the design decisions. In

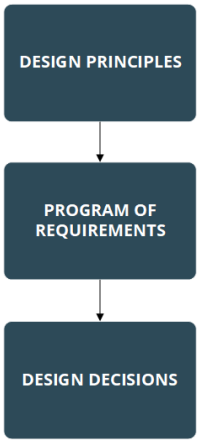



*Figure 1*. From principles to design decisions

the appendix the full traceability is provided. Step 4 demonstrated the potential use of these design decisions and discusses an expert validation, upon which a second version of the design decisions was generated.

## 4. DESIGN CHOICES

Before going in to the results of the research, it is of importance to better understand how protective CTPs work and how identity is an integral part of it.

### 4.1. The case of Protective Cash Transfer Programs

At the start of every CTP lies a geographical demarcation and a market survey to establish whether a local market is responsive or bound to be responsive at the time of cash disbursement. If not, an in-kind assistance program would be preferred. The design and development of a protective CTP is done by using guidelines of which many exist and which are often organization specific. Two general toolkits are provided by the ICRC[2] and the Cash Learning Partnership[3] (CalP). Synthesizing the steps and phases provided in these toolkits results in a generic flow diagram that is presented in figure 2. First a CTP is initiated, which can be done by a humanitarian organization or a government, but in all cases the local or national government must approve the initiative. Then a CTP is planned and designed. One can distinguish six design components: Objectives, Monitoring & Evaluation, Transfer Amounts, Targeting & Registration Method, Time Frames and Transfer Mechanism (Best Use of Resources Initiative, 2015; Harvey & Bailey, 2011). In the second step, the operational program is created which entails what distribution channels are used, who is involved and other practical details. Then the potential beneficiaries are targeted, done based on the vulnerability criteria that are defined in the planning phase. Criteria can be related to the disaster, have to do with socio-economic and demographic variables or focus on specific vulnerable groups (Red Cross Movement, 2017). The people that meet the criteria are then registered and identified. The cash can be distributed either as a conditional (specific rules for spending apply) or unconditional cash grant. Lastly the humanitarian organizations monitor the spending by doing follow-up interviews, focus groups and market surveys. This structure of events demonstrates the importance of identities for targeting, of assuring the right people receive assistance for a pre-specified number of times and for monitoring. Identity here has a functional purpose and is instrumentally used, or, in other words, it has a single purpose for humanitarian (cash based) assistance with an organization (USAID, 2017). In areas where multiple humanitarian organizations operate, this means people receive several functional identities and in some cases lead to people being "NGO fatigued" due to the many inquiries and data collections (Fabres, 2011).

There are several methods for targeting of which community based targeting and categorical selection are frequently used. Categorical selection is based on the selection criteria and people are either in or out the category, while community based targeting invites local representatives to have a say in who is included or not. Both of these methods are suboptimal, as including local representatives introduces local bias (Kelaher & Dollery, 2008) and categorical selection is highly dependent on the available data which is often scarce (Brooy, 2007). Once a list of people is set up, they should be registered and identified. Identification can also be seen as authentication, are the people listed as who they say they are and do they really meet the criteria.

Identities in CTPs are registered, validated and stored by the use of several information and identity systems. Sometimes comprehensive software is used, such as PIRS from the International Organisation for Migration (IOM) or BIMS from the UNHCR. But the turmoil in disaster environments does not always allow for state-of-the-art options to be used, so excel-sheets stored on local laptops and paper-based lists are still frequently used. We can see that these systems, combined with manual targeting, are prone to targeting errors, fraud and selection biases. Kebede (2006) finds that targeting errors might make the most vulnerable even worse off, because the scarce amount of resources can be bought by even fewer people. Within these systems there is a high degree of centralization and information siloes, i.e. there is little collaboration or interoperability. People that are selected for CTPs are unable to control their identities and have to trust humanitarian organizations will handle their data securely and respect their privacy. One could wonder about the emphasis on privacy in these crisis situations. However, recalling any ethnic cleansing or genocide, one can understand the importance of protecting personally and demographically

[2] http://rcmcash.org/

[3] http://www.cashlearning.org/toolkits/cash-toolbox

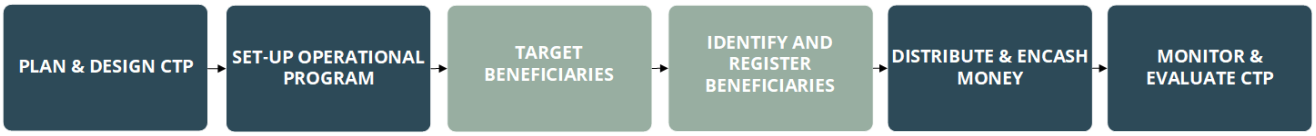



*Figure 2*. Flowdiagram of a Cash Transfer Program

identifiable information.

To summarize, identities play an integral part in CTPs. They allow for registration, monitoring and targeting of people that are in dire need of cash-based assistance. The identity systems used for CTPs come across similar and more context specific challenges that identity systems deal with. These realizations legitimize the application of a blockchain based self-sovereign identity system which can be designed for the purpose of collaboratively managing identities in an interoperable system.

### 4.2. Ten Design Decisions

So how would such a system look? In this article we propose a set of design decisions to convey this system design as it illustrates making trade-offs. These design decisions have been validated by translating them into BPMN and UML Class diagrams, furthermore the set has been validated by five experts. The experts had backgrounds in blockchain development, blockchain identities, generic identity management and humanitarian IT systems. In the following paragraphs the final version of the design decisions stemming from this research are discussed. To be clear, the first decision is to use blockchain as we must acknowledge that blockchain is no holy grail and other alternatives are out there.

**Design Decision #1: Use Blockchain Technology.** The decision for blockchain is made because it enables self-sovereignty, uses very strong encryption and because it encodes trust partly into the system. The openness of blockchain technology stimulates organizations to behave correctly which might improve collaboration between humanitarian organizations. Yet, blockchain is a nascent technology which comes with uncertainties. Also, there are multiple blockchains being developed for similar use-cases (not necessarily humanitarian) that could increases the overall inefficiencies of blockchains. One could question whether the humanitarian sector has the mandate to participate in this rat race, but at least the sector has a good use case. In case multiple blockchains are developed than at least these systems should be extremely interoperable.

**Design Decision #2: Use a Public Permissioned chain.** A public permissioned chain is open to all for registration of their identities, which people could do themselves if they own a device or could otherwise do at a registration terminal. To create and update blocks, nodes in the network should have certain authorities. This does interfere with the concept of at truly self-sovereign system, but it resembles the current governance system more which could favour implementation. A public permissioned chain does not fully encapsulate trust in a system, so there is a need for a trust-framework outside the technical system. This might create a barrier, because a group of individuals or organizations either allows or disallows organizations to join, in the meanwhile it also creates a buy-in and could yield a larger effort to make it successful. Lastly, permissioned chains are much more scalable than permissionless chains and its growth can be controlled (Hileman & Rauchs, 2017). This control can be an attractive feature for participants that might be weary of this new technology.

**Design Decision #3: Use Decentralized Identifiers and a fully User-centred System.** Each identity system needs an identifier that uniquely identifies an entity in the system. To make sure no double identifiers exist central authorities are often in charge of handing them out. However, blockchain and in specific decentralized identifiers (DIDs) require no central authorities to ensure uniqueness. On top, DIDs are a W3C standard which ensures interoperability and flexibility as they can be used on any blockchain. DIDs are pairwise pseudonymous, which means that they are only used between one identity owner and one other party (W3C, 2018). DIDs enable a fully user-centred design, which allows the identity owner to take full control of his or her identity and initiate all contact with other participants in the network (Sporny & Longley, 2016). An identity owner can have several hundred DIDs, for each digital relationship there is one. Only the DIDs are stored on the blockchain, which upon initiation of the owner can reveal a means of contact without storing any private information on the blockchain. The connection can be revoked when the owner wishes to. In figure 3 the workings of this user-centred design and DIDs is presented. In this scenario the identity owner has already acquired a basic digital identity. So the identity owner request a validated credential, for example a date of birth. The attribute provider has its own registry of information and provides a credential based on the information in that registry, signs the credential of which a public part is stored on the blockchain so it becomes clear for everyone in network that this particular attribute provider has signed it. The attribute provider then issues the credential, upon which the identity owner countersigns. To request a service with a service provider, or in this case a humanitarian organization that executes a CTP, the identity owner connects with the service provider. The service provider then sends an inclusion algorithm, that

the identity owner can fill in with credentials. It sends back whether the criteria are met and who has signed the credentials, the service provider can then check if it trusts the attribute providers.

**Design Decision #4: Use Hyperledger Indy as a Blockchain.** There are several permissioned blockchains that can be used. We chose Hyperledger Indy as it is developed specifically for self-sovereign identities, embeds privacy-by-design principles, is public permissioned and has a wide support of powerful international organizations Sovrin and TYKN. Using the roles provided by Hyperledger, only humanitarian organizations can be made service providers. This enables a functional purpose for CTPs.

**Design Decision #5: Use a GPLv3 license.** If the whole humanitarian sector should be able to use the system, it should not be made proprietary. This could make the system less attractive for others to join. There are several open source licenses, the GPLv3 is strongly protective and requires other users or developers to instantly open up their versions of the system (Hess, 2014). It does allow for commercial use, which might be frowned upon since it is realized with non-profit funds. This way of licensing the system, creates transparency for all stakeholders involved. The level-playing field is equal, which could bring more organizations to the table. A potential drawback is that it could result in free-rider behavior.

**Design Decision #6: Use Hyperledger Indy Roles and matching Interfaces.** Within Hyperledger Indy there are several roles. The highest in rank are the Trustees, which can be seen as a board of directors for the system. They appoint Stewards who run two types of nodes (Hyperledger, 2018). Validator nodes that can write and update the blockchain, and observer nodes that give reading access to the blockchain. Stewards appoint Trust Anchors, which can be identity providers, attribute providers or service providers. The users in the system are called identity owners or Custodians. The former control their own identity while the latter control the identity for somebody else. All communication between Trust Anchors, identity owners and Custodians is done outside of the blockchain via software agents. For this a Decentralized Public Key Infrastructure (DPKI) is used, that "is a collection of internet technologies that provides secure communications in a network" (Hyperledger, 2017) which requires no central authority.

**Design Decision #7: Offchain storage is to be determined by context.** For privacy purposes, only the DIDs and public-faced credentials are stored on the blockchain. All other information has to be stored offchain. Most notably the private key that gives access to an Identity Wallet holding all the DIDs for one person is stored offchain. This can be done on a personal device, if available, or on paper. The raw identity attributes or self-attested claims, e.g. identity attributes that have not been validated yet, can also be stored on the device or on paper. Each identity owner should have a backup available, which can be made via the software agents. This backup holds some centrality since it is stored via the software agents which can have multiple options available such as secure cloud storage's (positive for scaling purposes), Highly Secure Modules or Smartcards. The same applies here: it depends on the context which software agent is used. Several options exist and each option should be as safe and secure as possible.

**Design Decision #8: Social and offline key recovery, two-factor authentication and centralized account protection.** Self-sovereignty implies that key loss should also be arranged in a decentralized fashion, yet there are no solutions out there to prevent a permanent key loss. Additionally, a key loss might result in someone else taking over the account and misusing an identity. In this humanitarian context it could make people even worse off, as vulnerable people would now be the ones without digital identities. This must be prevented and therefore some of the centrality that is already included in the system by the permissioned architecture, is utilized as a means to retrieve access. Several techniques such as multi-signature signing (BitGo, 2018) or hierarchical deterministic key pairs (Robles & Appelcline, 2016) can be exploited to achieve this feat. Alongside, social recovery which comprises of assigning trusted peers in the network to recover a key or using an offline back-up to restore access are also offered. Finally, two-factor authentication (biometrics plus passphrase) can be used to access the account at centralized computer terminals in case of private key loss.

**Design Decision #9: Targeting is seen as a service not as a separate activity.** The system is designed with a functional purpose: providing a tool for interoperable and collaboratively managing of identities to improve targeting, identification and registration in CTPs. In the current practice, targeting is initiated by humanitarian organizations based on a set of inclusion criteria. Via various targeting mechanisms people are selected, which can result in inclusion errors, fraud and is time consuming. If targeting is seen as a service, than people should only be informed about its existence, how and when they can apply for the service. Using an inclusion algorithm that is send to the identity owner which verifies the credentials and matches it to the inclusion criteria, little bias is included and an objective inclusion score is retrieved. One could imagine people subscribing to a newsfeed in which all participants of the network can publish their CTPs and inclusion criteria, the identity owner can then reach out him/herself.

**Design Decision #10: Validation by attribute provider and appointed validator.** Many self-sovereign systems provide peer-validation, but its value is difficult to establish. It could be transformed into a trust score of sorts, but then the peers that validate must provide some kind of public validation which can be related to each other. Within a human-

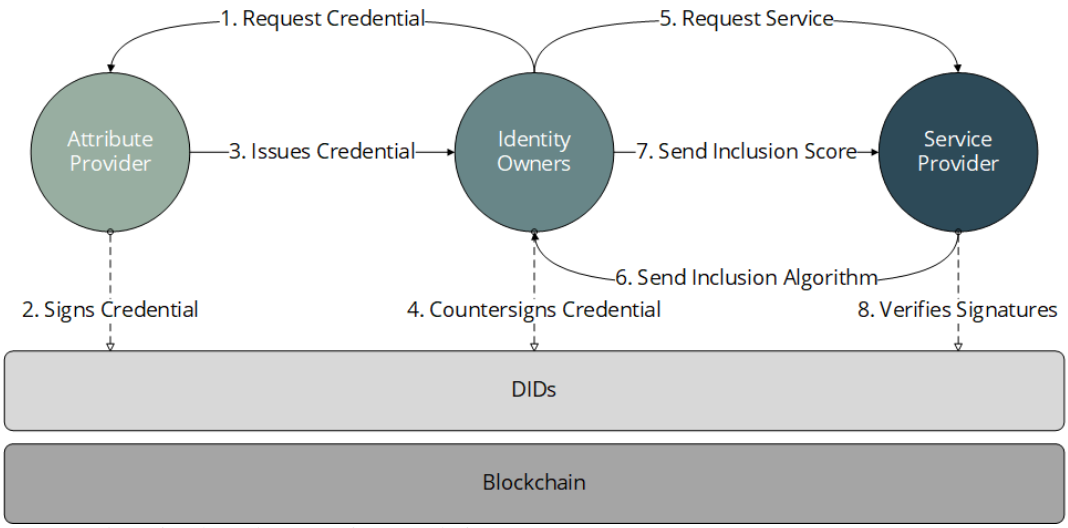



*Figure 3*. User-centred Design based on Sovrin Foundation (2018)

itarian context this is not preferable, since it could demographically classify groups of people. On the other hand, humanitarian organizations often collaborate with volunteers or community representatives that also sensitize the community for CTPs and have local knowledge. This creates the need for some peers to be able to validate in the field, but only if they are authorized by humanitarian organizations or other attribute providers. Validation is also possible by attribute providers that already hold some information on identity owners, for example schools, municipalities and tax offices. These can be approached by the identity owner to validate specific attributes.

## 5. DISCUSSION

The design decisions combined present a prescription upon which a digital identity system for CTPs could be developed. They serve a functional purpose. Yet, in the wider context of humanitarian assistance and identity in general, we can reflect on the opportunities for the design decisions to also serve a foundational purpose. A foundational purpose implies that there is a single system useful for multiple purposes. E.g. beneficiaries could also use their digital identities for taking out insurance or acquiring a mobile phone contract. (USAID, 2017). This would give identity owners, attribute providers and service providers a continuous incentive to keep information up-to-date. It might be desirable to first develop this system with a functional purpose since CTPs are a suitable use case to create an installed base of identity owners. Especially since humanitarian organizations have a limited mandate outside times of distress, the value of an already functioning system might persuade nation states to join and create a foundational system with a continuous value proposition. The current design decisions do not immediately allow for this as only humanitarian organizations are allowed to provide services. Nonetheless if Stewards and Trustees decide to open-up the role for service provider, other non-humanitarian organizations could take on this role. National and local governments, other authorities but also private organizations could provide these services. In that case the system would also be useful for CTPs that have the purpose of promotion or prevention. This would truly break-up information silos within and outside of the humanitarian sector while protecting the privacy of each identity owner. The added value for collaboration and interoperability lies mainly in the provision of a tool, which could bring together all involved organizations in a process management approach. If the right process design is created which has an acceptable entry-barrier but makes it difficult for participants to leave the negotiation table, the set of design decisions could be transformed into a final technical and institutional design. So although blockchain takes away a lack of trust in data sharing and breaks up silos, working with blockchain based systems is not trustless, even more so if a permissioned chain is used (Hileman & Rauchs, 2017). Organizations might still distrust credentials given to identity owners and this is a problem technology alone will not solve and might not be solvable at all. Finally, the decision to go with a permissioned system comes with some centrality. Nevertheless, the privacy of people is better protected and there are no single-point-of-failures due to the distributed architecture. The permissioned character also allows for controlled growth of the system, which can be particularly important as existing programs and aid workers must have time to adapt.

## 6. CONCLUSION & FUTURE RESEARCH

This study takes a DSR strategy and systems engineering approach. Within the case study of CTPs we focus on creating a self-sovereign digital identity system with a functional

purpose. The unique combination of Humanitarian Information Management Principles (HIMP), Privacy-by-Design (PbD) principles and Self-Sovereign Identity (SSI) principles lays at the foundation of the ten design decisions above. This contributes to the academic knowledgebase as it combines the ideological concept of self-sovereignty is combined with the practical measures to improve collaboration and better protect the privacy of data subjects. We found that the design decisions, if taken out of the context of CTPs, can serve a foundational purpose but this is dependent on the specific roles of participants. Significant added value of this study can be found in that the design decisions can bring together important stakeholders as it offers flexibility, transparency and interoperability. Without these design decisions it would be much more difficult to get the right organizations around the table. Nonetheless, the critical decisions and final agreements shall be made collaboratively and require trust regardless of what a technical system can offer. Future research should therefore focus on how this process design might look. This should take in the current humanitarian governance structures, formal and informal powers and financial arrangements. The result of this research could be a concise participation model, proposed leading actors and process rules. Throughout the process the representation of the design principles should be monitored. Other future research has to be done on the preferences and needs of identity owners. Cultural differences, illiteracy, digital immaturity and ownership of devices, all play a role in how identity owners might perceive the system. This requires field-research, co-design sessions and translating the results into interfaces. Lastly, when the system has a more foundational purpose the information should be kept up to date by the community and identity owners themselves. Several researchers have already touched upon the theories of Elinor Ostrom and self-governance in relation to blockchain based systems, it would be interesting to see if this theory or other theories could be of assistance in composing the right environments and incentives to keep information up-to-date. This would truly realize a global digital identity system where information is up-to-date and in control of the people that it belongs to. Not only the humanitarian sector would benefit, but humanity in general.

## References


Allen, C. (2016). *The Path to Self-Sovereign Identity.* Retrieved from http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Arnold, C., Conway, T., & Greenslade, M. (2011). *Cash Transfers* (Tech. Rep.). Department for International Development.

Baars, D. (2016). *Towards Self-Sovereign Identity using Blockchain Technology* (Unpublished doctoral dissertation). Universtiy of Twente.

Barder, O., Blattman, C., Cameron, L., Egeland, J., Elmi, M., Faye, M., ... Woodman, L. (2015). *Doing cash differently: How cash transfers can transform humanitarian aid* (Tech. Rep. No. September). ODI. Retrieved from https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf doi: 2052-7209

Best Use of Resources Initiative. (2015). *Cost Efficiency Analysis: Unconditional Cash Transfer Programs* (Tech. Rep.). New York: IRC. Retrieved from https://www.rescue.org/sites/default/files/document/954/20151113cashcefficreportfinal.pdf

BitGo. (2018). *BitGo: Making Digital Currencies Usable for Business.* Retrieved from https://www.bitgo.com/info/solutions#custody

Brien, C. O., Scott, Z., Smith, G., Barca, V., Kardan, A., Holmes, R., & Watson, C. (2017). *Shock-Responsive Social Protection Systems Research Synthesis Report* (Tech. Rep. No. January). Oxford: Oxford Policy Management.

Brooy, J. L. (2007). A Weighted Welfare Analysis of Local Price Inflation. *Journal of Human Security*, *5*(2), 65–82.

Cavoukian, A. (2009). *Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices* (Tech. Rep.). Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf%5Cnwww.privacybydesign.ca doi: 10.1007/s12394-010-0062-y

Churchman, C. (1967). Guest editorial: Wicked problems". *Management sciences*, *14*(4), 141–142.

Deloitte. (2017). *Key Characteristics of the Blockhcain.* Deloitte Touche Tohmatsu India LLP. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-key-characteristics-noexp.pdf

Development Initiatives. (2017). *Global Humanitarian Assistance Report 2017* (Tech. Rep.). Bristol: Development Initiatives. Retrieved from http://devinit.org/wp-content/uploads/2017/06/GHA-Report-2017-Full-report.pdf

Dunphy, P., & Petitcolas, F. (2018). A First Look at Identity Management Schemes. *IEEE Security and Privacy Magazine*.

Fabres, B. (2011). Think Global, Act Global in the Mekong Delta? Environmental Change, Civil Society and NGOs. *Advances in Global Change Research*, *45*(1), 7–34. doi: 10.1007/978-94-007-0934-8

Garcia, M., & Moore, C. M. T. (2012). *The Cash Dividend*. Washington D.C.: The World Bank. Retrieved from http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-8897-6 doi: 10.1596/978-0-8213-8897-6

Gelb, A., & Decker, C. (2012). Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries. *Review of Policy Research*, *29*(1), 91–117.

Gonzalez Morales, L., Hsu, Y., Poole, J., Rae, B., & Rutherford, I. (2014). *A World That Counts* (Tech. Rep.). IEAG. Retrieved from www.undatarevolution.org

Guha-Sapir, D., & D'Aoust, O. (2010). *Demographic and Health Consequences of Civil Conflict* (Tech. Rep.). Washington, D.C.: The World Bank. Retrieved from http://wdr2011.worldbank.org/sites/default/files/pdfs/WDRBackgroundPaper-SapirandD'Aoust.pdf?keepThis=true&TB_iframe=true&height=600&width=800

Harvey, P., & Bailey, S. (2011). *Cash transfer programming in emergencies* (Vol. 44; Tech. Rep. No. 11). London: ODI. doi: 0855985631

Hess, K. (2014). *Decisions, decisions. How do you choose an open source license?* Retrieved from https://www.zdnet.com/article/decisions-decisions-how-do-you-choose-an-open-source-license/

Hileman, G., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study* (Tech. Rep.). Cambridge, UK: Cambridge Centre for Alternative Finance. Retrieved from https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf

Hyperledger. (2017). *Introduction âĂŤ hyperledger-fabricdocs master documentation.* Retrieved from http://hyperledger-fabric.readthedocs.io/en/release-1.1/blockchain.html

Hyperledger. (2018). *Getting Started with Libindy.* Retrieved from https://github.com/hyperledger/indy-sdk/blob/master/doc/getting-started/getting-started.md

Jacobovitz, O. (2016). *Blockchain for Identity Management* (Tech. Rep. No. December). Beer Sheva: Ben-Gurion University. Retrieved from https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Stockholm: Springer International Publishing. doi: 10.1007/978-3-319-10632-8

Kebede, E. (2006). Moving from emergency food aid to predictable cash transfers: Recent experience in Ethiopia. *Development Policy Review*, *24*(5), 579–599. doi: 10.1111/j.1467-7679.2006.00349.x

Kelaher, D., & Dollery, B. (2008). Cash and in-kind food aid transfers: The case of tsunami emergency aid in banda aceh. *International Review of Public Administration*, *13*(2), 117–128. doi: 10.1080/12294659.2008.10805125

Nyst, C., Makin, P., Pannifer, S., & Whitely, E. (2016). *Digital Identity : Issue Analysis Executive Summary* (Tech. Rep. No. June). Guildford, UK: Consult Hyperion.

OCHA. (2002). Best Practices in Humanitarian Information Management and Exchange. In *Symposium on best practices in humanitarian information exchange.* Geneva: United Nations Office for the Coordination of Humanitarian Affairs.

Pega, F., Walter, S., Liu, S., Pabayo, R., Lhachimi, S., & Saith, R. (2014). Unconditional cash transfers for reducing poverty and vulnerabilities: effect on use of health services and health outcomes in low- and middle-income countries. *Cochrane Database of Systematic Reviews 2014,*(6), 1–18. doi: 10.1002/14651858.CD011135.www.cochranelibrary.com

Red Cross Movement. (2017). *M3_3_2_1 Targeting criteria.* Geneva: International Red Cross and Red Crescent Movement. Retrieved from http://webviz.redcross.org/ctp/docs/en/1.toolkit/Module3ResponseAnalysis/M3_3Targeting/M3_3_2Identifytargetingcriteria&mechanisms/M3_3_2_1Targetingcriteria.docx

Robles, K., & Appelcline, S. (2016). *Hierarchical Deterministic Keys for Bootstrapping a Self-Sovereign Identity.* Retrieved from https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/draft-documents/hierarchical-deterministic-keys-for-bootstrapping-a-self-sovereign-identity.md

Smedinghoff, T. J. (2012). Solving the legal challenges of trustworthy online identity. *Computer Law and Security Review*, *28*(5), 532–541. Retrieved from http://dx.doi.org/10.1016/j.clsr.2012.07.001 doi: 10.1016/j.clsr.2012.07.001

Sovrin, & TYKN. (2018). *Paper Sovrin.*

Sovrin Foundation. (2018). *Sovrin âĎć : A Protocol and Token for Self- Sovereign Identity and Decentralized Trust* (No. January).

Sporny, M., & Longley, D. (2016). *A Web-based Ledger Data Model and Format.* Retrieved from https://www.w3.org/2016/04/blockchain-workshop/interest/sporny-longley.html

The World Bank Group. (2017a). *Identification for Development (ID4D).* Retrieved from http://www.worldbank.org/en/programs/id4d

The World Bank Group. (2017b). *Technical Standards for Digital Identity: Draft for Discussion* (Tech. Rep.). Washington, D.C.: International Bank For Reconstruction and Development/The World Bank.

UN OCHA. (2016). *Global Humanitarian Overview 2017* (Tech. Rep.). New York City: United Nations. Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/GHO_2017_publication_corrections_digital.pdf

USAID. (2017). *Identity in a Digital Age: Infrastructure for Inclusive Development* (Tech. Rep.). Washington, D.C.: USAID. Retrieved from https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

Van De Walle, B., & Comes, T. (2015). On the Nature of Information Management in Complex and Natural Disasters. *Procedia Engineering*, *107*, 403–411. Retrieved from http://dx.doi.org/10.1016/j.proeng.2015.06.098 doi: 10.1016/j.proeng.2015.06.098

Van De Walle, B., Van Den Eede, G., & Muhren, W. (2009). Mobile Response. In J. Löffler & M. Klann (Eds.), *Lncs* (pp. 12–21). Springer-Verlag. Retrieved from http://link.springer.com/10.1007/978-3-642-00440-7 doi: 10.1007/978-3-642-00440-7

W3C. (2018). *Decentralized Identifiers (DIDs) v0.10.* Retrieved from https://w3c-ccg.github.io/did-spec/

Wolfond, G. (2017). A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review*, *7*(10), 35–40. doi: http://doi.org/10.22215/timreview/1112

## APPENDIX

Table 2
*Overview of Principles based on Allen (2016), Cavoukian (2009) and OCHA (2002) and mapped to requirements*

| **Principles** | **Source** | **Rationale** | **Satisfied by Requirement** |
|---|---|---|---|
| Existence | SSI | Users must have an independent existence | R.1 |
| Control | SSI, PbD | Users must control their identities | R.2, U.3, U.4 |
| Access | SSI | Users must have access to their own data | U.1, U.3, U.4 |
| Transparency | SSI, PbD | Systems and algorithms must be transparent | C.3, C.13, C.15 |
| Persistence | SSI, HIMP | Identities must be long-lived | U.3, U.4 |
| Portability | SSI | Information and services about identity must be transportable | I.5 |
| Interoperability | SSI, HIMP | Identities should be as widely usable as possible | C.14, R.10 |
| Consent | SSI | Users must agree to the use of their identity | R.6, U.4 |
| Minimalization | SSI, HIMP | Disclosure of claims must be minimized | U.4 |
| Minimization | SSI, HIMP | Only relevant data is collected | R.4 |
| Protection | SSI, PbD | The rights of users must be protected | C5, C.6, C.7 |
| Proactive; Preventative | PbD | Design for it in advance, prevent incidents from happening | Integral to design |
| Privacy by Default | PbD | Privacy must be embedded in the design as the default | C.7 |
| Humanity | HIMP, PbD | System must do no harm | C.5 |
| Accessibility | HIMP | Each humanitarian actor must have access | C.10, C.11 |
| Inclusiveness | HIMP | System must stimulate collaboration and partnership | C.11, C.14 |
| Accountability | HIMP | System must evaluate the reliability and credibility of the data | T.3 |
| Objectivity | HIMP | A variety of data sources must be used | R.7, R.8 |
| Timeliness | HIMP | Data must be collected, analyzed and disseminated efficiently | T.7 |

Table 3
*Design decisions and system mapped onto program of requirements*

| ID | Requirement | Satisfied? | Decision |
|---|---|---|---|
| R.1 | Each Person Affected shall be able to register for one digital identity as an Identity Owner | **No** | **2,3** |
| R.2 | Each Person Affected shall be able to self-register or register by delegate | **Yes** | **2** |
| R.3 | Each Person Affected should add a geo-location when registering | **Yes** | **6** |
| R.4 | System shall only request a maximum amount of identity attributes | **Yes** | **2** |
| R.5 | System should check for double identities | **No** | **3** |
| R.6 | Humanitarian Organizations shall ask Person Affected to provide consent for the use of data | **Yes** | **4** |
| R.7 | Only humanitarian Organizations shall be able to register as an attribute provider, identity provider and service provider | **Yes** | **2,4** |
| R.8 | Community Representatives and Authorities should be able to register as an attribute provider | **Yes** | **2,4** |
| R.9 | Humanitarian Organizations, Community Representatives and Authorities must have an humanitarian registration interface | **Yes** | **6** |
| R.10 | System must allow all humanitarian organizations to become part of it | **No** | **1,2** |
| I.1 | A Person Affected shall be able to have identity attributes validated by several attribute providers | **Yes** | **3** |
| I.2 | Attribute providers shall be able to validate identity attributes and geolocations | **Yes** | **3** |
| I.3 | Attribute providers shall be able to issue verifying credentials | **Yes** | **3** |
| I.4 | Attribute providers must have an easy to use validation interface | **Yes** | **6** |
| I.5 | Person Affected must always be able to access his/her credentials in a private storage | **Yes** | **7** |
| U.1 | Person Affected must have an easy to use user-interface | **Yes** | **6** |
| U.2 | A Person Affected shall be able to request services throughout the system | **Yes** | **3** |
| U.3 | Person Affected shall be able to safely access, update, disclose and revoke their identities | **Yes** | **1,3** |
| U.4 | Person Affected shall be able to regain access to their identity after loss of control or loss of access | **Yes** | **8** |
| T.1 | Humanitarian Organizations shall be able to match Person Affected with their inclusion criteria | **Yes** | **9** |
| T.2 | Humanitarian Organizations must have a service interface for targeting | **Yes** | **6** |
| T.3 | Humanitarian Organizations shall be able to verify identities based on issued credentials from other organizations | **Yes** | **1,3** |
| T.4 | Humanitarian Organizations must only be able to set up inclusion criteria based on minimum amount of identity attributes | **Yes** | **9** |
| T.7 | Humanitarian Organizations should delete all information that is no longer necessary for a CTP project | **Yes** | **9** |
| C.1 | The system must have roles for Identity Owners, Attribute Providers, Service Providers and Identity Providers | **Yes** | **2,6** |
| C.2 | A Person Affected should be able to provide feedback during use of the system | **Yes** | **5** |
| C.3 | System should be able to provide open response to the feedback of people | **Yes** | **2** |
| C.4 | Humanitarian Organizations shall be able to create sub-entities to pass down responsibilities | **Yes** | **2,4** |
| C.5 | All participants and the system must safely store all information | **No** | **1,2,7** |
| C.6 | System must provide secure end-to-end encryption for all communication and sharing of data | **Yes** | **3** |
| C.7 | System must provide the highest form of privacy feasible | **Yes** | **1,4,7** |
| C.8 | System should enable an overview of where people have been registered | **Yes** | **6** |
| C.9 | System must demand high data standards for all humanitarian organizations | **Yes** | **2** |
| C.10 | System must be inclusive and accessible for all humanitarian organizations | **No** | **1,2** |
| C.11 | System must be accessible at all times | **Yes** | **1,2** |
| C.12 | System must be flexible and able to scale up | **Yes** | **1,2,4** |
| C.13 | System must be open-source | **Yes** | **5** |
| C.14 | System must use interoperable standards for digital identification | **Yes** | **1** |
| C.15 | System must open up the governance structure online | **Yes** | **2** |
| C.16 | System must have a functional purpose and grow into a foundational purpose | **Yes** | **2** |
| C.17 | System must be accompanied by a participation model and process approach | **Yes** | **2** |
| C.18 | System must not have a single owner | **Yes** | **1** |
| C.19 | System must have an incentive system to demonstrate good behavior | **Yes** | **2.4** |
| C.20 | Actors in the system shall be able to communicate with each other if communication is initiated by the Identity Owner | **Yes** | **3,6** |