A Survey on Blockchain for Healthcare

Challenges, Benefits, and Future Directions

Arbabi, Mohammad Salar; Lal, Chhagan; Veeraragavan, Narasimha Raghavan; Marijan, Dusica; Nygard, Jan F.; Vitenberg, Roman

DOI
10.1109/COMST.2022.3224644

Publication date
2022

Document Version
Final published version

Published in
IEEE Communications Surveys and Tutorials

A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions

Mohammad Salar Arbabi, Chhagan Lal, Narasimha Raghavan Veeraragavan, Dusica Marijan, Jan F. Nygård, and Roman Vitenberg, *Member, IEEE*

***Abstract*—Continuously generated volumes of health data make healthcare a data-intensive domain. This data needs to be collected, stored, and shared among different healthcare actors for various purposes, such as reporting, analysis, collaborative research, and personalized healthcare services. However, the existing data storage and exchange solutions in the healthcare domain exhibit several challenges related to, e.g., data security, patient privacy, and interoperability. Recently, the industry and research community turned its focus to the possible use of blockchain technology to solve some of these challenges in the healthcare domain. The blockchain technology along with the support from smart contracts is considered a salient facilitator for secure and efficient health data sharing. This is due to its unique features, such as decentralization, trustlessness, immutability, traceability, and transparency. In this paper, we provide a comprehensive survey of the state-of-the-art efforts that envision the use of blockchain-based solutions in the healthcare domain. To this end, we introduce a systematic framework for classifying and analyzing such systems. The framework consists of classification in several dimensions: interactions between healthcare entities, functional components of healthcare storage systems, challenges in the healthcare domain that can be overcome by using the blockchain technology, and benefits for healthcare storage systems derived from the fundamental features of the technology. When analyzing over 40 systems and solutions proposed in the state-of-the-art, we perform their rigorous placement by identifying the exact scope of each solution and mapping it to the above taxonomies of interactions, functional components, challenges, and benefits. We additionally provide an extensive discussion of compliance with privacy-related regulations of *General Data Protection Regulation (GDPR)* in EU, and *Health Insurance Portability and Accountability Act (HIPAA)*. Following the results of the analysis, we have outlined a number of important research gaps and future directions yet to be addressed.**

***Index Terms*—Health data, blockchain and smart contracts, security and privacy, health data collection, health data storage, health data sharing, healthcare interoperability, health data protection regulations.**

Manuscript received 25 May 2021; revised 31 January 2022, 21 June 2022, and 16 September 2022; accepted 12 November 2022. Date of publication 24 November 2022; date of current version 24 February 2023. This work was supported by the Research Council of Norway through IKTPLUSS Program under Grant 288106. *(Corresponding author: Mohammad Salar Arbabi.)*

Mohammad Salar Arbabi, Narasimha Raghavan Veeraragavan, and Roman Vitenberg are with the Department of Informatics, University of Oslo, 0316 Oslo, Norway (e-mail: mohamarb@ifi.uio.no).

Chhagan Lal is with the Department of Intelligent Systems, Cybersecurity Group, Delft University of Technology, 2600 GA Delft, The Netherlands.

Dusica Marijan is with the Department of Validation Intelligence for Autonomous Software Systems, Simula Research Laboratory, 0164 Oslo, Norway.

Jan F. Nygård is with the Department of Registry Informatics, Cancer Registry of Norway, 0304 Oslo, Norway.

Digital Object Identifier 10.1109/COMST.2022.3224644

I. Introduction

IN HEALTHCARE, a significant volume of data is continuously generated as a result of various medical procedures such as diagnostics, treatment and monitoring of patients, but also from clinical trails [1], [2]. Once collected, the health data (HD) is stored in the patients journal. As the patient is handled in the healthcare system, more data are generated and stored, as well as previous data are accessed.

In particular, the availability of current and previously generated data helps the doctors to make more informed medical decisions, which leads to the improvement of the quality of treatment received by a patient. Usage of data in this context is termed primary usage, i.e., individual data on a particular patients for the health care need for that particular patient.

Furthermore, secondary usage of HD, i.e., in-depth analysis of data for generation of medical knowledge, can result in the creation of new treatments and drugs [3], [4], [5].

However access to data and data sharing, both in the individual care of patients and for medical research, are difficult for several reasons. Strict regulations govern access to data and data sharing [4], [5], and security and privacy guarantees imposed by regulatory bodies [6], [7], [8], while data non-interoperability between different stakeholders exacerbate the problems [9], [10], [11], [12].

In the contemporary HD management scenarios, the sensitive nature of data forces the healthcare providers to keep data in a secure domain with several protective measures. These measures can include intrusion detection systems, network firewalls and encryption. The scattered structure of data storage throughout different healthcare systems lead to the creation of HD silos. These data silos cause obstacles for both effective collaborative patient health care and medical research. Therefore, new solutions for HD access and data sharing between multiple healthcare providers has been proposed in the literature [13], [14], [15], but these solutions have several shortcomings related to data security [2], user privacy [16] and compliance management [17]. Hence, there is a need to envision solutions for efficient and secure HD exchange between healthcare providers. Recently, the industry and research community turned its focus on the possible use of blockchain technology to solve one or more of the above challenges in data sharing in healthcare domain.

Blockchain is a disruptive technology which creates trust in an unsafe environment without needing central authorities. It has been commonly expected to bring in significant changes

or even reshape the future of many industries [18], [19], [20]. The initial use of blockchain was proposed for financial and banking sectors, and it proved its potential with the successful deployment of Bitcoin [21] (the cryptocurrency that popularized the blockchain technology [22]). The inherent features of blockchain, such as lack of need for a trusted third party, data integrity, transparency, and verifiability make it a suitable candidate for data-sensitive domains such as healthcare [23], [24]. The ongoing research efforts uses blockchain-based solutions to not only address the challenges related to the secure storage of such a huge volume of HD, but it also provide ways to ensure the integrity and confidentiality of the stored data, and at the same time focuses on providing high availability of data among patients, medical personnel, researchers, and collaborators.

Currently, the blockchain-based solutions for healthcare systems are still at early stages of design and development, but numerous efforts and initiatives in this direction are underway. Along with blockchain, the use of Smart Contract (SC) brings several additional benefits for efficient HD management and sharing in a distributed environment [25], [26]. For instance, by adding specific data structures in SCs while receiving data from data subjects leads to the creation of a homogeneous data storage which is maintained at different medical facilities. This data homogeneity will support an efficient exchange of data between different stakeholders involved in the sharing process, thus supporting interoperability. Moreover, the SCs can record the access control and consent rules, which will help regulate and monitor third party data access an data sharing.

A. Motivation and Contributions

Following the advent of numerous proposed solutions in this domain, surveys started to emerge [16], [27], [28], [29], [30], [31], [32]. These past contributions focused on introducing characterizations and taxonomies for specific aspects or challenges of blockchain-based healthcare storage (HSt) systems.

In our survey, we take a holistic outlook. First, we enumerate interactions between different types of healthcare entities (patients, healthcare institutions, registries, and research institutions), support them by real-life scenarios, and explain why it is important to differentiate between interactions when discussing storage challenges and benefits of the blockchain technology. Secondly, we systematically consider the functional components of the HSt systems, namely data storage, sharing, and collection. We differentiate between these components when considering individual systems and challenges they resolve. Thirdly, we analyze the meaning of each non-functional requirement for each functional component of HSt systems and describe resulting challenges. Based on this analysis, we propose a taxonomy of 20 storage-related challenges derived from non-functional requirements of HSt systems, grouped into three categories: security, privacy, and interoperability. Fourth, we list nine potential benefits for HSt systems derived from the fundamental features of the blockchain technology.

When analyzing over 40 systems and solutions proposed in the state-of-the-art, we perform their rigorous placement by identifying the exact scope of each solution and mapping it to the above taxonomies of interactions, functional components, challenges, and benefits. We additionally provide an extensive discussion of compliance with privacy-related regulations of *General Data Protection Regulation (GDPR)* [33] in EU, and *Health Insurance Portability and Accountability Act (HIPAA)* [34].

In summary, our paper has the following contributions:

- This is the first survey to the best of our knowledge that systematically considers interactions between different types of healthcare entities and their effect on the requirements and challenges.
- We present a generic design description of a blockchain-based healthcare (BBHC) architecture and discuss its various components along with their working methodology and interactions from a systematic point of view. By doing so, our goal is to identify the functional components in the healthcare sector and to present the non-functional requirements for each component and the challenges associated with satisfying each requirement. We aim to provide a broader picture of how different components in a BBHC framework fit together and collectively address various challenges that currently exist in the healthcare domain. In particular, this is the first survey to the best of our knowledge that covers the functionality of data collection and differentiates between data sharing and data transfer.
- We provide a comprehensive survey on the state-of-the-art research efforts on BBHC applications. In particular, we categorize all the existing efforts by identifying the functional components in the healthcare sector and non-functional requirements for each functional component, where each surveyed solution addresses one or more of these requirements in specific components.
- We discuss the real world implementation efforts (e.g., testbeds, and pilots) that have been carried out to deploy various blockchain-based solutions for healthcare.
- We discuss compliance with privacy-related regulations at the granularity of individual requirements.
- We present a Summary Care Record (SCR) use case. SCR is an electronic health data management system that provides access to selected patient information adapted to medical emergencies regardless of where patients have received their treatment. SCRs are maintained in many different countries for their respective citizens.
- Finally, we present open issues and challenges in the practical usage of blockchain for healthcare services along with possible solutions to address them. Moreover, we present future research directions that need attention from the research community working in this area.

B. Organization

The rest of the article is organized as follows: in Section II, we provide an overview of actors and their interactions in healthcare systems. We also present basic information about

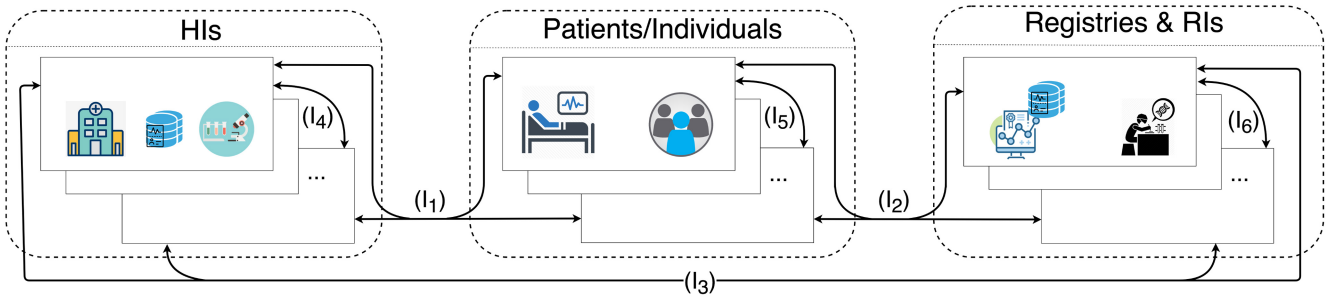

Fig. 1. An overview of the healthcare sector.

the blockchain technology and smart contracts. In Section III, we introduce the functional components and non-functional requirements of HSt systems. Furthermore, we discuss the challenges of HSt systems which derive from fulfilling each non-functional requirement in each of the functional components in these systems. Later, in Section IV, we discuss the fundamental features of blockchain and SCs and how these features can derive benefits for the HSt systems and can facilitate solutions for overcome the aforementioned challenges. In Section V, we survey and discuss the blockchain-based solutions for HSt systems proposed in the academic existing literature and real-world implementations. In Section VI, we discuss related work and compare our study with other surveys in this domain. Finally, in Section VIII, we discuss unresolved challenges in the integration of blockchain and SCs in the healthcare sector and outline gaps and future directions for research.

II. Background

To better understand the challenges in the healthcare domain, we provide preliminaries in this section. First, we present an overview of the entities involved in a healthcare system, and the interactions among them, which serve as the main focus of this study. Afterwards, we present a relevant background about the blockchain technology and smart contracts. In later sections, we explain how these technologies can contribute to addressing a variety of challenges that arise in the context of interactions between the entities in healthcare systems.

A. Overview of the Healthcare System

In this work, we limit the scope of our study of the healthcare sector to the (i) healthcare institutions (HIs), (ii) individuals or patients, and (iii) health registries and research institutions (RIs), and the interactions among these three entities. In our study, we focus on these three entities since they are the only entities in the healthcare systems that have access to primary HD and because the interactions between them are general and applicable to healthcare systems in different countries and contexts. For instance, health insurance providers may have access to parts of HD, yet the mechanism of interaction with insurance providers differ in different healthcare systems [35], [36], [37].

HIs include hospitals, general practitioners, laboratories and other healthcare service and service providers. Individuals are the people who benefit from the provided healthcare services. These individuals will be considered as patients in the scope of the healthcare sector when they receive an ongoing or completed healthcare services by HIs.

In many countries, HIs are obliged by law to report the HD to health registries. We consider the scope of HD as data regarding individuals' physical and mental health conditions (e.g., dietary supplements, exercise and etc.), history of illness, received treatments, clinical trials, tests and results. Health registries store, maintain, and process the collections of HD related to patients with a specific diagnosis, condition, or procedure. Health registries have grown in number and functionality and have been described in detail [38], [39].

The quantity, role, and the scope of the functionality of health registries vary in each country, state or region [40], [41]. However, the goal in common in the registries is to provide quality improvement in healthcare services and provide data for medical research. In order to do so, registries must collect data and curate them into accurate and well-structured data, and provide statistics and feedback to government and HIs. This will enable them to plan and scale healthcare services, and to improve their quality of health care given to patients [42].

As initially proposed by authors in [43], and shown in Figure 1, the interactions in the healthcare systems include both interactions between the mentioned three entities (interaction types I_1, I_2 and I_3 in Figure 1), and also the interactions between different entities of the same category (interaction types I_4, I_5 and I_6 in Figure 1. In Figure 1, several boxes for each category of entities indicate that there are multiple entities of the same category.

Individuals or patients interact with HIs to benefit from provided healthcare services (I_1). This interaction type includes getting a healthcare service in a hospital, getting tests and results in laboratories, and many other services that HIs provide. However, the HIs are generally isolated from one another. They can be located in different areas, cities or countries and patients might lose track of the treatment they received in certain HIs. If patients want to monitor and audit the services and results they have received from different HIs, they will interact with registries.

Registries also can inquire from patients about the quality of the healthcare services and treatment they received or whether

to verify the data they store and maintain (I_2). Registries are supported by law to collect HD from different HIs under a predefined regulation and store and maintain the HD. This requires that HIs transfer the HD to registries (I_3) and they are indeed obliged by law to conduct the transfer of HD to the corresponding registry.

Furthermore, in certain scenarios, different HIs or registries need to interact with each other. As mentioned before, HIs are isolated from each other and they report HD to the corresponding registries. In a case where a patient for instance is required to provide test results or other types of HD to receive a healthcare service, the interoperability of the HIs and the interaction between different HIs would become more important (I_4).

Patients can also share data with other patients or individuals to inquire more information about their health condition or to share their conditions with others (I_5).

Finally, registries do interact with other registries for maintaining their data (I_6) or in order to provide the history of HD for patients that received healthcare service in different domains. For instance, a cancer registry and a cause of death registry need to establish a continuous interaction channel to keep their data updated and aligned with the results of the treatment and the provided healthcare service and their results and statistics. The scope of I_6 interaction also includes collaboration RIs for innovative healthcare services.

Almost all of the contributions in the state-of-the-art so far have focused on Interaction types I_1-I_4, as we will demonstrate later in Section V-A, and to the best of our knowledge there are no contributions addressing I_5 and I_6 in the healthcare sector. In this survey we will not discuss these I_5 and I_6 interaction types any further until in Section VIII when we introduce the research gaps of the existing literature.

Some of the interaction types described above include either a HD *transfer* or *sharing*. To differentiate between these two concepts, we describe HD sharing as when a temporary access to a specific HD is required from one of the entities in a scenario where the HD is stored in the storage layer of another entity. An example of this scenario could be where a doctor needs to have knowledge of the previous diseases or treatments of a patient or a history of the related health condition in patient's family members.

HD transfer happens when the HD needs to be transferred from the storage layer of the entity that stores the data, into the storage layer of the data requestor entity. For instance, when patients travel geographically, and require to receive healthcare service in another region, the health condition and history of the patient should be available in the new region aligned with the structure, format and policies in the new region. We differentiate between sharing and transfer with whether the entity that requires the HD would store the data in their storage layer or not. We will describe more about the requirements of HD sharing and transfer along with HD storage and collection in Section III-A as the functional components of a healthcare system.

As the authors assert in [43], the activities within the mentioned six interactions require constant interchange of consent- and other patient-related sensitive HD, which effectively entails exchanging data across multi-institutional borders. Additionally, one of the key objectives of the HIs would be to protect the personal and sensitive HD related to patients. Adversely, HIs can assist healthcare providers in planning and conducting related experiments and analysis.

Patients can store a journal and history of their HD within either a cloud storage providers or personally in their own devices or a hard copy in the form of *Personal Health Records (PHR)*. Also, within HIs, HD are stored in the form of *Electronic Medical/Health Records (EMR/EHR)*. These HD include personal and sensitive information (e.g., demographic information, and medical histories) about patients.

Thus, it becomes a valuable data source for cybercriminals. For instance, when stolen or accessed illicitly, it can be sold to a third party (e.g., insurance companies). Therefore, healthcare providers need to ensure the security of their underlying infrastructure that powers the whole ecosystem over which the HD is collected, stored, accessed, and shared. Moreover, the system must also be secured from internal attackers (e.g., malicious employee or third party service provider) to support the privacy and integrity of stored data.

To ensure that healthcare providers implement strong security and privacy-preserving measures during the handling of patient's HD, the regulatory bodies in different countries have imposed laws, such as GDPR [33] in EU, and HIPAA [34] and HIPAA's revision called *health information technology for economic and clinical health (HITECH)* [44] Act in USA. Apart from ensuring that all the required measures are taken to secure the patient data whenever it is stored, shared, or transferred, the regulations also demand that the data must be accessible to data owners on request and also to the third party, if it has the owner's consent.

As we discuss further in Section III, recent incidents and HD leakages bring about vulnerabilities in the current architecture of the healthcare systems and require rethinking and consideration of alternative approaches. These vulnerabilities include (but are not limited to) (i) reliance on a trusted third party, (ii) inefficient consent management from the data owner, (iii) lack of transparency and the possibility to verify and audit the procedures that take place within the system and (iv) scattered data among different actors in the healthcare sector.

As we further discuss the features of the blockchain technology in Section IV, blockchain with its unique features and benefits could be utilized to improve and obtain a higher level of interoperability and to ensure the security of sensitive data and patients' privacy.

We discuss the functional components of the healthcare systems in Section III-A and their nun-functional requirements in Section III-B and the existing challenges for fulfilling the non-functional requirements in each component in Section III. We also introduce the benefits of applying blockchain technology and smart contracts in the healthcare sector in Section IV.

B. Blockchain Technology

Blockchain is a distributed ledger, which consists of a series of chronologically ordered blocks that are appended to the ledger and connected with each other in a linked-list data-structure. To provide integrity and immutability of data in the

ledger, the blockchain prevents any updates in the committed blocks. To ensure this, each block contains the hash of the previous block, and the ledger is replicated across peers that participate in the network.

A block usually contains a set of timestamped transactions that are bundled together. To ensure adequate security, blockchain systems adopt various cryptographic primitives such as hashing algorithms, digital signatures, and PKI protocols. In the blockchain systems, there are two key types of participants: those that generate the transactions, and those that validate and store them in the ledger.

A blockchain network runs on a peer-to-peer topology where each node is expected to store the same copy of the ledger. The network consists of a set of nodes or organizations that do not have a preexisting trust relationship among them. Therefore, to ensure that each peer node has the same copy of the ledger at any given time, the new valid block that will be appended in the ledger is selected by executing a consensus mechanism. In particular, a consensus mechanism (e.g., *Proof-of-Work (PoW)*, *Proof-of-Stake (PoS)*, or *Practical Byzantine Fault Tolerance*) is a protocol that ensures synchronization among all network peers (i.e., nodes that maintain the ledger and might also process the transactions) about the transactions that are valid and that are about to be added to the blockchain [45].

Therefore, the mentioned consensus mechanisms are pivotal for the correct functioning of blockchain and need to be tested properly before their use in real-world applications. The key components and functionalities of a blockchain system enable some unique features including immutability, decentralization, consensus, provenance, and finality, which makes it a promising solution in many application domains [46], [47], [48], [214].

Typically, blockchains are categorized based on their permission model. Based on this categorization, blockchain can either be permissionless or permissioned and can also be divided in public, private or consortium ledgers. In relevant literature, public and permissionless blockchains are considered equivalent and used interchangeably. However, these two categories are concerned with different authentication and authorization mechanisms.

A permissionless blockchain (e.g., Bitcoin and Ethereum) allows anyone to become a participant and perform activities such as taking part in a consensus mechanism, sending new transactions throughout the network, and maintaining the ledger state. In a permissioned blockchain (e.g., Hyperledger Fabric), on the other hand, the participation is constrained, and only the pre-verified parties with an established identity are allowed to join the network. Permissioned blockchains require a minimum level of trust among the participants of the consortium and hence, nodes need identities and mutual authentication to participate in the network.

Different blockchain types do not have adherent advantages comparing to other types and each and every type can have their own performance setup and usability in different contexts depending upon need and implementation environment. The choice of a blockchain platform depends on the specifications and performance requirements of the target application, such as required number of transaction per second, transaction commit latency, and service availability [49].

There are other benefits and drawbacks for each of the blockchain types, apart from the trust among the participants, e.g., scalability [50], security and privacy [51], and degree of decentralization. These should be taken into account when making a choice to utilize the efficient blockchain platform. Since the detailed description of blockchain and its associated techniques are beyond the scope of this work, we refer the interested readers to the following survey articles that provide in-depth knowledge about the blockchain functionalities, benefits, challenges, and applications:

- In [49], the authors present a comprehensive survey on blockchain technologies by reviewing the literature published during the last few years. In particular, the key requirements and their evolution while transitioning from permissionless to permissioned blockchains is discussed along with a description of different blockchain platforms that exist today.
- In [52] and [53], the authors provide a systematic survey of different attacks and their countermeasures in the context of permissionless blockchain platforms.
- In [18], the authors present a literature survey of approaches that use blockchain-based solutions to achieve several security services, such as authentication, privacy, access control, data and resource provenance, and integrity, in various distributed applications. The challenges associated with the use of blockchain-based solutions in providing the security services are also discussed along with the possible ways to address them.
- In [45], the authors provide a survey of different consensus protocols that are being used in different blockchain systems. The analyses and comparisons given in the paper provide new insights in the fundamental differences of various consensus protocols concerning their suitable application domains, critical assumptions, expected fault tolerance threshold, scalability, limitations, and trade-offs.
- In [54], the authors present a systematic and comprehensive comparative study of blockchain design across different systems. They introduce a generic layered architecture that applies to all blockchain systems regardless of the type. The study of the systems is organized across these layers so that the design of each layer is considered separately from the rest. The comparison is organized by clearly identified aspects: definitions, roles, entities, and the characteristics and design of each of the layers.

C. Smart Contracts

The term *Smart Contract (SC)* was coined in 1990s by cryptographer Nick Szabo. He defined SC as "a set of promises, specified in digital form, including protocols within which the parties perform on the other promises". However, practical applications of SCs did not emerge until the evolution of distributed ledger technologies (DLTs) such as Bitcoin and Ethereum, in which the immutable and distributed nature of the blockchain and consensus protocols made it feasible to implement SCs. Generally speaking, a SC can be seen as a computer

program that digitally allows the verification and enforcement of contracts between parties in a blockchain system.

Typically, SCs are deployed on and protected by blockchain, and they possess certain unique characteristics and provide a number of advantages. First, since the SCs are deployed and verified on blockchain ledger, the code implementing the SCs is immutable due to the tamper-resistant feature of blockchain. Second, the execution of SCs is done by consensus nodes without mutual trust in a decentralized manner. Third, an SC enables automation of tasks. For instance, it could automatically initiate a transfer of digital assets between involved parties when certain predefined conditions specified in the contract are met or a trigger is sent via a transaction.

Bitcoin was the first cryptocurrency to facilitate the use of SC for sending and receiving bitcoins via a simple scripting language. However, Bitcoin's scripting language has limitations concerning the logical, arithmetic, and cryptographic operations that it supports, which are not suitable for expressing complex business logic.

Ethereum became the first public blockchain platform that supports SCs with advanced and customized logic by using its Turing-complete *Ethereum Virtual Machine*. In Ethereum, the SCs can be seen as accounts which are controlled by program code, unlike the user accounts which are controlled by user's private key. Both contract and user accounts can hold and send/receive Ether. Ethereum supports development of SCs in several high-level languages such as Solidity and Serpent, and regardless of the language, the SC code is complied to create the corresponding ethereum virtual machine bytecode which is then deployed for execution on the underlying blockchain. The blockchain along with the SCs provides a suitable platform for the design of various types of *Decentralized Applications*, e.g., games, gambling, supply chain management, voting, and crowdfunding.

Since the SCs usage are at early stages, and these contacts deal with the asset management and transfer, they are a promising target for cybercriminals. Hence, advanced techniques and tools are required to ensure that the SCs are tested for various security vulnerabilities before their deployment on a blockchain platform. Apart from Ethereum, there are many open-source popular blockchain platforms such as Hyperledger-fabric and Corda, that support the execution of complex SCs and facilitate the creation of decentralized applications.

III. Challenges of Healthcare Data Management

There have been many incidents in recent years that prove healthcare registries and HIs are facing major new challenges related to provision of security and privacy guarantees for HD. Recent examples of data leakages have shown that patients have every right to be concerned about their privacy and be aware of the potential risk that their sensitive HD might be misused. For instance, in Norway, hackers have recently breached the systems of *Health South East*, with nearly three million patients' data potentially compromised as a result [55]. Internationally, examples include the 2015 UCLA Health System massive data breach that affected 4.5 million patients [56].

In the same year, the healthcare company Anthem Inc. Reference [57] reported that as many as 80 million customers of the USA's second largest health insurance company had their data breached, exposing names, dates of birth, and Social Security numbers. In March 2018, 150 million accounts from Under Armour's MyFitnessPal [58] were breached. Often, information is leaked unintentionally, or due to negligence on the part of a data custodian [59].

A spa in Nova Scotia regularly received mental health records for over 10 years [57] from doctors due to the fax number of the spa and mental health referral office differing by a single digit. The messages contained patient names, contact information, and mental health history. Thus, there is definitely a need for more secure channels and mechanisms for collecting, storing, and sharing sensitive information without jeopardizing patients privacy due to random incidents or security vulnerabilities.

Due to its data-driven and data-sensitive nature, HSt systems have unique non-functional requirements, mainly concerning the security and privacy of patients' records, as well as interoperability. However, the requirements may differ depending on the functionality that needs to be provided. In order to systematically present non-functional requirements, we group common functionalities of healthcare data management systems together and refer to such groups as *functional components*. In this work, we identify three functional components of healthcare data management systems, namely data collection, storage, and sharing and transfer. We present non-functional requirements separately for each of the components and discuss the associated challenges.

In this work, we only focus on challenges of HSt systems that can be overcome by utilizing blockchain technology and SCs. There exist studies [60], [61] in the state-of-the-art that investigate for instance, scalability of blockchain-based systems in a variety of different domains, including healthcare. However, we believe such general challenges are inherent to adopting blockchain-based solutions in any domain. Since they are not specific to HSt systems, we do not consider them in our study.

A. Functional Components

1) HD Collection: Within healthcare systems, different entities and actors (hospitals, administrative, physicians and laboratories, to name a few) conduct data collection through a variety of forms: questionnaires, billing records, data collected for treatment by physicians and laboratories, administrative hospital forms, etc. This data being collected includes health conditions and additional personal information about the race, ethnicity, language, family history and more. GDPR and similar regulations stipulate that the collector needs to inform the user about the collected data in a timely fashion, even if the collection process uses indirect data sources.

In recent years, healthcare systems have become increasingly dependent on EHR capabilities and features. The adoption of standards for record formats and the proposed

legislation to protect patient data have received significant attention in healthcare systems [62]. The integration of new components adopted by healthcare systems, such as IoT devices, wearables and mobile health technologies, is poised to create the *Internet of Healthcare Things (IoHT)* [63].

As mentioned in [63], the early integration between healthcare systems, wearables, and IoHT devices involved tracking a set of vital signs such as heart rate captured by smart watches and other wearables. However, with the advent of novel technologies enhancing healthcare services, the scope of patient data expanded rapidly. These devices and wearables can be used to monitor user activities, health status, characteristics and conduct user profiling or transmit sensitive and personal healthcare data for further processing with or without users' knowledge or consent.

HD collection also takes place when patients visit care providers or by clinical treatments, triage, physicians' notes, questionnaires or any other scenario where any personal data regarding patients' health will be collected. Additionally, educational, research and engineering institutions are collecting derived data from registries for research and educational purposes. HD are important resources for clinical care, planning and decision making, quality improvement, drug and pharmaceutical sector, assessment, and scientific research and discoveries.

2) HD Storage: As mentioned in [64], HD can be stored in the following six types:

1) *Demographics* include personally identifiers and information such as name, date of birth, address, and account or medical record numbers, and descriptive information such as race, gender, income level, educational status, nativity, immigration status, and housing status.
2) *Diagnosis* is a description of individuals' health status and the possible presence of diseases, infection or injury. They often include additional information on the severity of individuals' condition or prognosis.
3) *Procedures* describe the medical interventions or services a medical professional provides to a patient.
4) *Screening tests, laboratory information, and radiology* data include the ordered tests and results and the dates of the demanded service and additional files and pictures such as x-ray images, ultrasound results and etc.
5) *Medication prescriptions and adherence data* are prescribed medications information which can include the prescribed drug names, their dosage.
6) *Narrative/qualitative case notes* are other types of data and case notes which include the reasons for a visit provided by the patients and other observational information provided by the doctor.

These six common types of the HD can be stored in a structured or unstructured format. For instance, HD such as practitioners' notes can be stored in free text or as descriptive files or images, which incurs additional challenges in aggregation and cross-system comparisons since they might be stored in different standards and formats. It is critical for different healthcare systems to be aware of the format and standards of the stored HD when collaborating with each other.

When measured by volume, the majority of healthcare data are stored in an unstructured form [64] which adds to the complexity of healthcare systems to ensure interoperability. Additionally, HD are usually scattered among different health providers as patients are transferred between different organizations and hospitals and they relocate to different cities and countries. This mobility and scattered HD can result in isolated data silos, which adds to the complexity of data storage and hinders creation of a unified and holistic view of patients' HD.

Data protection rules and legislation also add extra complexity to personal and healthcare data storage. More than 30% of the 99 GDPR articles are related to storage. Analysis conducted in [65] identifies the following key features that a storage system must support to be GDPR-compliant. Article 46 of GDPR [33] limits the geographical locations and distributions of the data and data centers that will host and store personal data. This limitation implies that storage systems must provide the ability to find, control, and manage the physical location of the data storage facilities at all times.

Additionally, Article 5.1 of GDPR defines limitations about the duration of storage. Under GDPR Article 5.1, no personal data can be accessed for an indefinite period of time. Therefore when storing HD the duration of the access should be explicitly mentioned. Thus, storage systems need mechanisms for auditability and verification of all the operations, whether in the data path (read or write), or control path (changes to metadata or access control). These operations are required to be logged as per GDPR articles 30, 33 and 34 about records of activity processing and about data breach notifications.

Furthermore, storage systems utilized for accessing HD in healthcare systems, must support fine-grained and dynamic mechanisms for access control and for managing patient consent. The consent and access preferences should be acquired under specific circumstances to fulfill the requirements of specific data protection laws and regulations. These laws and regulations include limited access to permitted authorities, under pre-established purpose proposal and for a specific and predefined period of time as defined by GDPR (GDPR Articles 5.1, 15, 20 and 21 about storage limitation, right of access by users, right to data portability and right to object).

GDPR also mandates that personal data be encrypted both when stored and when shared and transferred (GDPR Articles 25 and 32 about protection by design and by default and security of data). While it has been argued that pseudonymization can help to protect the privacy and security of the data and reduce the necessity of data encryption, under GDPR, pseudonymous information would still be personal and would require encryption.

3) HD Sharing & Transfer: Sharing or transferring HD can be done for several reasons, but most importantly, to (i) provide medical and health history and the corresponding HD by patients to receive treatments (interaction type I_1 as mentioned in Figure 1), (ii) develop medical and treatment profiles and journals (interaction type I_3 as mentioned in Figure 1), (iii) facilitate patient' treatment and HIs' interoperability (interaction type I_4 as mentioned in Figure 1) or

(iv) conduct research on derived data (interaction type I_6 as mentioned in Figure 1).

Conducting health and medical research can provide valuable information about disease trends, risk factors and also help with health interventions and innovations, treatments quality, healthcare service and patterns of healthcare, costs and etc. HIs also share collected HD with registries, as required by healthcare laws and policies, and other HIs to facilitate the treatment patients need. Additionally, RIs require derived data from registries which are collected from patients at hospitals in the first place to conduct their intended research. Hospitals and clinics continuously share HD with registries for logging, funding and several other purposes.

In parallel with the rapid accumulation of electronic health-related data, ethical considerations and public concerns related to clinical data sharing for biomedical and behavioral research have been raised. The debate on how ethical it is to use data, that was primarily collected and stored for clinical care, for research purposes spans scientific, legal, ethical, regulatory, and patients' concerns. Many patients may not be aware of how their data are being used for research. Some may receive a consent form, but this requirement can be waived in certain circumstances.

Consent has been typically treated broadly and in a binary form (i.e., patients either consent or not), and tiered approaches to informed consent are seldom utilized. Innovative systems, like a consent management system that empowers patients about the current use of their data could offer an alternative to current practices. However, institutions may be hesitant to adopt such systems, since this might decrease participation in data sharing for research and potentially biased research results [66]. The financial and political costs of implementing such systems, as well as their efficacy in terms of patient and provider satisfaction, are currently sparsely investigated. Technical obstacles also exist, as ways of ensuring compliance to patients' choices may be difficult to implement and maintain.

The existing approaches for HD sharing are managed by a centralized authority controlled by a third party service provider, and is inefficient and insecure. For example, HIPAA report [67] indicates that a data breach of a total of 500 or more records is reported in January 2020, while the report published in 2019 shows a total of 510 data breaches where a large number (nearly 577,511) of health records were exposed, stolen, or disclosed without appropriate permissions.

These issues of inefficiency and insecurity of the current systems include but are not limited to (i) lack of transparency and accountability when data access operations are performed by third parties, (ii) lack of trust between entities sharing the data in inter-system and intra-system domains, (iii) low security of data (e.g., integrity, authenticity, authorization and confidentiality) while being shared, and (iv) the existence of a single point of failure. Some of the issues are due to a central authority being in charge of sharing and managing the data.

Moreover, the centralized mechanism in which the medical records are being stored and shared greatly effect the availability of records. The ability of blockchain to create a decentralized and secure data sharing platform between several untrusted entities provide much needed support for HD sharing across different stakeholders in a healthcare system. In particular, with the help of the decentralized data sharing capabilities along with the unique features of blockchain, some of the current limitations of HD sharing can be addressed in an efficient manner.

B. Non-Functional Requirements

Communication and data management standard for healthcare devices are necessary, and many international standards are considered as prerequisites for the certification of healthcare devices and communications [68]. However, these standards do not focus on the specific and design requirements especially in security and privacy aspects of the healthcare interactions and required communications. Non-functional requirements are defined specifications and requirements that describe the system's operations, interactions, capabilities and constraints that would enhance the functionality.

We focus on security, privacy and interoperability requirements of healthcare data management systems. For each of these three classes of requirements we investigate issues related to data collection, storage and sharing. For each pair of a functional component and a non-functional requirement, we identify related challenges that have been addressed by blockchain-based solutions in the existing literature, and list these challenges in Table I.

In Table I, columns represent functional components of HSt systems: HD collection, storage, sharing, and transfer. These components are described in detail in Section III-A. Each row in Table I represents a non-functional requirement of HSt systems. The non-functional requirements, categorized in three main groups of security, privacy, and interoperability, are described in detail in Section III-B. Each cell presents the challenges of fulfilling the non-functional requirement in a functional component of HSt systems. The challenges are indexed in the table and described in detail in the rest of this section. There are cases where the challenges of fulfilling a non-functional requirement are the same for different functional components. In these cases, we visualize the challenge shared by different functional components by merging multiple columns of that row together. Challenge C_1 in the first row is an example of this scenario.

1) Security: We investigate and present security challenges of different functional components in the healthcare systems. The challenges are classified into (i) authentication, (ii) authorization, (iii) integrity, (iv) non-repudiation, and (v) availability and resilience to *denial of service (DoS)* attacks.

a) Authentication: In certain healthcare scenarios, patients relocate geographically and require healthcare services and medical treatments provided by different healthcare providers, sometimes in different countries. Countries, however, follow different regulations and data protection laws. In this case, the issue of authentication and the identity of the users and actors expand beyond the scope of a single organization and entity. This necessitates a mutual authentication mechanisms for the actors in the healthcare sector, which poses a challenge.

TABLE I
CHALLENGES OF FULFILLING NON-FUNCTIONAL REQUIREMENTS OF HST SYSTEMS IN EACH FUNCTIONAL COMPONENT

<table>
<tr><th colspan="2" rowspan="2">Non-Functional Requirements</th><th colspan="3">Functional Components</th></tr>
<tr><th>Data Collection</th><th>Data Storage</th><th>Data Sharing & Transfer</th></tr>
<tr><td rowspan="6">Security</td><td>Authentication</td><td colspan="3">C_1: Decentralized Identity Management and Mutual Authentication</td></tr>
<tr><td rowspan="2">Authorization</td><td colspan="3">Operation Policies for Different Data Categories</td></tr>
<tr><td>C_2: Create Operation Policy</td><td>C_3: Read & Write Operation Policy</td><td>C_4: Read Operation Policy</td></tr>
<tr><td>Integrity</td><td>C_5: Communication Channel Integrity</td><td>C_6: Stored Data Integrity</td><td>C_7: Access Policy Integrity</td></tr>
<tr><td>Non-Repudiation</td><td colspan="3">C_8: Decentralized Key Management and Signature Verification</td></tr>
<tr><td>Availability (Resilience to DoS Attacks)</td><td colspan="3">C_9: Dependency or distrust in third-parties</td></tr>
<tr><td rowspan="5">Privacy</td><td>Confidentiality</td><td colspan="3">C_{10}: Data should be auditable but also confidential</td></tr>
<tr><td>Anonymity & Unlinkability</td><td colspan="3">C_{11}: Personal Identifiers should remain confidential and unlinkable</td></tr>
<tr><td>Transparency & Auditability</td><td>C_{12}: Data collection Logs, Purpose of Collection</td><td>C_{13}: Storage Purpose, Duration, Data Access Logs</td><td>C_{14}: Sharing Purpose and Access Policies Logs</td></tr>
<tr><td>Accountable Privacy</td><td>C_{15}: Patients awareness, Legitimate purpose & fair collection, Purpose limitation, Specific and informed patient consent, Record-keeping</td><td>C_{16}: Storage security and access mechanisms for periodic reviews</td><td>C_{17}: Informing patient of forwarding, Record-keeping of data disclosures, Transfer restriction, Transfer security, Third party deletion</td></tr>
<tr><td>Consent Management</td><td colspan="3">C_{18}: Consent should be freely given, specific, informed, unambiguous and explicitly obtained</td></tr>
<tr><td colspan="2">Interoperability</td><td colspan="3">C_{19}: Scattered Data, C_{20}: Different formats, standards and policies</td></tr>
</table>

As the authors mention in [69], most identity management schemes today are centralized where a single entity, such as an organization, owns and controls the authentication mechanisms of the system. The centralized identity management and authentication controller will face challenges due to emerging privacy and security issues. Firstly, there is a fundamental assumption of trust in a third-party centralized organization or an entity that manages and controls the authentication mechanism in healthcare scenarios. Additionally, there is an issue of interoperability between different geographical healthcare providers that follow different laws and regulations and employ different identification, identity management, and authentication mechanisms. Distributed ledger technologies and blockchain can help the healthcare system to overcome the aforementioned challenges by facilitating development of a distributed mutual authentication mechanism.

b) Authorization: Authorization is the function of specifying access rights or privileges to resources related to information security. In the last few years XML-based access control languages like XACML [70] and *Platform for Privacy Preferences Project (P3P)* have been increasingly used for specifying complex policies regulating access to resources. As per requirements of GDPR, for conducting operations on personal data, users must be able to define and be in charge of operation policies.

These operations include data creation in HD collection phase and read, write (update) and deletion while storing and sharing personal data including healthcare related data. Current access control mechanisms, such as attribute-based policy [71] and risk-based access control [72] mostly focus on preventing unauthorized access to healthcare devices, data and information [68]. However, it is challenging to ensure the confidentiality and integrity of the healthcare data that will be shared, accessed, updated and modified by different health providers and authorized users. In order to overcome this challenge, an efficient, immutable and verifiable access control mechanism is needed in each and every component of healthcare system to ensure the above requirements and identify or prevent security and privacy violations in accessing the data.

c) Integrity & non-repudiation: Integrity ensures that HD being captured, stored and shared, are consistent in each functional component, and in transition to other components, and not tampered with or modified. This requirement is crucial for every component of the healthcare systems and applies to any kind of intentional or unintentional data tamper. Managing important and sensitive HD requires assurance of reliability

for the provided services. If the sensitive HD of the patients are not immutable and not protected against tampering in the transition from data collection to storage and access during the medical treatment, it may result in improper treatment based on erroneous data and may lead to crucial consequences for patients' health.

The HIPAA Security Rule [73] clearly asserts that the healthcare entities must "implement policies and procedures to protect electronic personal healthcare information from improper alteration or destruction". In addition, as mentioned in [74], repudiation threats can be of high concern as the users can dispute their signature authenticity after accessing HD and deny that the transaction has been triggered by them.

To overcome the mentioned integrity and repudiation challenges, modern solutions are utilizing digital signatures and *public key infrastructure (PKI)* schemes. However, the conventional approach to PKI presents several challenges. Generally, there exist two approaches to PKI: *Certificate Authority (CA)*-based PKI and *Web of trust (WoT)*. While CA-based PKI (e.g., X.509 standard) is the most common approach, it relies on the existence of a third party trusted by all the entities in the network to act as the CA, i.e., to issue a signed certificate to each and every other entity and to certify the ownership of a public key.

As mentioned in Section III-B1a, entities in the healthcare systems can have a broader scope of identities and be geographically scattered, which means they might trust different CAs and follow diverging standards. On the other hand, WoT systems are based on networks of trust [75]. In WoT, members of the network employ transitivity of trust: a node A establishes trust in another node B by verifying that B is already trusted by node C such that A already trusts C. The signed certificate also needs to be issued by some entity in whom the verifier has previously established trust.

However, these two approaches are argued to have shortcomings, especially in the healthcare sector. The first approach relies on the centralized entities of CAs, which can be considered a single point of failure. Due to the lack of sufficient transparency in issuing certificates and verifying the ownership of public keys, the security and privacy of the system and the PKI mechanism can be criticized as insufficient [75]. Unlike the CA-based PKI, the trust is decentralized in the WoT approach. In WoT-based PKI networks, members will be considered as *trusted* if their trustworthiness is already approved by other trusted nodes. This trust establishment mechanism faces a barrier for nodes to participate in this scheme, since it takes time and a lot of interaction to accumulate enough votes in this scheme.

d) Availability and resilience to DoS attacks: It is crucial that HD be available and accessible to the users of the healthcare systems anytime and anywhere. For instance, in case of an emergency where patients are receiving first aid treatment, it is very important that HD would be available to verify the history of the patient, allergies, reactions to specific drugs, etc. The availability in this context refers to both system and transaction levels [51].

As mentioned in [51], "At the system level, the system should run reliably even in the event of a network attack. And at the transaction level, the data of transactions can be accessed by authorized users without being inconsistent or corrupted". Examples of transactions in the scope of healthcare systems could be interaction with a care provider, accessing HD of patients, granting or revoking consent, and every interaction that patients could make with other care provider parties to produce a HD.

The rapid growth in the number of insecure devices, including remote health monitoring and IoHT, and the increase of traffic volume for collecting, sharing and transferring data produced by these devices makes *distributed denial of service (DDoS)* attacks a crucial security vulnerability [76] in the healthcare sector. This is especially true because sensitive HD can be valuable and attractive source for attackers. DDoS attacks are typically performed with the goal of disrupting available services on the network by creating enormous number of transactions to suspend network resources.

The motivation behind these attacks can vary from marketing and business benefits to personal and political reasons. Most organizations lack sufficient resources and flexibility to cope with the mentioned attacks by utilizing their own resources [76]. The first solution to address this security vulnerability is to adopt DDoS protections services offered by companies such as *Akamai* [77] or *CloudFlare* [78] and there has been an increase in exploiting the offered resources of these cloud-based companies in recent years [79].

However, the mentioned solutions requires a third party *DDoS protection service* provider, which result in additional costs and a decrease in service performance [76]. Since the detailed description of DDoS attacks and the currently existing defense mechanisms are beyond the scope of our work, we refer the interested reader to the existing survey article [80] that provides in-depth coverage of DDoS attacks, the challenges they pose and the existing defense mechanisms.

The impact of DDoS attacks can be very significant in healthcare systems, where the availability of data could be a matter of life or death, e.g., in a medical emergency situation [81]. Security vulnerabilities pose a threat for the availability of the HD and hence, availability of healthcare services. The vulnerabilities of the centralized controller make it a single point of failure and a performance bottleneck.

Various mitigation techniques have been proposed to prevent this vulnerability in the healthcare sector. However, only a fraction of these techniques can been considered viable for scalable and globally accepted deployment because of their effectiveness and implementation costs and practical feasibility. Most of these contributions rely on the existence of a trusted third party, e.g., a cloud managed by a single organization, which creates a risk for violating security and privacy requirements.

2) Privacy: In this section, we discuss privacy aspects that are considered by the existing literature in the healthcare sector. These include (i) HD confidentiality, (ii) anonymity and unlinkability, (iii) HD transparency and auditability, (iv) accountable privacy, and (v) consent management for data access.

a) HD confidentiality: In the context of the healthcare sector, confidentiality should be ensured not only for the content of medical records to keep them private from any external entities, but also from unauthorized internal personnel and entities within the healthcare system and even within the same organization. As mentioned above, HD include health conditions and additional personal information about race, ethnicity, language, family history, medical conditions, etc. This means that the data can be of high business value for different organizations that seek to perform data analytic as part of their business.

The high value and the sensitive nature of HD make it more important and challenging to keep the data confidential. Even the knowledge of the existence of a medical record, or a medical treatment or specific HD could constitute a privacy risk in hands of unauthorized users. This is especially the case if such knowledge can be combined with adversarial background knowledge to enable certain inferences [82] about user identities or linkable interactions. Furthermore, user access preferences should be kept confidential from external parties, since the integrity and confidentiality of these preferences are essential for patients.

b) Anonymity & unlinkability: As it is necessary to collect and store direct identifiers of the patients such as their name or social security numbers and other descriptive data that can be used to discover the identify of the patients (such as current living city and country, home address, height, and weight), it is imperative that these data be treated with the highest level of confidentiality possible.

On the other hand, this data is required to keep an integrated history of patients' medical treatments and healthcare journal. Therefore, storing and collecting it is inevitable and of high importance. Several initiative have proposed using pseudo-anonymous information for patients. However, under GDPR anonymized data is also considered as personal information and should be treated accordingly [83].

Furthermore, in case of an event where patient identifiers and HD are leaked to unauthorized internal or external parties, an important requirement of unlinkability arises. The requirement means that the unauthorized parties should not be able to link the leaked information about a patient to any other data of the same patient stored by HIs, and should not be able to access that other data. This requirement has a high inter-dependency with the confidentiality requirements.

c) Transparency & auditability: Patients need a transparent view of how their HD is being managed by different entities in healthcare sector. Such transparent view will enable patients with auditability of their HD history. Additionally, patients have the right to benefit from a transparent view of healthcare provider policies, adherence of HIs to those policies, and any other meta-data associated with their HD. The concept of transparency is indirectly included in Article 8 of GDPR, which states that "Everyone has the right of access to data which has been collected concerning him or her" [33].

Within the healthcare sector and the interaction between the actors in the healthcare systems, this means that all individuals and patients have the right to be explicitly informed about any of the activities of collection, storage and sharing of their HD and the purpose of conducting each activity and the duration, result and outputs and the entities in charge of conducting these activities.

Transparency in each of the functional components of the healthcare systems will increase the trust of individuals in the processing activities conducted within healthcare system. The established trust will incentivize patients to become more involved and to willingly participate in research activities that require access to his or her data, and they are able to verify that the security and privacy guarantees by the healthcare system are met. Additionally, transparent view of the medical and HD provided to the patients can result in more accurate and reliable content as the users would be able to audit and verify the data.

In addition to the transparency and auditability requirements of patients, HIs must fulfill security and privacy requirements of their policies and the HD they keep from patients. From the HIs' point of view, HD, and any associated meta-data, should be transparent to only the patient as the data owner and other specific authorized entities (such as registries). Fulfilling patients' auditability and transparency, along with HIs' security and privacy requirements can provide a challenging trade-off in the healthcare sector. As a result, today, individuals' trust is negatively affected by the lack of transparency in how the private data is being maintained and processed [84]. Individuals are not always aware of how their data is being accessed and processed and there exists no verifiable mechanism for auditability of access to their HD and for the activities conducted on top of it [85].

d) Accountable privacy: As proposed in [86], a three-tier terminology simplifies discussion of accountability by distinguishing between the accountability of policy, procedures and practice. By this classification, the organizations should be able to demonstrate that (i) they have defined a clear and properly documented privacy policy, (ii) their established procedures are sufficient to implement the privacy policies, and (iii) they are able to provide the proof that the privacy policies have effectively been met.

The authors of [87] discuss key requirements for providing accountability evidences across different stages of the personal data life cycle. They also propose mechanisms for implementing those requirements. The purpose of the accountability mechanisms in the healthcare systems should be to provide sufficient means to patients so that they would be able to verify the compliance of healthcare providers and their actors with the personalized privacy requirements and access privileges.

However, accountability in the currently existing HD management systems is highly dependent on the trust in authorities that provide the mentioned evidences: the users need to trust the entities to provide correct, transparent and tamper-proof reports of accesses to their data. Additionally, the authors of [88] discuss GDPR regulations pertaining to accountability of the personal data, namely, (i) providing data authenticity, (ii) fulfilling security requirements of processing, (iii) allowing the demonstration of compliance with the data processing principles, (iv) supporting the demonstration of compliance with codes of conduct and certified procedures, (v) recording data describing the legal context, (vi) keeping an up-to-date

and accurate record of all the processing activities and finally, (vii) availability of records of processing.

e) Consent management: Since there exist a large volume of HD, it could support the experiments fueled by the application of statistical in-depth data analysis, risk analysis techniques, and predictive methods for developing novel treatments and solutions aimed at better management of health services for patients. However, the regulatory requirements demand that the patients have control over their data, and the data should only be provided to third parties upon the patient's consent, unless the regulatory requirements explicitly states otherwise.

Individuals whose data are being collected, stored, shared and processed should be in charge of deciding who can perform these activities on their personal data. They should also be able to audit who has conducted the mentioned operations on their personal data, based on which purpose, for which duration and verify whether their access preferences were satisfied.

GDPR specifies the following requirements for acquiring consent from data subjects as mentioned in [88]: (i) Consent should be explicitly given; (ii) The system must provide records of granted and revoked consent by the data subjects for accessing their personal data, which should include the purpose and the duration of access; (iii) The system must allow users to modify and change their consents whenever they demand; (iv) The system must ensure that the consent provision by a data subject was actively and willingly given. This means that the consent transaction should not be obtained through inactivity or pre-checked boxes, and that it is confirmed in words. Finally, (v) the withdrawal of consent shall not affect the lawfulness of processing based on the granted consent before its withdrawal.

Ideally, these rights could be addressed by means of a *consent management system (CMS)*. A CMS acts as a platform between data subjects, data controllers and should provide addressing access control and transparency requirements. However, when the CMS is owned and controlled by a single entity, data subjects and other parties involved are forced to trust this entity, even if they would not wish to do so. Additionally, the fine-grained level of access management, verifiability and transparency for consent management is not straightforward to implement. As mentioned in [89], it is reasonable to assume that data subjects among data controllers and data processors would be more willing to trust a consortium of non-colluding entities over a single entity.

An ideal consent management system needs to be secure and to guarantee integrity of the stored consent records, and it should have high availability so that the data holders and data requesters can access and verify authorization documents of patient consent for data sharing. Moreover, there should exist a mechanism that would allow requesters to get patient consent, in a very specific and fine-grained manner, for accessing their medical records. The CMS should also allow users to modify their consent preferences dynamically.

In particular, the consent document should include specific permissions concerning what type of medical records can be accessed, for what duration, and purpose and context of the data usage. Additionally, the data owner should be able to approve further use or revoke any permissions at any time, and have a complete control over the data utilization by the data holders and requesters. Such control implies limiting the timeline of data access, the entities by whom data has been accessed, and the purpose.

At present, however, the process of consent acquisition and management in some healthcare systems and research centers still relies on paper-based techniques [90], [91]. The transformation process of migrating the consent management from paper-based to electronic-based is an ongoing effort, and it is characterized by many open challenges [92]. Some of these significant challenges include minimal control over the granularity of consent permissions, the difficulty in handling dynamic consent management (e.g., changes in consent over time and due to change in the context) [93], and ethical concerns that arise due to binding of consented data with intelligent systems [94] and lack of transparency and user-centric control.

3) Interoperability: Interoperability between the healthcare systems is essential to facilitate a meaningful exchange of HD, to provide personalized care and to support mobility. The data should be exchanged in a way that makes it suitable to use for further purposes. The critical limitations that hamper interoperability between HIs are the use of data storage silos and the lack of standardization in the formats (e.g., encryption schemes, data structures, and query language) of data storage. Separate non-integrated storage silos of patient's medical records at different institutes not only make interoperability difficult, but also result in fragmentation and possible duplication of healthcare data, limited or slow access to HD, and low data quality.

Moreover, a centralized storage creates a single point of failure, which could result in a loss of data due to a technical fault or a security attack. Large volumes of HD are created and stored in different medical systems every day. Since these systems diverge in terms of clinical terminologies, software apps, technical and functional components, and technology platforms, this leaves the stored data with no globally defined standard for accessing and sharing across the systems.

GDPR also adds to the complexity of interoperability by defining the following requirements about data portability and interoperability as investigated by authors in [88]: (i) The system must allow portability of personal data in a structured, common, automatic format; (ii) It should be possible to transfer personal data to another data controller or other countries and geographic locations. In addition, (iii) recording of the proper measures must be enabled by a third country or an international entity that would allow the transfer of the mentioned personal data. Furthermore, it is stated in [88] that (iv) "the system must enable interoperability for the transfer and portability of personal data and must allow the communication between institutions involved in the processing of the same personal data".

Specifically, healthcare industry is currently struggling with problems such as fragmented data silos, communication latency, communication security, and heterogeneous medical workflows caused by vendor-specific and incompatible

TABLE II
DATA PROTECTION LAWS AND REGULATIONS IN DIFFERENT REGIONS

Region	Data Protection Law
United States	HIPAA (Health Insurance Portability and Accountability Act) The Health Information Technology for Economic and Clinical Health (HITECH) National Institute of Standards and Technology (NIST)
EU	Data Protection Law from Government General Data Protection Regulation (GDPR)
United Kingdom	Data Protection Act (DPA)
Russia	Personal Data Act by Russian Federal Law
Brazil	Law of the Constitution
India	IT Act
South Korea	Personal Information Protection Act
New Zealand	Health Information Privacy Code
Common Wealth	National Electronic Health Transition Authority (NEHTA)

medical institutes. Thus, it makes difficult to support efficient personalized care. The lack of a trusted link between these independent healthcare systems along with an end-to-end connecting network can be seen as one of the fundamental problem that causes the above mentioned issues in this domain. On the other hand, every country has their own policies and regulations for information privacy which makes the sharing and transferring of the sensitive and personal medical and HD more challenging. Information protection regulations of several countries are investigated by [89] and represented in Table II.

C. Summary and Lessons Learned

In Section III-C, we present a detailed discussion on the challenges that the existing healthcare systems face along with their impact on the HD management. First we identify the functional requirements (i.e., HD data collection, storage and sharing or transfer) of HD management. Then we describe how these functional requirements are achieved in the current healthcare systems and what specific challenges arise in their implementation. In particular, we identify non-functional requirements associated with each functional requirement (please refer to Table I). In this survey, we mainly focus on the non-functional requirements of HD management that are related to security, privacy and interoperability. We specifically points out to the key facts that make fulfilling these requirements in healthcare more difficult compared to other domains.

Finally, we discuss how the blockchain technology along with SCs can be effectively utilized to address some of these challenges.

Next, we present a number of key lessons learned from the review of challenges:

- The healthcare sector consists of numerous entities that are in continuous interaction with one another. To identify different challenges of HSt systems, the scope of the entities and their interactions is of high importance. For instance, every interaction in HSt systems needs multiple functionalities and non-functional requirements. Furthermore, we discuss the challenges of HSt systems derived from fulfilling each non-functional requirement in each of the functional components in HSt systems.
- HD sharing and transfer are sometimes used interchangeably in the existing literature. However, data protection rules and regulations (such as GDPR) propose distinction between the two functionalities based on the duration of the data being shared, the purpose of sharing and etc. The key issues that hinder HD sharing between two institutions or HD transfer from one institution to another are the lack of trust between these institutions, and the lack of transparency concerning the use of data once it is shared or transferred.
- HD semantic brings additional complexity to the challenges of HSt systems that is not sufficiently studied in the existing literature. For instance, X-ray images or RNA sequence data can be massive in size and can reveal metadata about personal identifiers. These characteristics of the HD exacerbate the challenges related to storage and privacy.
- There exist several challenges of HSt system that cannot be resolved by applying blockchain technology and SCs by itself. For instance, despite many contributions that focus on the anonymity of users in blockchain-based systems [95], [96], and more specifically, anonymity of patients in BBHC systems [97], [98], applying blockchain or SCs cannot provide anonymity by itself; providing the anonymity in BBHC systems requires additional mechanisms and considerations.

IV. BENEFITS OF BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS FOR THE HEALTHCARE SECTOR

In recent years, many research institutions and industries have made efforts to envision the use of blockchain and SCs in the healthcare domain. In this paper, we survey these efforts, identify the key benefits of the technologies, and discuss how these benefits improve various aspects and address challenges listed in Table I. We present our classification of the benefits in Figure 2. It is important to note that we limit our survey to the state-of-the-art contributions proposed for the healthcare domain without including contributions in other domains that might be applicable to healthcare.

As demonstrated in Figure 2, we classify the benefits of blockchain and SCs into two groups. First, in Section IV-A, we introduce the fundamental features of blockchain and SCs (indexed as *F#* in Figure 2). Furthermore, in Section IV-B, we

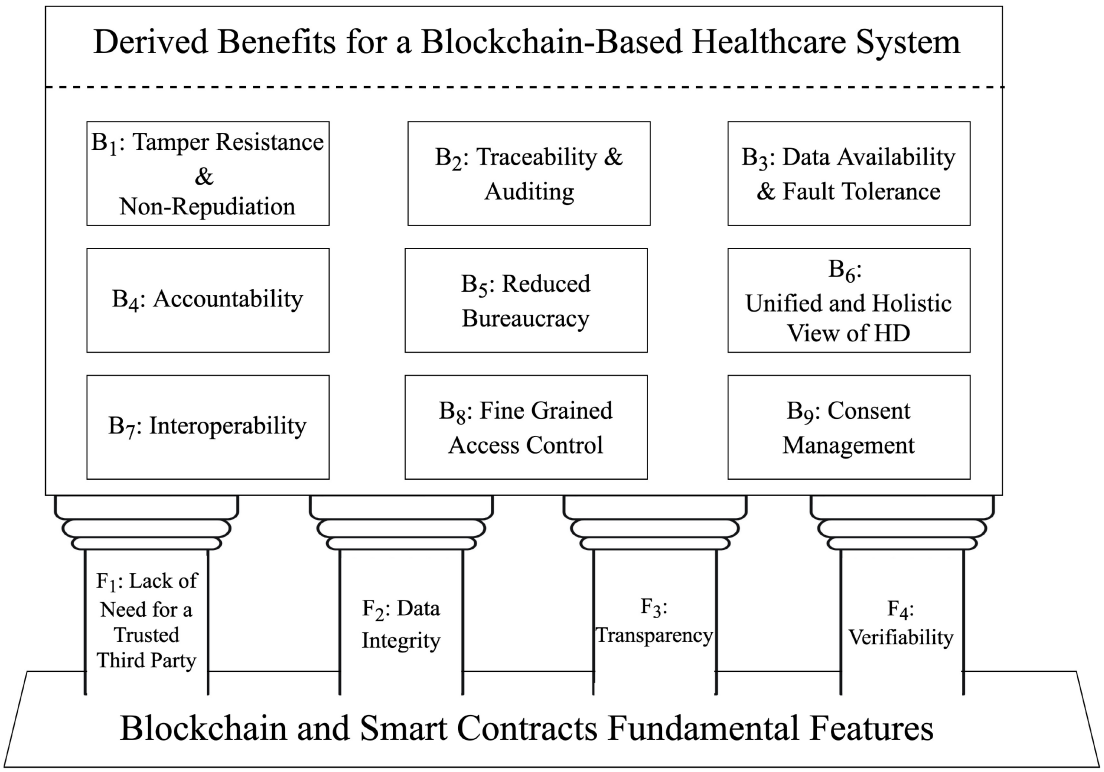

Fig. 2. Benefits for healthcare domain envisioned by the usage of blockchain technologies and smart contracts.

introduce and describe the derived benefits of blockchain and SCs for the healthcare sector and as proposed in the existing literature (indexed as *B#* in Figure 2). These derived benefits are tailored for the healthcare sector to address the challenges in healthcare as listed in Table I.

A. Fundamental Features of Blockchain Technology and Smart Contracts

Fundamental features of blockchain and SCs are inherent features of these technologies, regardless of the context and domain they are used in. However, according to the use case of the system and the context, these features could be adjusted to address the system and context specific requirements. We discuss on lack of need for a trusted third party, data integrity, transparency, and verifiability as fundamental features of blockchain and SCs as 4 pillars of the benefits of these technologies. We will discuss on verifiability and transparency together as these two features are closely tied and the degree of transparency can directly affect the verifiability feature of the blockchain system.

1) Lack of Need for a Trusted Third Party: In order to have secure communication and transactions, distributed systems frequently rely on the existence of a central trusted authority. In blockchain systems, there is no hierarchy of authority, and all decisions are made by consensus between the participants, without a central controller.

2) Data Integrity: As mentioned in Section III-B, integrity of data ensures that the data is immutable to any unauthorized modification and tamper attempts. In case of a centralized controller, users have no alternative but to trust the controller to ensure data integrity. In blockchain, however, each block submitted to the ledger will also include a hash of the previous block and this mechanism will result in a chain of hash pointers to the previous blocks up to the very first block in the ledger. This chain of hash pointers will require the recalculation of all the hash chain of the later blocks in case of a modification of the block content and the acceptance of the participants, which is very difficult to carry out in practice. This fundamental feature of the blockchain ledgers ensures the integrity of the data stored on-chain. Several contributions in the state-of-the-art have proposed storing HD directly on-chain. Although this mechanism can ensure integrity of the HD, but it also faces challenges in scalability with respect to the size of the data stored on-chain.

Several initiatives (e.g., *BigchainDB* [99]) have proposed a novel blockchain ledger that is more efficient in terms of on-chain data storage, however, they have not been addressed by the contributions in the existing literature. Other contributions proposed storing the HD off-chain and ensuring the integrity of the HD by storing a metadata (e.g., hash of the HD) on the ledger which will reduce the required storage size. Furthermore, the fundamental integrity feature of the blockchain platforms can ensure that both HD and their corresponding metadata, such as patients' preferences regarding the access policies and consent configuration for accessing the data, will remain tamper-proof.

3) Transparency & Verifiability: Within a centralized system, different participants have to trust the central entity

to verify the state of the system and transaction within the scope of the system on their behalf. On the other hand, in blockchain-based systems, the ability to observe and verify the state, transactions and the ledger could be provided to many participants. This verifiability feature relies on the degree of the blockchain ledger transparency to the participants. In order to be able to verify the transactions and the state of the system, a participant would need a transparent access to the information stored within the system.

However, as mentioned in Section II-B, there exists an inherent tradeoff in different types of blockchain-based systems with respect to ensuring transparency and privacy. In public blockchains such as Bitcoin or Ethereum, anyone can verify the state of the system which is referred to as *public verifiability*. Public verifiability, however, can also bring about issues for patients' privacy in the healthcare sector. Information about the patients' status, and the history of treatments is private; patients have the right to restrict access to their HD to specific entities. The main issue is to provide transparency and verifiability by permitting access to selected entities while keeping the data confidential from the others.

To provide transparency to certain entities to facilitate verifiability and to keep HD confidential from unauthorized entities, a number of blockchain-based solutions have been proposed. For instance, a consortium blockchain can provide limited transparency and view of the ledger, and provide verifiability by specific users whose identity is known to the system. This can ensure that the data stored on-chain will only be accessible to limited set of participants in the ledger which patients might trust. With permissionless blockchains, there are initiatives that propose fulfilling the above confidentiality requirements, by means of utilizing cryptographic techniques to encrypt data on ledger.

These techniques, however, are known to come at the cost of lower computation efficiency since they makes use of computationally expensive cryptography mechanisms to fulfill privacy requirements while providing sufficient required transparency to the ledger state [100]. The choice of exploiting different techniques and blockchain types to provide the right balance between transparency and confidentiality of data should be adjusted based on the requirements of the system and the context in which blockchain is being used.

B. Derived Benefits for a Blockchain-Based Healthcare System

Applying blockchain and SCs in the healthcare sector can provide benefits to healthcare beyond the fundamental and inherent features of these technologies as we described in Section IV-A2. As demonstrated in Figure 2, we identify 9 derived benefits of exploiting blockchain and SCs in the healthcare sector. Namely, (i) HD tamper resistance & non-repudiation, (ii) traceability and auditing, (iii) HD availability & fault tolerance, (iv) accountability, (v) reduced bureaucracy and expenses in healthcare systems, (vi) unified and holistic view of HD, (vii) Interoperability, (viii) fine-grained privacy control, and finally (ix) consent management. We will introduce and discuss each one of the mentioned derived benefits. We group the last two derived benefits (fine-grained privacy control and consent management) and discuss them together as the role of the blockchain and SCs to provide these two benefits are similar.

1) HD Tamper-Resistance & Non-Repudiation: In blockchain-based systems the integrity of the data can be well assured by either storing the data on-chain or off-chain and storing a metadata (e.g., checksum) on the ledger. The stored data on-chain (access, consent policies, HD metadata and etc.) would be protected against any tampers by the hash chain mechanism in blockchain ledger. This feature is relied in the immutability fundamental feature of blockchain and SCs as described in Section IV-A2. Additionally, as we mentioned in Section III-B1c, the existing PKI schemes, namely CA-based and WoT, face challenges for overcoming repudiation challenges. Blockchain can ensure non-repudiation for healthcare systems since it can provide the mutual authentication between participants in the network and overcoming the challenges of the two mentioned PKI schemes. As a result, different participants in the healthcare system cannot deny granting or withdrawing consent, requesting to collect, store, share or transfer HD or triggering any transaction in the scope of the healthcare system.

2) HD Traceability & Auditing: Traceability is defined as the ability to identify and verify the components and chronology of events in all steps of a process [101]. In healthcare systems, patients need to be able to trace and audit whether their HD is managed as per access preferences and policies they have specified. They need also to be endowed with the ability to audit their treatment state, trace their HD and the history of their medical, treatment and health journal, and the compliance of the access log histories. HIs also need to audit the compliance of the data processing agreement between data subjects, data controllers and data processor. In a BBHC system, traceability will be provided in an untrusted environment based on the fundamental features of blockchain such as verifiability, transparency and immutability. Since the history of all transactions are stored in the blockchain ledger and those transactions are linked together, it is feasible to provide the feature of traceability and auditing for a BBHC system.

3) HD Availability & Fault Tolerance: To overcome the availability vulnerabilities mentioned in Section III-B1d, many contributions have been made, mainly in four broad categories of (1) attack prevention, (2) attack detection, (3) attack source identification, and (4) attack reaction to propose a defense mechanism against DDoS attacks [80]. Most of these initiatives, propose the development of specific gossip-based protocols [76] as part of the design of their solution. As a result, the deployment and integration of such proposed contributions and solutions become more complex to support the proposed protocols. Instead, fundamental features of blockchain and SCs, namely lack of need for a trusted third party, can be utilized to avoid the complexities of adopting new proposed protocols.

Different blockchains use different consensus protocols and can guarantee tolerance to a proportion of faulty nodes. For instance, PoW, are known to be tolerant of up to 25% of the computation power while practical byzantine fault tolerance

consensus algorithms can also ensure resilience 33% of the adversary voting power defined within the network [102]. Different systems that rely on different blockchain types can guarantee resilience to a proportion of adversary nodes based on the design of the consensus protocol. These features can provide availability and fault tolerance for the system and avoid the deployment and adoption complexities.

4) Accountability: Accountability aims to empower individuals by providing the possibility to check the compliance of organizations with their policy, procedures and practice privacy requirements. However, accountability in currently existing HD management systems relies on trust in authorities that provide related evidences. Besides, users need to trust the authorities to provide correct, transparent and tamper-proof report of how their HD is being managed.

HIs have to (i) define a clear and properly documented privacy policy, (ii) demonstrate that their procedures are sufficient to implement the intended privacy policies, and (iii) provide proofs that the privacy policies have effectively been met. Providing these reports are not necessarily reliant on blockchain technology. However, blockchain-based systems can facilitate ensuring accountability requirements, as discussed in Section III-B2d, based on fundamental features of blockchain and SCs, in a tamper-proof, transparent, verifiable, and auditable mechanism while avoiding additional costs to provide these features and also avoiding cross-system adoption complexities.

5) Reduced Bureaucracy and Expenses: Physicians and healthcare researchers are educated in the science of medicine and treatment of patients and have traditionally been less oriented toward the administrative aspects of healthcare [103]. Additionally, the increasing regulations in the scope of data protection for healthcare and medicine have resulted in the expansion of mandatory requirements and legislations, which has inevitably led to the growth of administrative bureaucracy in healthcare [103]. Since SCs can encapsulate legal prose without the need for a trusted third entity to act as an intermediary, utilizing SCs can save on paperwork, intermediary fees and other types of bureaucracy in the healthcare sector.

Moreover, in current healthcare services, and in scenarios where patients seek treatment by healthcare providers, patients would need to carry a journal of their medical history and the related laboratory tests and results. If patients need to be involved in the task of managing their HD, this overhead may disincentives them from taking actions that would improve their own treatment and well-being. By utilizing a blockchain-based access control mechanism and a secure data storage layer, healthcare providers could get access to the required HD they seek anytime and anywhere, if they are authorized to do so by patients. By doing so, storage costs in healthcare can be significantly reduced and the time and cost efficiency of accessing the required HD and providing the necessary treatments and healthcare services could be boosted [104].

6) Unified and Holistic View of HD: As mentioned in Section III, the issue of scattered data and isolated data silos in healthcare sector hinders access to patient's medical history and creation of a unified and holistic view of patients' HD. SCs can retrieve data from multiple sources. Since the contracts are not reliant on any specific database, they can facilitate overcoming heterogeneity between isolated healthcare data silos. SCs can overcome the siloed data challenges by providing an integrated view of the data and hence, integrated access to patients' HD if required. The proposed integrated view of HD will also benefit from fundamental features of blockchain and SCs as described in Section IV-A. To this end, researchers have already begun studies that explore the ability to integrate *Fast Healthcare Interoperability Resources (FHIR)* with blockchain technologies [105], [106].

7) Interoperability: As we discussed in Section III-B3, the critical limitations that hamper interoperability between HIs are the use of data storage silos and the lack of standardization in the formats of data storage. Additionally, different data protections laws and regulations, as demonstrated in Table II can add more challenges to the interoperability limitations. We discussed how blockchain and SCs can provide a unified and holistic view of HD which can overcome the challenges of siloed HD in Section IV-B6.

In addition, SCs can check the input HD against a predefined data standard upon receiving a request to store or update HD from an external entity. This can be used to enforce compliance with or convert the data to a predefined data entry format. The use of such SCs will ensure that the data models have a homogeneous data storage and access structure across all the healthcare systems. This homogeneity will facilitate interoperability of access to different data storage systems, and it will lay the ground for efficient data sharing across multiple healthcare systems. Verifying the compliance to data protection laws and regulations could also be facilitated based on integrity, transparency and verifiability fundamental features of blockchain and SCs and also accountability guarantees of a BBHC system as described in Section IV-B4.

8) Fine-Grained Privacy Control & Consent Management: Consent management systems and mechanisms, along with defining access policies and privacy controls have been in use for some years in different sectors including the healthcare. However, when a single entity or an organization controls the consent management and access and privacy policies, data owners have no other alternative but to trust the centralized entity. SCs can record fine-grained policies defined by patients or data owners concerning the usage of their HD. These policies can help to enforce the multi-level access control management and the dynamic consent management, which are needed during the data collection, storing, processing, sharing and accessing process in different healthcare applications. Moreover, the SCs can regulate and monitor data access by third parties, and automatically report on such an access to the clients, and provide auditability an verifiability features, according to the GDPR regulations.

C. Lessons Learned

In this section, first we review the fundamental features of using blockchain technologies and SCs. These features are generic and applicable to different application domains. Then, we identify and present a set of benefits that are derived from the fundamental features and that are advocated by

the state-of-the-art contributions in the healthcare domain. We discuss how these derived benefits could help addressing the challenges described in Section III (please refer to Table I).

Key lessons learned from the review are summarized below:

- Blockchain technology and SCs have fundamental features, namely, i) lack of need for a trusted third party, ii) data integrity, iii) transparency, and iv) verifiability that are inherent features of these technologies regardless of the context and domain they are used in.
- Applying blockchain technology and SCs in healthcare domain can provide benefits to this sector beyond the fundamental and inherent features of these technologies as demonstrated in Figure 2.
- The use of blockchain technology provides many benefits for the HD management, and addresses several non-functional requirements. At the same time, it adds new technical as well as regulatory challenges related to scalability and interoperability, compliance with GDPR polices, privacy preservation, and system usability. Therefore, additional techniques should be incorporated to address these new challenges, while taking the design complexity into account.

V. Blockchain-Based Solutions for Healthcare

In this section, first, we survey the currently existing solutions that use blockchain technology to address challenges of traditional healthcare systems listed in Section III. In addition, we discuss specific efforts taken in academia or industry in which the BBHC solutions are implemented, deployed, and analyzed in real-world scenarios (e.g., pilots, testbed, and business applications). Our goal is to provide insights into how blockchain technology is actually being used and in what specific applications of healthcare.

A. Academic State of the Art Proposals

This section presents the findings and analysis of 45 research articles that investigate the use of blockchain and SCs in the healthcare domain. We summarize these findings in Table III.

In our study, we only focus on the contributions in the state-of-the-art that propose blockchain-based solutions with clearly identifiable benefits due to the use of blockchain and SCs. Solutions for healthcare that are based on other technologies have been surveyed in [11], [107], [108], [109]. Secondly, the healthcare ecosystem is highly diverse. Our scope, as presented in Section II-A is limited to the three main entities of HSt systems, namely, i) patients/individuals, ii) HIs, and iii) registries and RIs, and to the interactions between them. This is because they are the only entities in the healthcare systems that have access to primary HD and because the interactions between them are general and applicable to healthcare systems in different countries and contexts. For instance, health insurance providers may have access to parts of HD, yet the mechanism for interaction with insurance providers differs in different healthcare systems [35], [36], [37]. Similarly, we do not consider supply management for drugs and medical equipment.

To survey the existing solutions, we investigate the interaction type addressed in the currently existing systems as described in Section II-A and demonstrated in Figure 1. For each interaction type, we need to consider the functional components, as discussed in Section III-A, and the non-functional requirements, as discussed in Section III-B. We have mentioned the challenges of HSt systems in Table I and we investigate the contributions in the state-of-the-art to identify the set of challenges each contribution have addressed.

Furthermore, we investigate the improvements each contribution aimed to provide for the healthcare sector by utilizing a BBHC solution. These improvements are related to the fundamental features of blockchain and SCs discussed in Section IV-A, and to a subset of the derived benefits addressed in Section IV-B.

We also briefly mention the objectives and the proposed mechanisms each contributions has suggested. For instance, MedChain [110] and MedRec [111] specifically focus on blockchain-enabled storage of medical records, while the authors of [112], [113], [114] provide blockchain-assisted access control solutions that supports fine-grained access to Electronic Health Records (EHRs) stored in an off-chain storage. Similarly, the authors of [25] propose the use of blockchain-based SCs to manage EHRs and IoT medical devices. An HD sharing system based on blockchain deployed in the cloud has been proposed in [25], [115]. Furthermore, the authors of [116] use blockchain along with other techniques such as *ciphertext-policy attribute-based encryption (CP-ABE)* cryptographic access control [117], and *content extraction signature* to support efficient access control to medical records, while the authors of [118] propose a healthcare blockchain system that uses SCs to support secure and automated remote patient monitoring. Recently, the authors of [119] have proposed a dynamic consent managing approach in clinical trails via private blockchain. Additionally, in [120], the authors propose a blockchain-enabled secure technique for sharing medical records in which symmetric cryptography is used to preserve the confidentiality of medical records. The solution by the authors utilizes *key-policy attribute-based encryption (KP-ABE)* as well as CP-ABE to control the access levels of different stakeholders involved in data accessing operations.

We additionally note down the data type each contribution claims to have focused on. We observe that there is no commonly accepted terminology or taxonomy for data types in this context. The surveyed state-of-the-art uses different terminology, e.g., Electronic Health Records (EMR), Personal Health Records (PMR), etc. In our work, we present a holistic definition of HD in Section II-A as data regarding individuals' physical and mental health conditions (e.g., dietary supplements, exercise and etc.), history of illness, received treatments, clinical trials, tests and results. However, for each work surveyed in Table III, we mention the terminology for the data type that the authors utilized in their work.

In a nutshell, we conduct a systematic classification of the contributions in the state-of-the-art and introduce each contribution as a formulation of (i) addressed HD data

TABLE III
EFFORTS TOWARDS ADDRESSING HEALTHCARE CHALLENGES BY BLOCKCHAIN-BASED SOLUTIONS

Proposal	Data Type	Interaction type[1]	Challenges Addressed[2]	Fundamental Blockchain Features[3]	Benefits[4]	Objective	Proposed Mechanism
[23]	EHR[5]	I_1	C_3, C_4 C_6, C_{10}, C_{13}, C_{19}	F_1, F_2, F_3	B_1, B_2, B_5, B_6, B_7, B_8	To provide patients the authority to access and control the transmission of their health records	To store access policies and links to off-chain stored data on-chain and control the access and authentication by SCs
[111]	EMR[6]	I_1, I_2	C_1, C_3, C_4, C_6, C_7, C_9, C_{10}, C_{16}, C_{17}, C_{19}	F_1, F_2	B_1, B_3, B_4, B_5, B_6, B_7, B_8	Provide to patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites	MedRec enables patient data sharing and incentives (access to anonymous HD) for medical researchers to sustain the system
[113], [114]	EMR	I_1	C_1, C_2, C_3, C_4, C_6, C_7, C_{10}	F_1	B_1, B_3, B_8	Present a new EMR access architecture to achieve a more precise granularity and flexibility for queries and access authorization	Based on the assumption that data will be stored online
[25]	EHR	I_1, I_4	C_5, C_6, C_9, C_{10}, C_{13}	F_1, F_3	B_1, B_3	Provide a remote healthcare monitoring system and abnormally detection	Use of SCs in Ethereum to address the security and privacy requirements
[115]	PHR[7]	I_1, I_2	C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_{10}, C_{19}	F_1, F_2	B_1, B_5, B_8	Enable users to own, control and share their PHR securely, in a GDPR compliant way and provide for researchers to collect high quality PHR	Classifying PHR into dynamic and static data for acquisition methods. Integrating blockchain and cloud storage
[116]	EMR	I_1	C_4, C_6, C_7, C_{10}, C_{19}	F_1, F_2	B_1, B_3, B_7	Blockchain-based privacy-preserving data sharing system for EMRs	Content extraction signature, Data stored on cloud and indexes on-chain, Access control policies governed by SCs
[119]	CTD[8]	I_1, I_2, I_3	C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_{12}, C_{13}, C_{14} C_{18}	F_1, F_2, F_3, F_4	B_1, B_2, B_7, B_8	GDPR-compliant and dynamic consent management for collection, storage and sharing of clinical trials	Integration between REDCAP, HyperLedger Fabric and Composer and a web application as an interface
[81]	EMD[9]	I_4	C_1, C_4, C_9	F_1, F_2	B_1, B_3, B_6	Efficient and scalable to record and access patient emergency relevant HD	Combining FTPS based file transfer tools and hyperledger fabric blockchain
[105]	HD	I_1	C_3, C_4, C_6, C_7, C_{11}, C_{13}, C_{14}	-	B_1, B_2, B_4, B_5, B_8	Facilitate private and auditable HD sharing and HD access permission handling by a blockchain-based system design	Anonymity based on SC IDs. Workflow automation by design of SCs. Integrity ensured with checksum.
[121]	-	-	C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_{12}, C_{13}, C_{14}, C_{18}	F_1, F_3, F_4	B_1, B_2, B_8, B_9	Scalable consent management system to ensure high throughput and low latency of endorsing data access requests and granting or revoking consent	Only manage and audits consent to data access rather than data itself, Built on top of hyperledger fabric, Design and analysis of the state world design in fabric
[122]	EHR	I_1	C_1, C_2, C_3, C_4	F_1, F_2, F_4	B_1, B_2, B_3, B_5, B_8	Efficient and fine-grained access control mechanism	Managing EHRs by using blockchain-based access control mechanism and hyper ledger fabric
[123]	EHR	-	C_1, C_3, C_6, C_8, C_{10}, C_{11}	F_1	B_1, B_3, B_5, B_7, B_8	Ensure security through blockchain an provide risk prediction of diseases of patient for prevention of critical cases	Privacy and security of EHR is managed in blockchain by using lattice cryptography which resists quantum attacks. Deep Learning prediction models on stored EHR Records
[124]	IoT&W[10]	I_1	C_1, C_6, C_7, C_9, C_{10}, C_{13}, C_{14}, C_{19}	F_1, F_2, F_3, F_4	B_1, B_2, B_3, B_7, B_8	GDPR-compliant data storage and sharing	Checksum of data and access policies stored on-chain, Encryption of Data
[125]	EMR / EHR	I_1	C_1, C_3, C_4, C_6, C_7, C_8, C_{10}, C_{13}, C_{14}, C_{18}	F_1, F_2, F_3, F_4	B_1, B_2, B_8, B_9	Secure and efficient data accessibility for the patient and the doctor	Signature of the encrypted data stored on-chain for authentication and integrity, data stored off chain
[126]	EMR	I_1, I_2, I_3	C_1, C_3, C_4, C_6, C_7, C_{11}, C_{12}, C_{13}, C_{14}, C_{19}	F_1, F_2, F_3, F_4	B_1, B_2, B_3, B_7, B_8	Propose a cross organizational EMR sharing framework to resolve the trust concerns	Predefined access policies by SCs and also granting access if necessary, Encrypted Data stored off-chain and hash of resource identifiers on-chain

(continued.)

TABLE III
(Continued.) EFFORTS TOWARDS ADDRESSING HEALTHCARE CHALLENGES BY BLOCKCHAIN-BASED SOLUTIONS

Proposal	Data Type	Interaction type	Challenges Addressed	Fundamental Blockchain Features	Benefits	Objective	Proposed Mechanism
[127]	CTD	I_1, I_4	C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{12}, C_{13}, C_{14}, C_{19}, C_{20}	F_1, F_2, F_3, F_4	B_1, B_2, B_6, B_8	Propose a decentralized application to foster effective CTD sharing while maintaining security of data sources and privacy of users	Authenticity developed SCs, Enforcing EHR standards, asymmetric encryption of data
[128]	EMR	I_1, I_2, I_3, I_4	C_1, C_3, C_4, C_6, C_9, C_{10}, C_{13}, C_{14}, C_{16}, C_{17}	F_1, F_3, F_4	B_1, B_2, B_3, B_4, B_8	Overcome the centralized model security and privacy shortcomings while enable patient centric data sharing via blockchain	Ethereum private blockchain, web-based interface to set access policies via SCs. Data stored off-chain, Request for access, access records, updates, policies and checksums stored on-chain
[129]	EHR	I_1, I_4	C_1, C_3, C_4, C_6, C_7, C_9, C_{10}, C_{13}, C_{18}, C_{19}	F_1, F_2, F_3	B_1, B_2, B_6, B_7, B_8, B_9	Patient centric health information exchange base on standards of the office of national coordinator	private ethereum ledger, SCs and features and asymmetric encryption. Blockchain to store and retrieve keys
[130]	MI[11]	I_1	C_1, C_3, C_4, C_6, C_{10}, C_{13}, C_{14}, C_{19}, C_{20}	F_1, F_2	B_1, B_2, B_5, B_7, B_8	Decentralized framework for storing and sharing medical images within a secure mechanism and enable patients for data ownership	Ethereum ledger and SCs for access policies and IPFS [131] for content addressing and storage
[132]	EMR & PHR	I_1	C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_{10}, C_{12}, C_{11}, C_{13}, C_{14}, C_{15}, C_{16}, C_{17}, C_{19}	F_1, F_2, F_3, F_4	B_1, B_2, B_4, B_6, B_7, B_8	Secure and efficient data management framework	Ethereum SCs for checking the authenticity and authorization of entities who want to access the data, under the assumption that every device has a pair of key
[133]	EHR	I_1	C_1, C_3, C_4, C_6, C_7, C_{10}, C_{13}, C_{14}, C_{19}	F_1, F_2, F_4	B_1, B_2, B_3, B_7, B_8	Decentralized healthcare network for secure EHRs sharing	Adopting the structure of MedRec, Signcryption to provide data authenticity, Attribute-based authentication to trace users who have accessed EHRs
[134]	HD	I_1, I_3, I_4	C_1, C_3, C_4, C_6, C_7, C_9, C_{10}, C_{11}, C_{13}, C_{14}	F_1	B_1, B_2, B_7, B_8	Present a system design where blockchain is used to share medical analyses between hospitals, medical clinics and RIs based on access policies defined by the patients	two types of chains: a private *sidechain* to keep information about real ID of the patients, and a public *mainchain* to store HD marked with a temporary ID to protect confidential data.
[135]	EMR	I_1, I_3, I_4	C_2, C_3, C_5, C_6, C_7, C_{11}, C_{12}, C_{13}, C_{14}, C_{19}	F_1, F_2	B_1, B_2, B_5, B_7, B_8	EMR sharing between institutions and the ability to collect and view a patient's entire medical history and to keep them anonymous	Data Stored in a centralized DB replicated and indexes stored on-chain while personal information excluded and stored with pseudo anonymous ID
[136]	CTD	I_1, I_4	C_2, C_3, C_4, C_{11}, C_{12}, C_{13}, C_{14}, C_{18}	F_3	B_2, B_6, B_8	To present a dynamic consent management architecture for privacy-preserving data acquisition for CTD analysis	No technical or implementation details presented
[137]	EHR	I_1, I_4	C_3, C_4, C_{10}	F_1	B_1, B_5, B_8	Propose and independent-update ABE scheme with multiple authorities for telemedicine systems	Attribute Based Encryption
[138]	PHR	I_1, I_2	C_3, C_6, C_7	F_1, F_2	B_1, B_5	Mobile healthcare for PHR data collection, sharing and collaboration	Implementation of access control scheme by utilizing hyperledger fabric

(continued.)

TABLE III
(Continued.) EFFORTS TOWARDS ADDRESSING HEALTHCARE CHALLENGES BY BLOCKCHAIN-BASED SOLUTIONS

Proposal	Data Type	Interaction type	Challenges Addressed	Fundamental Blockchain Features	Benefits	Objective	Proposed Mechanism
[139]	EHR	-	C_3, C_4, C_6, C_7, C_{10}, C_{16}, C_{17}	F_1, F_2	B_1, B_3, B_4, B_8	Blockchain-based searchable encryption scheme	Data stored off-chain in cloud, indexes stored on-chain. SCs used to authorize entities that can search the indexes of the data
[140]	EHR	I_1, I_4	C_3, C_4, C_6, C_7, C_{10}, C_{13}, C_{14}, C_{19}	F_1, F_2, F_3	B_1, B_2, B_6, B_7, B_8	Facilitate secure, trustable management, sharing and aggregation of EHR data	A hybrid data management approach where the actual EHR data will be encrypted and stored off-chain and the metadata will be stored on-chain in ledger
[141]	PLD[12]	I_1	C_2, C_3, C_4, C_6, C_7, C_{16}	F_1, F_4	B_1, B_4, B_8	Privacy-preserving scheme for fine-grained access control for large-scale physiological and wearable HD	Storage in IPFS and checksums stored on-chain
[142]	EHR & EMR	I_1, I_4	C_4, C_6, C_7, C_{14}, C_{19}	F_2, F_3	B_1, B_2, B_6, B_8	Efficient exchange of HD between patients and practitioners	Off-chain storage and a patient centered blockchain-based mobile and web UI for access control module
[143]	D&T[13]	I_1	C_6, C_{10}, C_{11}	F_1, F_2	B_1, B_3	Establish a shared key mechanism to meet the integrity, availability and privacy requirements of the data	Establish a shared key by using Sibling Intractable Function Families
[144]	HD	I_1, I_3	C_5, C_6, C_7, C_{11}, C_{12}, C_{13}, C_{14}, C_{19}	F_1, F_2, F_3, F_4	B_1, B_2, B_3, B_5, B_6, B_8	Enable patients to own and control their data without violating privacy	Utilizing blockchain as storage system and unified and simple indicator-centric schema as storage model. Purpose-centric access control
[145]	EMR	I_1	C_6, C_7, C_9, C_{10}, C_{19}	F_2	B_1, B_3, B_7, B_8	Enable users to have control over their sensitive data that are collected and stored by wearable sensors	asymmetric data for encryption, checksum of data stored on-chain with addition to metadata used for efficient locating of the data
[146]	PMR[14]	I_1	C_6, C_8	F_1, F_2	B_1	Tamper-proof EHR management system	Use of ethereum public blockchain to store checksum of data
[147]	-	-	C_{13}, C_{16}	F_3	B_2, B_4	Introduce a GDPR-compliant system to provide traceability of data and the right to be forgotten	Implementation of the right to be forgotten relies on the central based infrastructure of the data controller
[148]	EMR	I_1	C_1, C_3, C_6, C_7, C_8, C_{16}, C_{19}	F_1, F_2	B_1, B_4, B_7, B_8	Patient centric access control for EMR capable of providing security and privacy	Sharing session keys on-chain via encrypting it with users' public key and broadcasting it as a transaction for access granting, Data stored on-chain unless it's massive
[149]	EHR	I_1, I_4	C_1, C_3, C_4, C_6, C_7, C_{10}, C_{18}, C_{19}	F_1, F_2	B_1, B_5, B_7, B_8, B_9	Proposing a blockchain-based secure EHR system that would enable patients and healthcare providers to access and share health records in a usable yet privacy-preserving manner	Patients can modify consent with the use of SCs and cryptographic techniques. Healthcare providers can share and transfer data after getting consent from patients.
[150]	PHR & MD[15]	I_1, I_2	C_3, C_4, C_6, C_7, C_9, C_{14}, C_{17}, C_{19}	$F1_1$, F_2, F_3	B_1, B_2, B_3, B_4, B_8	To propose a multi-role healthcare data sharing system framework based on blockchain and reduce the MD storage cost	Collaborative storage of blockchain and IPFS. Multi-role data sharing system.

(continued.)

TABLE III
(Continued.) EFFORTS TOWARDS ADDRESSING HEALTHCARE CHALLENGES BY BLOCKCHAIN-BASED SOLUTIONS

Proposal	Data Type	Interaction type	Challenges Addressed	Fundamental Blockchain Features	Benefits	Objective	Proposed Mechanism
[151]	-	I_1, I_2	C_1, C_2, C_3, C_4, C_6, C_7, C_9, C_{10}, C_{11}, C_{19}	F_1, F_2	B_3, B_6, B_8	To propose a Multi-access Edge Computing (MEC) and blockchain-based service architecture for the real-time data privacy, integrity, and authentication between IoT, MEC, and cloud	Utilizing the lightweight ECQV (Elliptic Curve Qu-Vanstone) certificates
[152]	HD	I_1	C_1, C_6, C_8, C_9, C_{10}, C_{13}, C_{14}, C_{16}, C_{17}, C_{19}	F_1, F_2, F_3	B_2, B_4, B_7, B_8	To propose a decentralized health architecture that integrates mobile-edge computing and blockchain for data offloading and data sharing in distributed hospital networks	Privacy-aware data offloading scheme where mobile devices can offload IoHD HD to the nearby mobile edge computing server under system constraints.
[150]	HD	I_1, I_2	C_1, C_3, C_4, C_6, C_9, C_{10}, C_{19}	F_1, F_2	B_1, B_3, B_5, B_6, B_7, B_8	Proposing a multi-role HD sharing system framework based on blockchain	Collaborative storage of blockchain and IPFS.
[112]	EHR	I_1, I_4	C_1, C_4, C_6, C_7, C_{11}, C_{13}	F_2, F_4	B_1, B_8	Privacy preserving verification	Decentralizing attribute-based signature, off-chain storage scheme
[153]	EHR	I_1	C_3, C_6, C_{10}, C_{11}, C_{13}	F_1, F_2	B_1, B_5, B_8	Blockchain-based framework for efficient storage and maintenance of EHRs	Development of SCs
[154]	HD	I_3	C_9, C_{14}	F_1, F_3	B_3, B_8	GDPR-compliant data sharing scheme	Applicability of a federated blockchain in allowing participants to share data

[1]Interaction type identifiers (I#) are derived from Figure 1. [2]Challenges identifiers (C#) are derived from Table I. [3]Fundamental feature of blockchain and SCs (F#), and [4]their derived benefits for healthcare storage systems (B#) are derived from Figure 2.
Addressed data types by contributions in the state-of-the-art: [5]EHR: Electronic Health Records, [6]EMR: Electronic Medical Records, [7]PHR: Personal Health Records, [8]CTD: Clinical Trials Data, [9]EMD: Emergency Medical Data, [10]IoT&W: IoT devices data and wearables, [11]MI: Medical Images, [12]PLD: Physiological Data, [13]D&T: Diagnosis and Treatment, [14]PMR: Personal Medical Records, [15]MD: Medical Data.

type, (ii) interaction type, (iii) challenges in healthcare they addressed, (iv) fundamental features of blockchain and SCs as the motivation behind the proposed BBHC solution, (v) derived benefits of proposing the BBHC solution for the healthcare sector, (vi) the objective each contribution aimed to achieve, and finally, (vii) the proposed mechanism to achieve their objective. The outcome of this classification is demonstrated in Table III. Finally, in Table IV, we show the frequency of the proposed contributions in the existing literature with respect to the functional components and non-functional requirements of the healthcare systems. This table could motivate other researchers in the field to identify the less explored sub-domains of healthcare sector in order to further enhance the healthcare services by proposing a novel BBHC solution.

Furthermore, in Table IV we present a systematic classification of the contributions at the granularity of specific non-functional requirements applied to a specific functional component of a healthcare system as discussed in Section III.

B. Real-World Implementations

Having surveyed academic proposals, we now discuss several of the most well-known real world implementations as mentioned in [155]. These prototypes, projects and proof of concept efforts have the aim to solve some of the challenges we list in Section III and to advance the state-of-the-art in terms of practical contributions. They mainly focus on providing the solution for HD management and monitoring, lowering bureaucracy and administrative operation costs and overheads, and enhancing interoperability in healthcare domain.

Gem [156] is an enterprise blockchain company. In 2016, Gem began a partnership with Philips to provide a blockchain healthcare platform called "*Gem Health Network*". This platform is designed on top of the blockchain ledger and provides a possibility for developers to deploy distributed applications [157]. The platform utilizes a permissioned blockchain to enable managing the authorization of participants to access and modify sensitive information. The authors claim that they ensure anonymity in their system and that the platform follows HIPAA guidelines while providing efficient health services. The motivation behind Gem is to integrate and connect different entities and participants of the healthcare sector and to have the patient in control of data sharing in an integrated solution, with the aim of overcoming isolated silos.

Another platform, named *Guardtime MIDA*, was established in a partnership of *Guardtime* [158] and Estonian electronic Foundation in February 2016 [159]. The aim of the platform is to accelerate the adaption of blockchain's transparency

TABLE IV
CONTRIBUTIONS PER ADDRESSED FUNCTIONAL COMPONENTS AND NON-FUNCTIONAL REQUIREMENTS

Non-Functional Requirements		Functional Components		
		Data Collection	Data Storage	Data Sharing
Security	Authentication	[114], [115], [119], [81], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130], [132], [133], [134], [149], [151], [152], [150]		
	Authorization	[114], [115], [119], [121], [122], [127], [132], [135], [136], [151]	[23], [114], [115], [119], [121], [122], [123], [125], [126], [127], [128], [129], [130], [132], [133], [134], [135], [136], [153], [137], [138], [139], [140], [149], [151], [150]	[23], [114], [115], [116], [119], [81], [121], [122], [125], [126], [127], [128], [129], [130], [132], [133], [134], [135], [136], [137], [138], [139], [140], [141], [142], [149], [151], [150]
	Integrity	[25], [115], [119], [121], [127], [132], [135], [138]	[23], [112], [114], [25], [115], [116], [119], [121], [123], [124], [125], [126], [127], [128], [129], [130], [132], [133], [134], [135], [153], [138], [139], [140], [141], [142], [143], [144], [145], [146], [149], [151], [152], [150]	[112], [114], [115], [116], [119], [121], [124], [125], [126], [127], [129], [132], [133], [134], [135], [138], [139], [140], [141], [142], [144], [145], [149], [151]
	Non-Repudiation	[112], [123], [125], [127], [146], [152]		
	Availability	[25], [81], [124], [127], [128], [129], [134], [145], [154], [151], [152], [150]		
Privacy	Confidentiality	[23], [114], [25], [115], [116], [123], [124], [125], [128], [129], [130], [132], [133], [134], [135], [153], [137], [139], [140], [141], [143], [145], [149], [151], [152], [150]		
	Anonymity & Unlinkability	[112], [126], [132], [134], [135], [136], [153], [143], [144], [151]		
	Transparency & Auditability	[119], [121], [126], [127], [132], [135], [136], [144]	[23], [112], [25], [119], [121], [124], [125], [126], [127], [128], [129], [130], [132], [133], [134], [135], [136], [153], [140], [144], [147], [152]	[119], [121], [125], [126], [127], [128], [130], [132], [133], [134], [135], [136], [140], [142], [144], [154], [152]
	Accountable Privacy	[132]	[128], [132], [139], [147], [152]	[128], [132], [139], [152]
	Consent Management	[119], [121], [125], [129], [136], [149]		
Interoperability		[23], [115], [116], [123], [124], [126], [127], [129], [130], [132], [133], [135], [140], [141], [142], [144], [145], [149], [151], [152], [150]		

and auditability features into the patients' HD management. The aim of the partnership was to overcome the challenges of HD exchange between different health providers, boost the interoperability of the HIs, enhance cross organizational accountability, reduce operational costs and provide artifacts for event and state detection from legal, audit, and compliance perspectives.

The motivation behind proposing *BurstIQ* [160] is to develop a platform and ecosystem that overcomes the challenges of isolated, inaccessible and non-standardized HD storage, access and sharing. BurstIQ utilizes and integrates blockchain technology, big data analytics, and machine learning techniques in addition to maintaining the security and privacy requirements as defined by HIPAA. Scattered data sources in this platform are unified and combined to form the *LifeGraphs*^{TM} within the platform. This structure will then be used as a basis for proposing *HealthWallet*^{TM} which can be used by healthcare participants to store, share and access their intended data.

Medicalchain [161] is a distributed ledger that allows permissioned based blockchain to securely store health and patient records. Medicalchain ledger will provide to its users the possibility to grant permission to other health providers in order to access their HD.

Another platform to propose a BBHC system is *PokitDok* [162]. PokitDok implements a platform-as-a-service paradigm allowing users to interact with other trading partners in the established *DokChain health alliance* platform to run applications on DokChain. The API offered by the platform facilitates eligibility checks, claims submissions, appointment scheduling, payment optimization, patient identity management, and pharmacy benefits.

The authors of *Cortex* [163] introduce a *hierarchical deterministic* based wallet for their proposed system [164]. This wallet controls access to the personal information and contains a tree-like structure with keys. Since different permissions strategies (namely read-only or read/write) with respect to accessing the data can be managed by users for every other node in the tree, users are provided a fine-grained access control mechanism for each and every sub-tree in the data storage layer. This data structure and format enables a flexible and easy to integrate structure with other third parties. In order

to be compliant with data protection regulations, the platform exploits data anonymization technique to protect the privacy of the users and their interactions in the platform.

Applying blockchain has also been proposed for additional applications in the healthcare sector that are beyond the scope we set for our survey in Section II-A. For instance *Modum* [165] and *iSolve* [166] have proposed exploiting blockchain for pharmaceutical management.

C. Summary and Lessons Learned

In this section, we provide a comprehensive analysis of the state-of-the-art efforts on integrating blockchain and SCs in different healthcare applications. These efforts aim at addressing one or more challenges mentioned in Table I. We have considered works proposed by both academia and industry. For each surveyed work, in addition to providing a brief description of the proposed approach and objectives, we identify the interaction types and HD related challenges it addresses, and the fundamental or derived features of blockchain and SCs that it utilizes. All these findings are summarized in Table III.

Key lessons learned from the review of BBHC solutions presented in the academic state-of-the-art and real-world implementations are summarized below:

- Most of the academic contributions in the state-of-the-art are focused on challenges related to HD storage and sharing as Table IV demonstrates. A number of BBHC solutions have also focused on HD collection, IoHT, sensors, and wearables. However, other functionalities of HSt systems (such as HD processing) are not considered in the existing literature. Additionally, a majority of the existing BBHC solutions are not evaluated with real data traces which makes it hard to assess their performance when deployed in real-world scenarios.
- We observe that each of the existing BBHC solutions focuses on a small subset of challenges mentioned in Table I, whereas it is important that most (if not all) of these challenges be addressed to create a secure, efficient and practical BBHC system. Therefore, there is a need to design BBHC systems in which different technologies are dynamically integrated into an organic whole in an efficient manner. Since the HD data is personal and sensitive in nature, the security and privacy related challenges require additional consideration during the design of a BBHC system.
- Several of the surveyed real-world implementations have been focusing on the integration of blockchain technology and smart contracts within healthcare storage systems. In particular, some of these implementations provide a blockchain-based data wallet aiming at providing the patients with the ability to manage authorization w.r.t. access to HD, transparent view of access logs, etc. However, since the proposed prototypes, projects, and proof of concept efforts are at early stages of development, it is too early to predict the extent of blockchain adoption in national infrastructures for medical storage or in EHR software.
- The existing BBHC solutions in the academic and real-world implementations are in the stage of high-level application design or initial pilots. A more thorough analysis is required to understand the practical requirements of BBHC solutions in more concrete and context-driven applications.

VI. Related Work

The rapid proliferation of blockchain deployments in the healthcare domain has resulted in a number of research efforts and publications over the last few years. Moreover, there exist survey articles that summarize the key findings from the available literature on Blockchain-based Healthcare (BBHC) solutions. Next, we will discuss these surveys in brief and describe how our survey advances the state-of-the-art.

The authors of [16] present a survey which specifically discusses the issues related to security and privacy during HD-sharing in BBHC systems. The survey classifies the existing solutions based on their blockchain platform type, i.e., permissionless and permissioned, and provides a detailed discussion of their benefits and limitations. The survey also discusses the issues related to the centralized storage platforms and cryptographic protocols that are currently being used to store the medical records in a secure and confidential manner.

Moreover, the authors present a discussion on the future of blockchain technology in HD sharing domain, which includes the usage of fine-grained access control techniques, solutions for efficient searching on encrypted data, and use of SCs. However, the paper lacks discussion on some important topics such as security and privacy while using off-chain data storage solutions, privacy solutions that support GDPR regulations, and secure consent management techniques.

In a recently published work [27], the authors provide a review of the research concerning the usage of blockchain in healthcare. The discussion includes the proposed systems (i.e., frameworks, concepts, and models), prototypes, and implementation techniques. Moreover, the reviewed blockchain-based solutions are compared with traditional healthcare data management methods, and the emerging trends in the area are discussed. In particular, the authors provide a generic overview of the currently existing efforts related to blockchain-based solutions without going into specific details. The scope of this review does not include issues such as interoperability, security and privacy, and scalability, which are important when designing a practical blockchain-based solution for healthcare applications.

An interesting study about research efforts in BBHC is presented in [28]. In particular, the authors aim to discover, extract, analyze, and synthesize the studies on the symbiosis of blockchain-based solutions in healthcare. The reviewed research works were mapped to one of the five primary scenarios (i.e., medical record sharing, medical supply chain, insurance claims, medical education, and clinical research) which are considered as potential healthcare applications where blockchain usage can provide improvements.

Moreover, a framework that will facilitate new research directions has been provided along with the establishment of

the state-of-evidence with an in-depth assessment. However, this work only reviews the research works that have been published until late 2018, whereas the research activities on BBHC solutions have rapidly increased in recent years. Another survey is presented in [29], with the main focus on the techniques for performing the systematic review. Furthermore, both these surveys leave a number of issues out of scope, such as SCs, and ongoing industrial efforts and pilots on BBHC applications.

Recently, the authors of [30] provided a survey of blockchain-based strategies for the healthcare domain. The paper includes a discussion of various solutions concerning medical record sharing, log management, patient monitoring, and consensus protocols in BBHC systems. It provides in-depth exploration of use cases such as healthcare IoT and supply chain management along with the security and privacy challenges in healthcare that could be addressed using blockchain technology. The survey additionally includes a brief discussion of industry efforts for improving medical information management by using blockchain technology, but it only considers two platforms (Medicalchain [167], and MedChain [110]). Moreover, the authors do not cover advantages of using SCs and dynamic consent management.

In addition, there exist other surveys that study blockchain challenges and benefits in multiple domains, including the healthcare sector. The authors of [168] study how blockchain technology is applied in the realm of smart cities from several perspectives including smart healthcare and supply chain management. The paper includes a discussion of how inhabitants of smart cities can gain benefits from the advances in medical technology and more specifically, blockchain-based solutions. Another recent survey presented in [169] provides an overview of blockchain and big data as well as the motivation behind their integration. The authors survey various blockchain services for big data acquisition, storage, analytics, and preservation in different blockchain applications such as smart healthcare.

Moreover, the authors of [170] study security concerns and vulnerabilities of blockchain-based applications in multiple domains, including healthcare. An in-depth survey of blockchain and cloud of things (BCoT) integration and its applications in different use-case domains such as smart healthcare is provided in [171]. Another survey presented in [172] studies potential applications of the blockchain technology and highlights the challenges and possible directions of blockchain research in healthcare from the perspective of data sharing, managing health records, and access control. The authors of [173] briefly discuss negative and positive effects of integrating blockchain technology in the healthcare sector.

Finally, there exist shorter surveys that target specific issues in BBHC. Reference [174] provides a survey on blockchain-based solutions that aims to address the challenges in specific e-health applications (e.g., patient monitoring, and smart pills). Reference [31] provides a review on how blockchain technology can facilitate the transition from business-driven to patient-driven interoperability by using five mechanisms for digital access rules, data aggregation, data liquidity, patient identity, and immutability. Reference [32] gives a generic overview of research challenges and opportunities that blockchain provides in the healthcare domain. Reference [175] lists the technical and legal challenges of blockchain technology applications in several domains, including the healthcare sector.

We summarize the comparison between the existing surveys and our work in Table V. More specifically, the table compares our survey with the aforementioned existing surveys which study BBHC solutions from the perspective of security, privacy, or interoperability. We conclude that our study has five novel elements (NOE) that advance the state-of-the-art.

To the best of our knowledge, our study is the first survey to (NOE_1) provide a systematic consideration of functionalities in HSt systems as opposed to considering specific scenarios, (NOE_2) provide a comprehensive and systematic analysis of challenges that HSt systems are facing, (NOE_3) systematically categorize the interaction types in HSt system and to consider the effect of the interaction types and their impact on HSt system challenges, benefits of blockchain-based solutions in healthcare sector, and research gaps, (NOE_4) provide a systematic mapping of blockchain-based contributions and solutions in the state-of-the-art to the taxonomy of (i) interaction types (I), (ii) HSt system challenges (C), (iii) fundamental features of blockchain and SCs (F), and (iv) derived benefits of blockchain and SCs for HSt systems (B), and finally, (NOE_5) consider compliance with various data protection rules and regulations in detail.

To demonstrate our first novel element, NOE_1, in Table V, we consider the functional components of HSt system we identify in Section III-A, namely, HD collection, storage, sharing, and transfer. While HD storage and sharing have already been considered by other surveys in the existing literature, the analysis has only been performed in the context of specific scenarios in healthcare systems. On the other hand, we discuss the general entities in healthcare systems in a broader context, as illustrated in Figure 1 and derive the functional components of HSt systems via a systematic analysis based on the functionalities of these entities. In particular, we are the first survey to consider HD collection in our work, and also to differentiate between HD sharing and HD transfer as per requirements of GDPR. To the best of our knowledge, our study is also the first to investigate the effects of functional components of HSt systems on challenges and consider how blockchain and SCs can contribute to overcoming these challenges within each functional component. In Table V, we indicate whether different surveys have considered each of the functional components in their study. We use "✓" to signify that the component has been considered (potentially in the context of a specific scenario) and "✗" otherwise.

Regarding NOE2, we derive challenges systematically by considering each non-functional requirement in the context of each functional component. We discuss each challenge, giving examples and connecting the challenge to the underlying non-functional requirement. This way, we end up with the 20 challenges discussed in Section III and presented in Table I. We also explain in Section III that the implications of non-functional requirements (and consequently challenges) differ for each functional component. In Table V, we compare coverage of challenges with other surveys in the state-of-the-art.

TABLE V
COMPARISON WITH STATE OF THE ART SURVEYS

Features \ References		[16]	[27]	[28]	[29]	[30]	[31]	[32]	[176]	[177]	[178]	[179]	[180]	Our Work
NOE_1	HD Collection	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓
	HD Storage	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓
	HD Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	HD Transfer	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
NOE_2	C_1	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
	C_3	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✓	✗	✓
	C_7	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓
	C_9	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓
	C_{14}	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
	C_{20}	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓	✓
	C_2, C_4, C_5, C_{12}, C_{15} to C_{18}	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
NOE_3	Security requirements, challenges, and benefits	I_1, I_4	I_1, I_4	I_1, I_4	I_1, I_4	I_1	✗	I_1, I_4	I_1	I_1, I_2	I_1	I_1	I_1	I_1, I_2, I_3, I_4
	Privacy requirements, challenges, and benefits	I_1	I_4	I_4	I_4	I_1	✗	I_1, I_4	I_1	I_1, I_2	I_1	I_1	I_1	I_1, I_2, I_3, I_4
	Interoperability requirements, challenges, and benefits	I_4	I_4	I_1, I_4	I_1	I_1	✗	I_4	I_1	I_1, I_2	I_1	I_1	✗	I_1, I_2, I_3, I_4
	Research Gaps	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	I_5, I_6
NOE_4	Interaction Types (I)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	Challenges of HSt systems (C)	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓
	Fundamental Blockchain and SC benefits (F)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	Derived benefits of blockchain and SCs in healthcare (B)	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓
NOE_5	HIPAA	‡[1]	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	‡
	GDPR	✗	✗	✗	✗	‡	✗	✗	✗	✗	✗	✗	✗	✓

[1]‡: Considered at coarse granularity

In our comparison, we leave out the challenges that have been covered by all surveys and focus on the remaining challenges with partial coverage. We use "✓" to denote that a challenge and its underlying context are discussed in a given survey (beyond brief mentioning), and "✗" otherwise.

NOE_3 consists in systematically categorizing interaction types of HSt systems, as discussed in Section II-A. Furthermore, we consider the impact of the interaction types on challenges in HSt systems, benefits that blockchain-based solutions can propose, and on the research gaps in the state-of-the-art. In Table V, we analyze the coverage of the interaction types by different surveys. While existing surveys do not consider an explicit taxonomy of interaction types, the relevant interaction type can be inferred from the context in most cases. We perform this coverage analysis separately for each of the four subcategories. The first three subcategories are about coverage of interaction types when discussing security-related, privacy-related, and interoperability-related aspects (i.e., groups of non-functional requirements and challenges presented in Table I). The fourth subcategory is about coverage of interaction types when discussing research gaps. For each group, we mention in Table V the interaction types (I_1 to I_6) each survey considers in their study. We use "✗" to indicate that a specific survey does not consider any interaction types in the context of one of the four aforementioned aspects.

Furthermore, as part of NOE_4, we systematically map each solution and system in the existing literature to the proposed taxonomy by the (i) considered interaction types, (ii) addressed challenges in each functional component in HSt systems, (iii) utilized fundamental blockchain and SCs features, and (iv) employed benefits of blockchain and SCs for the HSt systems. In Table III, we demonstrate this novel element by analyzing if other surveys have mapped the blockchain-based solutions existing in the state-of-the-art to each element of the proposed taxonomy. We use "✓" to signify presence of a mapping and "✗" to refer to lack thereof.

Regarding NOE_5, we consider in Table III how our and other surveys cover compliance with data protection rules and regulations. In this context, we differentiate between coarse-grained and fine-grained coverage. For instance, in this study we mention HIPAA guidelines on HD wherever applicable but only as general rules and guidelines. We do not consider how HIPAA rules and regulations can affect challenges of HSt systems and derived benefits of blockchain and SCs. On the other hand, when considering compliance with GDPR, we mention the challenges that GDPR articles bring to the HSt systems. We present affected functional components and additional issues for fulfilling non-functional requirements in HSt systems in Section III. We also consider how specific derived benefits of blockchain and SCs can help overcome

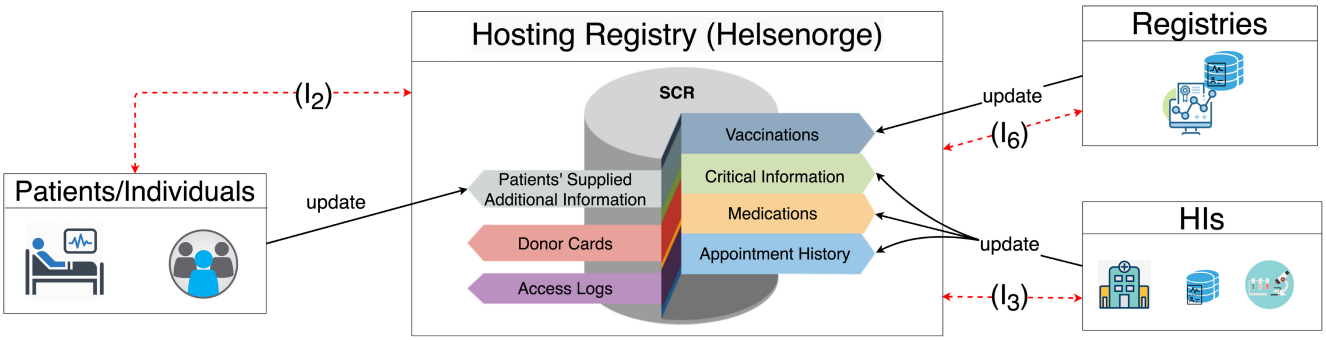

Fig. 3. An overview of interactions in SCR.

GDPR-related challenges. Hence, we say that our study considers compliance with GDPR at fine granularity and with HIPAA at coarse granularity.

We have performed a similar analysis for other surveys. Several surveys have considered data protection rules at coarse granularity and mentioned regulations such as HIPAA. However, none of the surveys in the state-of-the-art consider compliance with data protection rules at fine granularity. To visualize the coverage of compliance in Table III, we use "✓", "‡", and "✗" to indicate fine-grained coverage, coarse-grained coverage, and coverage being beyond the scope of a survey, respectively.

VII. Use-Case: Summary Care Records

In certain medical emergencies, having access to a summary of patients' health records (e.g., those pertaining to the allergies, blood type, and medications) can be a matter of life and death.

As mentioned in Section III, one of the main challenges of healthcare systems is lack of unified and holistic view of HD and scattered HD. HD are usually scattered among different health providers as patients are transferred between different organizations and hospitals and they relocate to different cities and countries.

In order to address the issue of scattered HD and to provide healthcare professionals with fast access to important health information about patients, *Summary care record (SCR)* are maintained for patients.

SCR is an electronic health system (a health information exchange) that provides access to selected patient information adapted to medical emergencies regardless of where patients received their treatment [181]. SCR is maintained at national level for citizens of many countries (such as England [182], Australia [183], Netherlands [184], and others as reported in [185]).

Since the information stored in SCRs can vary per country, for the rest of this section, we will focus on the Norwegian SCR system (called as the *kjernejournal* in Norway). In Section VII-A, we provide and overview of the Norwegian SCR system. Later in Section VII-B, we identify the concrete issues observed in the Norwegian SCR system and in Section VII-C we describe how blockchain technology and smart contracts can be beneficial to resolve these issues. Although these issues were observed in the context of Norwegian SCR, it is highly likely that the same SCR issues and benefits of the blockchain technology also apply to other national SCR systems.

A. Overview of Norwegian SCR

As of Spring 2017, the Norwegian SCR system had been rolled out to all hospitals, emergency call-centers, duty medical response-offices and dominant majority of the general practitioners [186] in Norway.

SCR in the Norwegian healthcare system collates information from multiple sources: it includes i) appointment history, ii) log of SCR usage iii) vaccinations, iv) critical information, v) patient supplied additional information, vi) donor cards, and vii) medications. The SCR is available to both patients and healthcare professionals [187].

Patients, registries, and HIs are the entities involved in accessing and updating SCRs and all information in SCR can be accessed by patients and HIs. Figure 3 illustrates the interactions that these entities conduct with SCRs. As we explain in detail below, patients update the patients' supplied additional information and donor cards. Critical information, medications, and appointment history are updated by HIs while information about vaccinations are maintained and updated within the associated registries.

In Norway, SCRs are hosted and managed by *Helsenorge* [188] which is a healthcare registry in the Norwegian healthcare system. Appointment history and information about the time and place of HSs that patients have received is also added to their SCR by the hosting registry. Additionally all queries for information that are stored within SCR are logged and patients can keep track of healthcare professionals who have accessed their SCR. The log is maintained by the hosting registry and is supposed to provide an overview of the date and the reason why their SCR was accessed and by which healthcare professional.

As mentioned earlier, SCRs are maintained by the hosting registry. However, other registries can also provide additional information to the SCR via *application programming interfaces (APIs)* that are within the SCR. SCRs include APIs to fetch the vaccination data in case other entities seek access to this data. For instance, in Norway, healthcare professionals can see patients' vaccination status in the SCR system which will be fetched from SYSVAK via APIs in case of need.

Critical information is registered into SCR by healthcare professionals at HIs, with patients consultation. Critical information has a vital role on the type of HSs that patients

will receive by healthcare providers. Examples of critical information in SCR and its effect on patients' HSs include severe allergies or hypersensitivity reactions to penicillin, previous narcosis issues, important treatments that patients are receiving, such as dialysis, life-prolonging treatments, and rare and severe conditions such as hemophilia.

Patients can contribute to improving their own SCR by providing patient-supplied additional information. This information help healthcare professionals to have a more complete view of their HD and health condition. This information can include i) contact information of relatives in case of illness or emergency, ii) special communication needs w.r.t vision, hearing, speech, language and etc., and iii) health condition or special diseases that healthcare professionals should be aware of. Patient-supplied additional information are added to the SCRs as a backup mechanism. This information is only accessed and trusted by healthcare professionals if there exists no related data in other parts of SCRs.

Additionally, patients are able to create a digital donor card in their SCR. Moreover, as patients collect prescribed medications from Norwegian pharmacies, a record about those medication is also added to their SCR [187].

B. Concrete Issues Observed in Norwegian SCR

The general challenges of healthcare storage systems in different interactions between entities, as listed in Table I, are also applicable to the case of SCR. Despite the huge financial investment and resources devoted to the Norwegian SCR system, the SCR is still not a routinely used tool in the Norwegian healthcare sector. In this section, we will focus on the concrete issues that have been observed and provide discussion on how these issues map to the general challenges of healthcare storage systems.

1) Lack of Transparency and Auditability of Updates on SCRs: Authors of [189] have conducted in-depth interviews with doctors and healthcare professionals from emergency clinics about the use of SCR in Norway. The results of the study show that healthcare professionals put limited trust in the HD quality of the SCR system since healthcare providers have to manually update the critical information about serious allergies, disorders, or other vital information on an on-going basis. The conclusion of the analysis suggests that trustworthiness is a particularly important issue in relation to doctors' use of SCR in Norway.

SCRs are accessed by healthcare professionals in case of emergency. In this scenario, patients are not in a condition to verify their HD and provide inputs for healthcare professionals. Hence, healthcare professionals need fast access to correct HD to be able to treat the patients. For instance, allergic reactions to certain medicines are vital information in the treatment that patients receive in case of an emergency.

Moreover, the impact of the health professionals' response time is a crucial parameter for patients in emergency as studied in [190]. If healthcare professionals do not trust the data that is stored in the SCR, as the results of the study of authors in [181] suggest, they might lose valuable time in a critical situation.

The issue with lack of trust of healthcare professionals in HD quality stored in SCR can be mapped to several general challenges of HSt systems we list in Table I; more specifically to C_{12} - C_{17} which refer to lack of transparency, auditability, and accountability in different functional components, namely collection, storage, and sharing of HSt systems.

Currently in the SCR systems, healthcare professionals have no ability to verify if the patients' SCRs are updated and include all relevant information about the treatments, laboratory results, etc. In fact, there exist no transparent view or an auditable mechanisms available for healthcare professionals to verify if the HD on SCRs are regularly updated by other healthcare professionals. While the SCR includes access logs, these logs are only accessible to the patients and only by request. To make it worse, updating the logs is the sole responsibility of the hosting registry of Helsenorge and the update procedure itself is not transparent. This issue can significantly impact the trust of healthcare professionals in the quality of HD stored in SCRs as the study in [189] suggests.

2) Data Snooping: As reported by the *Norwegian Board of Health* in its annual report [191], it is important that patients do not hesitate to receive HSs because of worrying that unauthorized people will have access to private information. Moreover, section 21.a of the *Health Personnel Act* [192] prohibits healthcare professionals from accessing patients' data without a concrete medical reason even if they are relatives with the patient. The privacy of patients must be safeguarded to ensure that individuals and patients have confidence in both healthcare professionals and the HSs they receive.

In Norway, multiple cases of snooping into patients data by doctors and nurses (who have not been the assigned healthcare professionals for patient treatment) have been reported on national news and media [193], [194], [195]. These incidents highlight the vulnerabilities and shortcomings in the Norwegian SCR.

Although patients have the ability to view the log of access to their SCR in the currently used SCR system in Norway, they have no alternative other than to trust authorities that provide reports of access to their SCR. The issues w.r.t HD snooping in SCRs highlight the requirement for having auditable and transparent view of SCR access logs. Patients need to have a transparent view of who have accessed their records, for what purpose and duration, and other criteria listed in Section III-B2c.

The issue w.r.t. data snooping in SCR can be mapped to several general challenges of HSt systems we mention in Table I; specifically C_2-C_4) authorization, C_7) access policy integrity, C_9) dependency and distrust in a third party, C_{12}-C_{17}) transparency, auditing, and accountable privacy in SCR management, and C_{18}) consent management.

C. Benefits of Blockchain and Smart Contracts for Norwegian SCR

In this section, we focus on how the blockchain technology and smart contracts can help to overcome the issues in the Norwegian SCR system described in Section VII-B. We also explain how this is related to the discussion of fundamental blockchain features in Section IV-A and to derived blockchain benefits in the healthcare domain discussed in Section IV-B.

As mentioned in Section VII-B1, one of the concrete issues observed in the Norwegian SCR system is that healthcare professionals do not trust the quality of HD stored in SCR.

One of the reasons for this lack of trust is that the information in SCR is updated with significant delay, and sometimes important information is not presented in the summary at all.

In order to address this, a blockchain-assisted SCR management systems could be devised. If the history of appointments and updates to the SCR are stored in the blockchain ledger, healthcare professionals could benefit from a transparent, fine-granular, and tamper-proof view of the logs of updates of HD in SCRs without the need of a trusted third party. A consortium blockchain for instance, can provide transparency to certain entities to facilitate verifiability of the stored data and to keep data confidential from unauthorized entities (as discussed more in detail in Section IV). In case of SCR, healthcare professionals will have the limited transparency to verify the history of patients' appointments and the updates to their SCR. The information w.r.t updates to the SCRs will also remain tamper-proof if stored in the blockchain ledger thanks to the data integrity feature of blockchain technology (discussed more in detail in Section IV-A2).

Moreover, authorized healthcare professionals will be provided a fine-granular view of the updates on SCR. Since the identity of healthcare professionals is typically known to the blockchain-based SCR storage systems, the transparent view of patients' appointment history and updates to the SCR could be provided along with the identity of responsible healthcare professionals. This level of granularity could increase the trust in the quality of information, alongside enhanced auditability. Additionally, if an important record is missing in an SCR, the root cause of the problem could be detected by comparing the SCR update log with other sources such as the appointment history. In this case, the faulty party could be held accountable.

The other concrete issue observed in the Norwegian SCR that could be resolved by using blockchain technology and smart contracts is the HD snooping discussed in Section VII-B2. In order to resolve this issue, records of accessing patients' HD on SCRs should be logged in a fine-granular manner; no single entity should have the ability to alter, hide, or remove these records.

If healthcare professionals are provided with smart contract API to get read or write access to the HD on SCRs, the log of the access operations could be kept on-chain. Moreover, if the identity of the healthcare professionals is known to the blockchain-based SCR management system, every access transaction will be signed by the private key. In this way, the blockchain-based SCR management system will provide non-repudiable evidence of healthcare professionals accessing HD on patients' SCRs.

Access management smart contracts could also be created with a pre-defined set of standards to log HD access by healthcare professionals at fine granularity (such as access purpose, healthcare professional identity, access duration, type of data, etc.). This level of granularity is required to provide compliance with personal data protection rules and regulations and preserve patients' privacy requirements that are mentioned in Section II.

Furthermore, by exploiting smart contracts for accessing SCRs, the information w.r.t access logs will be stored tamper-proof in the blockchain ledger and without the need of a trusted third party to maintain the access logs. In addition, the verifiability, transparency, and auditability features of blockchain technology and smart contracts (as discussed in Figure 2) endow patients with the ability to track access logs to their SCRs. Patients can monitor healthcare professionals that are accessing their data and verify the access log by comparing it with the HSs they have received. This can also be done without relying on trusted authorities such as the Helsenorge registry in the Norwegian SCR context.

VIII. Research Gaps and Future Research Directions

Despite the promising contributions in both academic literature and real-world implementations, some significant challenges remain unresolved in the integration of blockchain technology and SCs in the healthcare sector. In this section, we will mention the challenges and research gaps we have observed in the state of the art. It is noteworthy to mention that the research gaps we will mention are defined in the scope of the overview of healthcare we presented in Section II-A.

Following the study of both academic contributions and real-world implementations, we have identified a number of research gaps in the state-of-the-art. In this section, we discuss (RG_1) HD sharing between patients, (RG_2) HD sharing between Registries and RIs, (RG_3) creating patients and individuals identity, (RG_4) interoperability between blockchain-based healthcare systems, (RG_5) applicability of permissionless blockchain for BBHC system, (RG_6) mapping of the BBHC to individual blockchain systems, (RG_7) enabling network and communication technologies, and finally, (RG_8) potential usage of SCs in BBHC systems. We demonstrate research gaps RG_1 to RG_4 in Figure 4. Since RG_5 to RG_8 apply to all interaction types presented in Section II-A, we do not visualize their association with specific elements of BBHC systems.

A. HD Sharing Between Patients

As mentioned in the overview of healthcare systems in Section II-A and presented in Figure 1, I_5 involves patients and/or individuals interacting with each other. This is done by sharing personal HD with other patients, e.g., in order to gain more information and knowledge about the health condition they have to deal with. However, it can be observed in Table III that no related work has focused on this interaction type.

The interaction between patients and/or individuals is different from the other interaction type addressed by the existing literature. Patients and individuals are not obligated by any regulations to keep their data secure and comply to any privacy requirements. They can share their most sensitive HD without realizing the consequences for their privacy.

As of today, no platform adequately supports HD sharing functionality for patients and individuals. Although patients and individuals might chose to share their HD and the experiences they had with healthcare services with other individuals in social networks and forums, this is not a desirable solution from the privacy perspective. The access control mechanism

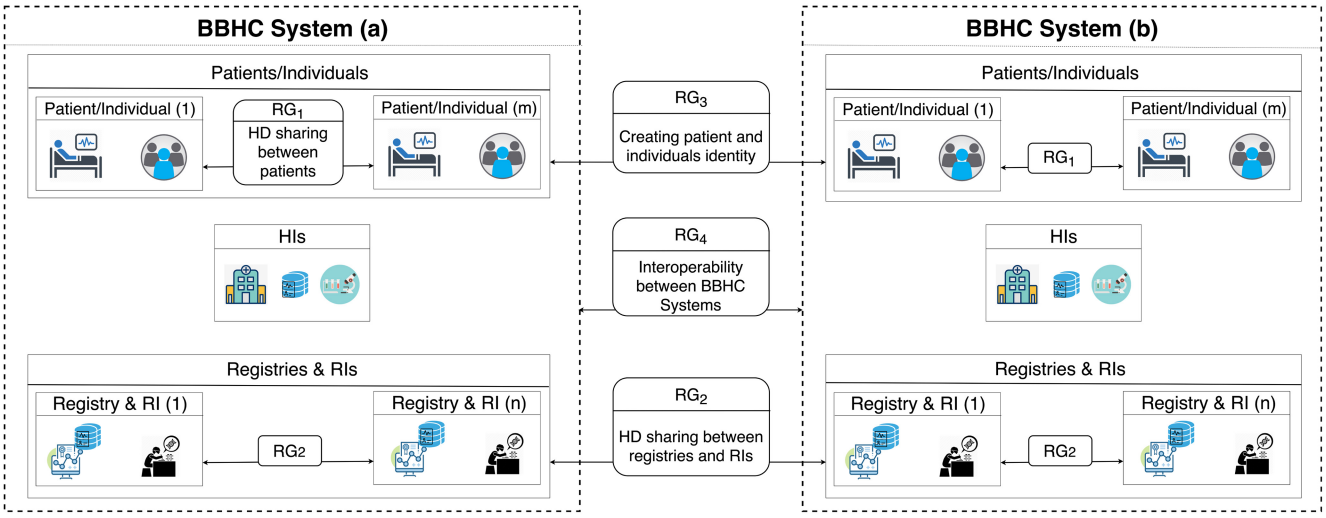

Fig. 4. An overview of research gaps in the existing literature and future research directions.

patients have on sharing their data on such forums today is limited to defining a list of other individuals who can see their HD and trusting those individuals to not share their HD any further.

Even if any explicit identifiers are excluded from the shared HD, specific HD such as genomics, contain information that may be used to identify person. HD linkability further exacerbates the problem. Patients and individuals cannot be solely considered responsible for preserving their privacy and confidentiality in a data sharing platform. Many attackers can trick patients into sharing their most sensitive HD to gain advantage of having access to their personal data. This scenario can be a crucial violation of patients' privacy and their HD security. These challenges highlight the necessity of a platform for secure and privacy-preserving health information sharing across patients.

Blockchain and SCs can facilitate creation of such platforms due to their desirable features such as non-repudiation, lack of need for a trusted third party, verifiability, accountability, etc. For instance, a blockchain can store filtered impersonal data subsets on-chain for the purpose of verification while the personal info will be stored off-chain. blockchain can also store an accountable and non-refutable history of sharing interactions across patients. However, there still remain unresolved challenges that would require further research.

First, it remains an open question who will host such a blockchain-based system and who will act as a node. Additionally, securely storing the HD off-chain, while preserving patient' privacy and not revealing any sensitive and personal information is a non-trivial task. Cloud-based storage and sharing have been proposed by the existing literature as surveyed by authors in [196]. However, cloud-based data sharing can violate patients' privacy requirements as we discussed in Section III-B2.

Furthermore, patients might intend to share their HD with other patients in various locations, and hence, in the scope of other BBHC systems. This scenario in fact can make the secure access management of such a sharing and guaranteeing patients' privacy more challenging. Since privacy requirements differ under various data protection rules in different jurisdictions, when patients share their HD from a healthcare service they received in one jurisdiction with a person in another jurisdiction, this may pose additional privacy concerns. Due to these and other challenges, creating such a sharing platform requires significant further analysis and research.

B. HD Sharing Between Registries and RIs

Similar to RG_1, the interaction between healthcare registries and between other RIs has not been the focus in the state-of-the-art as it can be observed based on Table III.

As mentioned earlier in Section II-A, a cancer registry and a cause of death registry, for instance, need to establish an interaction channel to keep their data updated and correct. The cancer registry requires information on the status of the patient. When a death is recorded in the cause of death registry, this information needs to be transferred to the cancer registry to ensure correct statistics on survival and mortality. The death certificate available to the cause of death registry may not indicate that a cancer disease has contributed to the underlying cause of death. In this case, the cancer registry needs to transfer relevant information to the cause of the death registry in order to ensure correct data and statistics.

Additionally, RIs need open and transparent collaboration to share their knowledge and benefit the society with the outcome of their research. Healthcare research can provide important information and discoveries about different aspects of healthcare services such as disease trends and risk factors, patterns of care, new discoveries about diseases and drugs, healthcare costs and more [197].

For instance, in order to get an approval for a new drug, vaccination or a treatment method, steps such as controlled and limited multi-center clinical trials with a few patients at each center ce be conducted and the data should be shared among all RIs to be analyzed. This scenario highlights the importance of existence of HD sharing and transfer between

registries and RIs which we refer to as interaction type I_6 in Figure 1 in the overview of healthcare sector. However, such a functionality is not considered in the existing literature.

Sharing and transfer of HD between registries and RIs exhibits differences compared to the functional components of healthcare systems we discussed in Section III-A. RIs can share data about new discoveries in the healthcare domain rather than personal data about patients. Hence, personal data protection rules we mentioned in Table II and other non-functional requirements we surveyed in Section III-B, such as consent management, cannot apply to this interaction type.

However, HD sharing and transfer between registries and RIs can bring about new requirements that are not considered in the state-of-the-art. For instance, compliance with national specific judicial requirements and research ethical considerations can be of high importance in the interaction between RIs. Intellectual property, confidentiality of data being shared between RIs, and the level of transparency of the healthcare research for public audience are considerations that should be further explored in this context. If RIs have confidence in a data sharing platform and a trust that their discoveries and intellectual properties are kept private and secure, they will have stronger motivation to share their discoveries in a controlled way. Additionally, in certain cases governmental controls and censorship might not allow researchers to share their discoveries freely. The first cases of COVID-19 and the interaction between HIs and RIs could be an illustration of such cases [198], [199], [200]. However, these issues could be resolved if RIs had certain privacy assurances by utilizing a blockchain-based platform.

Furthermore, data from the healthcare research (e.g., genomics) can be much more extensive in comparison to the HD in interaction types I_1-I_4. This can in fact affect the data storage models and on-chain and off-chain storage requirements. In addition, there are different types of RIs focusing on distinct areas of research (e.g., patient-related or laboratory discoveries etc.) which would affect the granularity of sharing data between these entities.

The above considerations for the interaction between registries and RIs are underdeveloped in the existing literature and hence, we are motivated to propose it as a research gap. Blockchain and SCs can help with addressing these challenges. For instance, blockchain can provide an accountable record of intellectual property for RIs or facilitate establishing a fine-grain data sharing platform without the need for a trusted third party. However, there many questions that remain open such as the choice of blockchain type that can be applicable in this scenario and the trade-off between confidentiality and transparency of data being shared.

C. Creating an Identity for Patients and Individuals

The government-issued identities are extensively used in healthcare systems of each country and jurisdiction. However, patients can travel to different locations and require healthcare services in countries other than their own. In this scenario, patients and individuals might have different passports and identities issued by various governments in each country and healthcare system. Hence, patients will be registered under different identities in multiple healthcare systems which will make it more challenging to provide a unified and holistic view of their health journal and would require a secure and controlled linkage between their identities to be established.

As of today, only government issued identities have been in use in the healthcare sector. In BBHC systems however, patients and individuals might not necessarily be registered under government-issued identities. Several contributions in the state of the art have suggested using blockchain-based self-sovereign patient identity mechanisms and decentralized identity management schemes in the healthcare sector. Such solutions are surveyed in [97] and [98].

For instance, patients and individuals can create pseudonym identities for themselves to discuss their illness and health conditions or their experience with healthcare services (or any other interactions between patients as described in interaction type I_5 in Figure 1) while remaining anonymous. Additionally, HIs and registries collect data from patients and individuals and need to aggregate the collected data from individual patients or report secondary HD to research agencies without revealing any information about patients' identity and other personal information.

Blockchain and SCs can be useful for creating decentralized identity schemes in healthcare and provide unique benefits such as non-repudiation as we described in Section IV. What remains as an open challenge in such scenarios, is how to establish a secure and controlled linkage between patients and individuals' identities in the healthcare sector. Such linkage is required in order to prevent isolated data silos effectively fragmenting patients health journal and history. Additionally, transactions associated with each patient or individual in a BBHC system might affect the state and information of several additional identities in other BBHC system.

For instance, imagine a scenario where a patient wants to provide consent for utilizing her anonymous HD about the treatment she received for an illness, for a research purpose. This patient might have received several treatments and interactions with HIs in different countries and hence in different BBHC systems. In this case, the consent that the patient will provide must also include other identities that the patient has in different BBHC systems.

The task of linking patients and individuals identities in different BBHC system is especially challenging in view of the privacy requirements. While there should be a controlled linkage between identities in BBHC systems, the linkage between identities should remain confidential to unauthorized entities since the information about linkability of different identities of patients and individuals can lead to leakage of their real identity. This challenge remains unresolved in the existing literature.

D. Interoperability Between BBHC Systems

Based on the overview of the healthcare sector, entities in the healthcare systems, and roles of each entity that we present in Section II-A, we assume that BBHC

system will be defined within the scope of countries and jurisdictions.

Registries in each country can have different scope of responsibilities, functionalities, and regulations to abide by. Hence, the setup, structure and configuration of each BBHC systems can differ per country and jurisdiction. As an example, as we demonstrated in Table II, different data protection rules and regulations take place in different regions which will in fact affect the interactions and how the HD is managed in each jurisdiction and country and hence, in each BBHC system.

As previously mentioned, there are scenarios when the same patient participates in different BBHC systems. If there is no data sharing between the two BBHC systems (e.g., due to the regulations), this scenario would require HD transfer between the systems as defined in Section II-A. However, HD transfer is also subject to regulations. For instance, Chapter 5 of GDPR (Articles 44-50), restricts transfer of HD to non-European countries if the HD pertains to European citizens and states requirements and adequate data protection guarantees in this context.

At present, as mentioned in Section III-B3, there are only few efforts that consider the interoperability between different blockchain platforms. Providing interoperability between different blockchain platforms is hard, but enabling communication of blockchain platforms with existing non-blockchain systems is even more challenging. Yet, for many applications, it is important to be able to obtain data from the outside world (i.e., off-chain).

A rapidly evolving approach to get data from the off-chain is to make use of blockchain oracles. Oracles are mechanisms that software systems provide as an external source of truth for BCs [201]. Since multiple BCs can use the same data, it promotes interoperability. The oracles can be centralized or decentralized [202]. Typically, decentralized oracles are considered more reliable, because centralized oracles constitute a single point of failure. The task of a blockchain oracle is to query data from external (i.e., off-chain) data sources and then to pass the data items to a (on-chain) SC. The evident issue here is to ensure the authenticity and integrity of the off-chain data because we have to trust the oracle [203].

To the best of our knowledge, none of the contributions in the existing literature considered interoperability between different BBHC systems and between blockchain and non-blockchain based systems. To ensure such interoperability, the first step would be to create interoperable identities for different entities in the scope of BBHC systems to provide mutual authentication as discussed earlier in detail in Section VIII-C. The other solutions such as the use of blockchain oracles should also be researched in this context. Furthermore, compliance with privacy requirements, as mentioned in Section III-B2 requires separate consideration under federated BBHC systems that comprise multiple interoperable systems. As an example, in case of public blockchains, the main issue is the visibility of the on-chain stored data and unlinkability to other transactions of patient's ID. On the other hand, in permissioned blockchain systems, controlled data sharing at fine granularity is of paramount importance.

E. Applicability of Permissionless Blockchain for BBHC Systems

We discussed in general the trade-off between permissionless and permissioned blockchain systems in Section II-B. In this section, we will consider the applicability of permissionless blockchain for BBHC systems. Although many contributions in the state-of-the-art, as listed in Table III, have proposed utilizing permissionless blockchain to develop a BBHC system, we observe some of the challenges that are yet unresolved.

In permissionless and public blockchains, all participants are able to read and update the state of the ledger. This feature can promote transparency as discussed in Section III-B2c. For instance, if we consider transparency for the interaction between registries and RIs, the public audience can be informed of the latest healthcare research trends and discoveries. Or in interactions I_1-I_4, everyone can verify the interactions within healthcare systems. However, public transparency of the content stored in blockchain comes with disadvantages and challenges of its own.

First challenge is the linkability of different HD records stored in a blockchain ledger as we discussed in Section III-B2b for interactions I_1-I_4. The same challenges apply for the interaction I_5 between patients as well. If a public blockchain is utilized to provide the functionality of HD sharing between patients, as we discussed in Section VIII-A, patients privacy requirements can be violated. Patients' interaction with each other and their associated data stored publicly on-chain could be analyzed to link different transactions together which can lead to revealing patient's true identity and their HD journal. There have been contributions in the state-of-the-art in domains other than healthcare, which aim to propose an auditable and privacy preserving public ledger (e.g., [204] in the financial and banking domain). However, it remains an open question whether public blockhain can provide similar guarantees in the scope of different BBHC systems that are potentially interconnected.

The other issue is about the content confidentiality of the data stored on-chain. We discussed the confidentiality requirement in Section III-B2a; several contributions (e.g., [71], [120], [139]) in the existing literature proposed various encryption techniques to store encrypted data on public blockchain so that only authorized users could access and decrypt the data. However, while encryption provides additional security guarantees for data, encrypted data is considered pseudonymized under GDPR. As mentioned in Recital 26 of GDPR, pseudonymized data still require proper fine-grained access control management, which is difficult to provide in permissionless blockchain. Besides, when data is stored on-chain it will remain there permanently and hence, stay exposed to long-term attacks, potentially including post-quantum methods.

Furthermore, it is not considered in the state-of-the-art how different groups of users and different roles could be defined using a public blockchain. In the scope of healthcare systems, there exist multiple entities with distinctive responsibilities and functionalities as discussed in Section II-A. Under GDPR,

these entities can also play the roles of data subjects, data controllers, and data processors such that every role has distinctive requirements. The allocation of entities to roles can be dynamic at runtime. It is not straightforward to create and maintain dynamic roles of different entities in a public blockchain. Furthermore, interoperability between different BBHC systems could add to the complexity of defining these roles.

Finally, public blockchains require adequate incentive models and computing power to maintain the integrity of the ledger. It is not considered yet in the existing literature what can be the incentive of entities in the healthcare domain to participate in the energy-consuming consensus mechanisms employed by permissionless ledgers. With lack of incentives for participants, there are no guarantees that enough non-malicious computing power will participate in the network especially since HD can be highly valuable for malicious participants.

F. Mapping of the BBHC to Individual Blockchain Systems

Healthcare systems comprise various functional components and non-functional requirements as we discussed in Section III. In Section IV, we addressed how blockchain and SCs can play a role in overcoming some of the challenges of fulfilling non-functional requirements in each functional component as proposed by the existing literature. However, providing a BBHC with the benefits of blockchain and SCs and mapping them to an individual blockchain is not straightforward. The state-of-the-art only provides preliminary ideas to this end.

To provide an example of the possible complexity of mapping BBHC functionalities while preserving non-functional requirements, we refer to the consent management platform proposed atop Hyperledger Fabric in [121]. Authors in [121] addressed the challenges of translating complex requirements of a consent management system to a new architecture of Fabric-based consortium blockchain [205]. In particular, the authors proposed several alternative ways to map the application state to the key-value world state in Fabric and analyzed the performance tradeoffs between different mappings.

In general, design of the mapping encompasses following aspects: (a) which data structured to store on-chain, off-chain, or in a hybrid solution (b) which blockchain system would be the best for storing these structures, (c) which storage mechanisms of a specific blockchain system would be most suitable (e.g., it is possible to use levelDB, CouchDB, or NoSQL databases in Fabric), and (d) what keys to use in a key-value store. None of these aspects has been sufficiently explored in the context of BBHC systems by the state-of-the-art.

G. Enabling Network and Communication Technologies

In order to implement blockchain-based solutions in real-life HSt systems, further research is required in the context of the infrastructure of healthcare systems, enabling technologies, and communication layer. Most of the HSt systems currently used by HIs employ legacy networks. Modifying these networks and the underlying technology would require further research and effort to provide the enabling network layer and communication technology to deploy real-life blockchain-based solutions in the realm of HSt systems.

Researchers should further analyze the changes that are required in the HIs' network capabilities and technologies so that they will be ready to deploy the blockchain-based solutions provided in the existing literature. In particular, the analysis should focus on the scalability of HIs' information network system in terms of storage, computation, and energy budgets. Additional questions may arise in the context of communication network technology as the enabler for the blockchain technology and SCs towards managing sensitive and private HD.

With rapid advancements of information and communication technologies, fifth generation (5G) of wireless networks has been introduced in the realm of healthcare systems [206]. Emerging 5G wireless networks and body area network (BAN) are facilitating a paradigm shift in remote patients' health monitoring [207]. With the integration of 5G networks with wearable and IoT devices in healthcare systems, device to device (D2D) communication facilitates the data exchange process between physically neighboring healthcare devices. However, D2D communication faces open challenges especially when exchanging personal and sensitive data such as HD.

Current D2D communication networks do not meet security requirements such as non-repudiation that can be used for the device and user authentication and authorization techniques [208]. More specifically, since nodes can join and leave the network in D2D communication, creating a flexible and scalable authentication mechanism is critical for D2D communication in healthcare systems. As we mention in Section III-B2b, one of the main challenges in HSt systems is the unlinkability of HD. The requirement means that the unauthorized parties should not be able to link the leaked information about a patient to any other data of the same patient stored by HIs, and should not be able to access that other data. The same requirement applies for the credentials and identity authentication of devices in D2D communication. If patients use certain devices to exchange data in D2D communication networks, the identity of the devices should not be linked to their true identity or any other associated HD and HSs. To this end, several contributions have been considered in the state-of-the-art [97], [98], [209] towards proposing self-sovereign identities for D2D communication networks.

Blockchain technology and smart contracts offer many features, such as transparency, immutability, decentralization and interoperability, as discussed in Section IV which can be utilized to deploy self-sovereign identities for D2D communication networks. There are, however, multiple challenges that need to be addressed first, such as the argument mentioned in Section VIII-C about creating digital identities for patients, which also applies to D2D communications. Another significant 5G-specific challenge for using blockchain in D2D communication is the volatile and dynamic availability of devices in the network, which requires further research on time efficiency and scalability of blockchain-based solutions

in these networks, as the number of devices increases over time.

Moreover, most of the current blockchain systems use a P2P network. P2P communication might be the most practical mechanism to use for self-organizing systems where the ledger may be updated by numerous participating nodes. However, for consortium and private blockchains, such as Hyperledger or Corda [210], there might be little need to utilize a P2P network [211] that imposes an unnecessary overhead and propagation delays. Since the propagation delays are not perceived as a bottleneck in blockchain, this questions has not received significant attention in the state-of-the-art. However, with rapid advancements in fifth and sixth generation (6G) [212] of wireless networks, novel communication technologies may increase the need for connectivity and lead to a shift in adapting 5G and 6G communication networks to guarantee low-latency, reliable connectivity and scalability. Further research is required to explore alternatives to P2P schemes in blockchain networks and DLTs, especially in the healthcare domain where the reliability and responsiveness of the communication may be of critical importance.

H. Potential Usage of SCs in BBHC Systems

It is evident from the state-of-the-art study in Section V that the integration of blockchain technologies in the healthcare domain could significantly improve the medical data management and sharing procedures in terms of a variety of aspects (e.g., trust, security, and privacy). The type and number of functionalities (e.g., access control, consent management, and data privacy methods) that will be envisioned by using the SCs along with the blockchain plays a crucial role in how secure and efficient the target integrated healthcare system will be. Coupled with the fundamental features (please refer to Figure 2) of the blockchain, the SCs could play a significant role in addressing many challenges that the current healthcare system faces concerning medical data collection, storage, and sharing across multiple stakeholders such as hospitals, research institutes, and insurance providers. Although the researchers have proposed many BBHC architectures to address various challenges in the traditional healthcare domain, the potential of the SCs has not been explored in depth. The rapid advancements in the functionalities of SCs should be fully exploited to securely and efficiently address the current healthcare data management challenges. To this end, next, we present a set of functionalities that SCs in a BBHC architecture can support to improve its security and performance.

- *Integration of multiple data sources:* SCs can retrieve data from multiple sources. Because the contracts are not reliant on any specific database, they can facilitate overcoming heterogeneity between the silos. This approach of data fusion by using SCs will provide more consistent, accurate, and useful information about a user than that provided by any individual data source. The SCs can be used to create a standard data input format, which will be used by different institutes to enter user data while interacting with the system. This will help reducing the heterogeneity in input data which will improve the system performance while performing data access operations. Moreover, with the use of blockchain oracles, hybrid SCs can be developed, where on-chain code and off-chain infrastructure are combined to support advanced dApps that react to real-world events (e.g., directly collecting and processing data generated by third party applications) and interoperating with traditional systems. Such hybrid SCs have great potential usage in the field of Medical Internet of Things (MIoT), where the data from the medical sensors could trigger specific events by directly contracting with the designated SCs executing on the blockchain system.
- *Consent management:* There are several attempts in the literature (please refer to Table III) to use SCs to enable consent management because SCs have the ability to record consent to data sharing by the patients. Furthermore, they can regulate and monitor access by third parties and report on such access to the clients, according to the GDPR regulations. However, the efficiency, scalability, and usability of the proposed SC-based consent management approaches is not evaluated with real-world scenarios. Moreover, there are no standardized procedures and guidelines to implement the consent management operations for HD management and sharing in a BBHC system. SCs could help implement fine-grained consent management policies, and they can ensure accountability by intercepting all the events that access user data, all these interceptions will be recorded in the distributed ledger which can later be checked during audits.
- *Privacy control and transparency:* SCs can manage a patient's consent and privacy control at fine granularity. They can also monitor the anonymization process for sensitive data in such a way that organizations accessing the data will not be able to detect any personal identifiers. This creates the potential of creating "quantifiable privacy" for patient data. Moreover, SCs can enable fine-grained access control over the data and operations on the data. While the data is private, the contracts can be transparent and verifiable. Such transparency leads to improved trust of the data owners in the storage infrastructure. Therefore, novel techniques that efficiently use the SC functionalities to support privacy preservation for data owners while keeping the usage of their information in the system transparent should be investigated. Furthermore, the usage of SCs in providing anonymity (i.e., unlinkability between data and its owner, and between transactions related to a single owner) to data owners, and confidentiality (i.e., protecting user data from unauthorized accesses and from unexpected failure or malicious network attacks) to transactions should be investigated.
- *Reduced bureaucracy and expenses:* Once deployed on the blockchain ledger with proper business logic, the SCs can significantly reduce the bureaucracy and expenses involved in managing the users information (i.e., HD is our case). It is because SCs have the potential to encapsulate legal prose in software without the need for a

trusted third party intermediary (such as lawyers), their utilization saves on paperwork and intermediary fees. Finally, since the SCs automate several operations on HD, it is important that these contacts are thoroughly tested for bugs and vulnerabilities [213] that could negatively impact the system performance and lead to several attacks on user data, which leads to legal complications and increase expenses due to installation of new SCs and compensations to data owners.

IX. Conclusion

In this survey, we have introduced a systematic framework for classifying and analyzing storage solutions and systems that apply the blockchain technology in the healthcare domain. The framework consists of classification in several dimensions: interactions between healthcare actors, functional components of storage systems, challenges in the healthcare domain that can be overcome by using the blockchain technology, and benefits of applying the blockchain technology derived from its fundamental properties.

Using this framework, we have analyzed over 40 systems and solutions for storage in the healthcare domain. Following the results of the analysis, we have outlined a number of important research gaps and future directions yet to be addressed.

Acknowledgment

The authors are grateful to Arlindo Flavio Da Conceicão, Thiago Garrett, and Andrea Merlina for their helpful suggestions that have contributed towards improving the presentation. The authors would also like to thank the anonymous reviewers and the associate editor for their valuable comments and feedback.

References

[1] S. Kumar and M. Singh, "Big data analytics for healthcare industry: Impact, applications, and tools," *Big Data Min. Anal.*, vol. 2, no. 1, pp. 48–57, Mar. 2019.

[2] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in *Proc. IEEE Int. Congr. Big Data*, 2014, pp. 762–765.

[3] Y. Yu, M. Li, L. Liu, Y. Li, and J. Wang, "Clinical big data and deep learning: Applications, challenges, and future outlooks," *Big Data Min. Anal.*, vol. 2, no. 4, pp. 288–305, Dec. 2019.

[4] V. Casola, A. Castiglione, K.-K. R. Choo, and C. Esposito, "Healthcare-related data in the cloud: Challenges and opportunities," *IEEE Cloud Comput.*, vol. 3, no. 6, pp. 10–14, Nov./Dec. 2016.

[5] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues," *IEEE Access*, vol. 6, pp. 17246–17263, 2018.

[6] A. R. Iossifova and S. Meyer-Goldstein, "Impact of standards adoption on healthcare transaction performance: The case of HIPAA," *Int. J. Prod. Econ.*, vol. 141, no. 1, pp. 277–285, 2013.

[7] D. A. Tamburri, "Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation," *Inf. Syst.*, vol. 91, Jul. 2020, Art. no. 101469.

[8] X. Larrucea, M. Moffie, S. Asaf, and I. Santamaria, "Towards a GDPR compliant way to secure European cross border healthcare industry 4.0," *Comput. Stand. Interfaces*, vol. 69, Mar. 2020, Art. no. 103408.

[9] S. Bhartiya, D. Mehrotra, and A. Girdhar, "Issues in achieving complete interoperability while sharing electronic health records," *Procedia Comput. Sci.*, vol. 78, pp. 192–198, Dec. 2016.

[10] O. Nee et al., "SAPHIRE: Intelligent healthcare monitoring based on semantic interoperability platform: Pilot applications," *IET Commun.*, vol. 2, no. 2, pp. 192–201, 2008.

[11] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[12] X. Yuan, X. Wang, C. Wang, J. Weng, and K. Ren, "Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing," *IEEE Trans. Multimedia*, vol. 18, no. 10, pp. 2002–2014, Oct. 2016.

[13] A. S. Shahraki, C. Rudolph, and M. Grobler, "A dynamic access control policy model for sharing of healthcare data in multiple domains," in *Proc. 18th IEEE Int. Conf. Trust, Security Privacy Comput. Commun. 13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, 2019, pp. 618–625.

[14] C. Xu, N. Wang, L. Zhu, K. Sharif, and C. Zhang, "Achieving searchable and privacy-preserving data sharing for cloud-assisted E-healthcare system," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8345–8356, Oct. 2019.

[15] Y. Yang et al., "Medshare: A novel hybrid cloud for medical resource sharing among autonomous healthcare providers," *IEEE Access*, vol. 6, pp. 46949–46961, 2018.

[16] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[17] M. R. Asghar, T. Lee, M. M. Baig, E. Ullah, G. Russello, and G. Dobbie, "A review of privacy and consent management in healthcare: A focus on emerging data sources," in *Proc. IEEE 13th Int. Conf. e-Sci.*, 2017, pp. 518–522.

[18] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.

[19] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[20] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[21] S. Nakamoto. "A peer-to-peer electronic cash system." Bitcoin. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[22] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[23] J. D. Vyas, M. Han, L. Li, S. Pouriyeh, and J. S. He, "Integrating blockchain technology into healthcare," in *Proc. ACM Southeast Conf.*, 2020, pp. 197–203.

[24] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, "ssHealth: Toward secure, blockchain-enabled healthcare systems," *IEEE Netw.*, vol. 34, no. 4, pp. 312–319, Jul./Aug. 2020.

[25] H. L. Pham, T. H. Tran, and Y. Nakashima, "A secure remote healthcare system for hospital using blockchain smart contract," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–6.

[26] E. Zaghloul, T. Li, and J. Ren, "Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, 2019, pp. 375–379.

[27] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[28] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis, and V. V. G. Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 1835–1852, Oct.–Dec. 2021.

[29] H. M. Hussien, S. M. Yasin, S. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *J. Med. Syst.*, vol. 43, no. 10, p. 320, 2019.

[30] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for Healthcare," *ACM Comput. Surveys*, vol. 53, no. 2, pp. 1–27, 2020.

[31] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, Jun. 2018.

[32] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.

[33] "General data protection regulation GDPR." European Commission. Accessed: Mar. 10, 2021. [Online]. Available: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

[34] "The health insurance portability and accountability act of 1996 (HIPAA)." Centers for Medicare & Medicaid Services. 1996. [Online]. Available: http://www.cms.hhs.gov/hipaa/

[35] K.-D. Henke and J. Schreyögg, "Towards sustainable health care systems: Strategies in health insurance schemes in France, Germany, Japan and the netherlands; a comparative study," Diskussionspapier, Technische Universität, Berlin, Germany, Rep. 2004/9, 2004.

[36] C. Schoen, R. Osborn, D. Squires, and M. M. Doty, "Access, affordability, and insurance complexity are often worse in the united states compared to ten other countries," *Health Affairs*, vol. 32, no. 12, pp. 2205–2215, 2013.

[37] L. L. Hagenaars, N. S. Klazinga, M. Mueller, D. J. Morgan, and P. P. Jeurissen, "How and why do countries differ in their governance and financing-related administrative expenditure in health care? An analysis of OECD countries by health care system typology," *Int. J. Health Planning Manage.*, vol. 33, no. 1, pp. e263–e278, 2018.

[38] R. E. Gliklich, N. A. Dreyer, M. B. Leavy, and J. Christian, *Registries for Evaluating Patient Outcomes: A User's Guide*. Washington, DC, USA: Govern. Print., 2014.

[39] E. Pukkala et al., "Nordic cancer registries—An overview of their procedures and data comparability," *Acta Oncologica*, vol. 57, no. 4, pp. 440–455, 2018.

[40] "Health registries." Norwegian Institute of Public Health. Accessed: Mar. 10, 2021. [Online]. Available: https://www.fhi.no/en/hn/health-registries/

[41] "U.S. Department of Health & Human Services National Institute of Health (NIH), List of Registries." 2022. [Online]. Available: https://www.nih.gov/health-information/nih-clinical-research-trials-you/list-registries

[42] J. L. Cronenwett, "Registries, research, and quality improvement," *Eur. J. Vasc. Endovasc. Surg.*, vol. 59, no. 4, pp. 503–509, 2020.

[43] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *Int. J. Med. Inform.*, vol. 134, Feb. 2020, Art. no. 104040.

[44] H. Burde, "The HITECH act: An overview," *AMA J. Ethics*, vol. 13, no. 3, pp. 172–175, 2011.

[45] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[46] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5416–5441, Apr. 2021.

[47] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[48] A. Merlina, R. Vitenberg, and V. Setty, "A general and configurable framework for blockchain-based marketplaces," in *Proc. 37th ACM/SIGAPP Symp. Appl. Comput.*, 2022, pp. 216–225.

[49] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3796–3838, 4th Quart., 2019.

[50] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep./Oct. 2019.

[51] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surveys*, vol. 52, no. 3, pp. 1–34, 2019.

[52] M. Saad et al., "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020.

[53] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[54] M. H. Tabatabaei, R. Vitenberg, and N. R. Veeraragavan, "Understanding blockchain: Definitions, architecture, design, and system comparison," 2022, *arXiv:2207.02264*.

[55] "Professional hack on norwegian health authority compromises data of three million patients." Accessed: Mar. 21, 2021. [Online]. Available: https://www.theinquirer.net/inquirer/news/3024692/norway-health-south-east-rhf-hacked

[56] "UCLA health system data breach affects 4.5 million patients." 2015. [Online]. Available: https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html

[57] "Massive breach at health care Company Anthem, Inc." 2015. [Online]. Available: https://eu.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/

[58] D. Evans, "MyFitnessPal," *Brit. J. Sports Med.*, vol. 51, no. 14, pp. 1101–1102, 2017.

[59] A. Zhang, A. Bacchus, and X. Lin, "Consent-based access control for secure and privacy-preserving health information exchange," *Security Commun. Netw.*, vol. 9, no. 16, pp. 3496–3508, 2016.

[60] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[61] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability challenges in healthcare blockchain system—A systematic review," *IEEE Access*, vol. 8, pp. 23663–23673, 2020.

[62] F. Girardi, G. De Gennaro, L. Colizzi, and N. Convertini, "Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain," *Electronics*, vol. 9, no. 6, p. 884, 2020.

[63] C. Dinh-Le, R. Chuang, S. Chokshi, and D. Mann, "Wearable health technology and electronic health record integration: Scoping review and future directions," *JMIR mHealth uHealth*, vol. 7, no. 9, 2019, Art. no. e12861.

[64] "Health care data 101." Dashconnect. 2018. [Online]. Available: http://dashconnect.org/wp-content/uploads/2018/03/Health-Care-Data-101.pdf

[65] A. Shah, V. Banakar, S. Shastri, M. Wasserman, and V. Chidambaram, "Analyzing the impact of GDPR on storage systems," in *Proc. 11th USENIX Workshop Hot Topics Storage File Syst. (HotStorage)*, 2019, p. 4.

[66] E. A. Bell, L. Ohno-Machado, and M. A. Grando, "Sharing my health data: A survey of data sharing preferences of healthy individuals," in *Proc. AMIA Annu. Symp.*, 2014, p. 1699.

[67] "January 2020 healthcare data breach report." Hipaajournal. [Online]. Available: https://www.hipaajournal.com/january-2020-healthcare-data-breach-report/

[68] A. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," 2020, *arXiv:2005.07359*.

[69] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[70] "Extensible access control markup language (XACML)—Organization for the advancement of structured information standards." 2013. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[71] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[72] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in *Proc. 31st Int. Conf. Distrib. Comput. Syst.*, 2011, pp. 373–382.

[73] J. Hash, P. Bowen, A. Johnson, C. Smith, and D. Steinberg, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (Hipaa) Security Rule*, U.S. Dept. Commerce, Technol. Admin., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2005.

[74] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth cloud security challenges: A survey," *J. Healthcare Eng.*, vol. 2019, Sep. 2019, Art. no. 7516035.

[75] L. Axon, "Privacy-awareness in blockchain-based PKI," Working Paper, Oxford Univ. Res. Archive, Oxford, U.K., 2015.

[76] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *Proc. IFIP Int. Conf. Auton. Infrastruct., Manage. Security*, 2017, pp. 16–29.

[77] E. Nygren, R. K. Sitaraman, and J. Sun, "The akamai network: A platform for high-performance Internet applications," *ACM SIGOPS Oper. Syst. Rev.*, vol. 44, no. 3, pp. 2–19, 2010.

[78] *CloudFlare Advanced DDoS Protection*, Cloudflare, San Francisco, CA, USA, 2014.

[79] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, "Measuring the adoption of DDoS protection services," in *Proc. Internet Meas. Conf.*, 2016, pp. 279–285.

[80] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surveys*, vol. 39, no. 1, p. 3, 2007.

[81] S. Hasavari and Y. T. Song, "A secure and scalable data source for emergency medical care using blockchain technology," in *Proc. IEEE 17th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, 2019, pp. 71–75.

[82] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[83] P. Voigt and A. Von dem Bussche, "The EU general data protection regulation (GDPR)," in *A Practical Guide*, vol. 10, 1st ed. Cham, Switzerland: Springer Int., 2017.

[84] J. Lederman, B. D. Taylor, and M. Garrett, "A private matter: The implications of privacy regulations for intelligent transportation systems," *Transp. Plan. Technol.*, vol. 39, no. 2, pp. 115–135, 2016.

[85] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y.-A. de Montjoye, and A. Bourka, "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics," 2015, *arXiv:1512.06000*.

[86] C. J. Bennett, *Implementing Privacy Codes of Practice (Plus 8830)*, Canadian Stand. Assoc., Toronto, ON, Canada, 1995.

[87] D. Butin and D. Le Métayer, "A guide to end-to-end privacy accountability," in *Proc. IEEE/ACM 1st Int. Workshop Tech. Legal Aspects Data Privacy Security*, 2015, pp. 20–25.

[88] D. Gonçalves-Ferreira et al., "OpenEHR and general data protection regulation: Evaluation of principles and requirements," *JMIR Med. Inform.*, vol. 7, no. 1, 2019, Art. no. e9845.

[89] M. M. H. Onik, S. Aich, J. Yang, C.-S. Kim, and H.-C. Kim, "Blockchain in healthcare: Challenges and solutions," in *Big Data Analytics for Intelligent Healthcare Management*. London, U.K.: Elsevier, 2019, pp. 197–226.

[90] J. Kaye, E. A. Whitley, D. Lund, M. Morrison, H. J. A. Teare, and K. Melham, "Dynamic consent: A patient interface for twenty-first century research networks," in *Eur. J. Human Genet.*, vol. 23, no. 2, pp. 141–146, 2015.

[91] D. Calvaresi, D. Cesarini, P. Sernani, M. Marinoni, A. F. Dragoni, and A. Sturm, "Exploring the ambient assisted living domain: A systematic review," *J. Ambient Intell. Humanized Comput.*, vol. 8, pp. 239–257, Apr. 2017.

[92] H. Atasoy, B. N. Greenwood, and J. S. McCullough, "The digitization of patient care: A review of the effects of electronic health records on health care quality and utilization," *Annu. Rev. Public Health*, vol. 40, pp. 487–500, Apr. 2019.

[93] C. Compert, M. Luinetti, and B. Portier, "Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance," IBM Security, Armonk, NY, USA, White Paper, 2018.

[94] D. Calvaresi, J.-P. Calbimonte, A. Dubovitskaya, V. Mattioli, J.-G. Piguet, and M. Schumacher, "The good, the bad, and the ethical implications of bridging blockchain and multi-agent systems," *Information*, vol. 10, no. 12, p. 363, 2019.

[95] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[96] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2543–2585, 3rd Quart., 2018.

[97] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020.

[98] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: State of the art and future perspective," *Sensors*, vol. 20, no. 2, p. 483, 2020.

[99] T. McConaghy et al., "BigchainDB: A scalable blockchain database," BigChainDB, Berlin, Germany, White Paper, 2016.

[100] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, 2018, pp. 45–54.

[101] I. Weber et al., "On availability for blockchain-based systems," in *Proc. IEEE 36th Symp. Rel. Distrib. Syst. (SRDS)*, 2017, pp. 64–73.

[102] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Security*, 2015, pp. 112–125.

[103] J. K. Penberthy and D. R. Penberthy, "The physician's dilemma: Healthcare and bureaucracy in the modern world," in *Groupthink in Science*. Cham, Switzerland: Springer, 2020, pp. 251–262.

[104] I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," *Appl. Health Econ. Health Policy*, vol. 16, no. 5, pp. 583–590, 2018.

[105] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the design of a blockchain-based system to facilitate healthcare data sharing," in *Proc. 17th IEEE Int. Conf. Trust, Security Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, 2018, pp. 1374–1379.

[106] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–18, 2018.

[107] T. Giannetsos, T. Dimitriou, and N. R. Prasad, "People-centric sensing in assistive healthcare: Privacy challenges and directions," *Security Commun. Netw.*, vol. 4, no. 11, pp. 1295–1307, 2011.

[108] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Comput. Surveys*, vol. 45, no. 1, pp. 1–54, 2012.

[109] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, pp. 1–44, 2021.

[110] J. Sandgaard and S. Wishstar. "MedChain white paper v1.0." 2018. [Online]. Available: https://www.medchain.us/doc/Medcha%20Whitepap%20v1.0.pdf

[111] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, 2016, pp. 25–30.

[112] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2018, pp. 1–9.

[113] X. Zhang, S. Poslad, and Z. Ma, "Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–7.

[114] X. Zhang and S. Poslad, "Blockchain support for flexible queries with granular access control to electronic medical records (EMR)," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2018, pp. 1–6.

[115] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, 2018, pp. 1–6.

[116] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–6.

[117] Y. Cheng, J. Ren, Z. Wang, S. Mei, and J. Zhou, "Attributes union in CP-ABE algorithm for large universe cryptographic access control," in *Proc. 2nd Int. Conf. Cloud Green Comput.*, 2012, pp. 180–186.

[118] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, pp. 1–7, Jun. 2018.

[119] G. Albanese, J.-P. Calbimonte, M. Schumacher, and D. Calvaresi, "Dynamic consent management for clinical trials via private blockchain technology," *J. Ambient Intell. Humanized Comput.*, vol. 11, pp. 4909–4926, Feb. 2020.

[120] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *J. Ambient Intell. Humanized Comput.*, vol. 11, pp. 4613–4641, Jan. 2020.

[121] R. R. Agarwal, D. Kumar, L. Golab, and S. Keshav, "Consentio: Managing consent to data access using permissioned blockchains," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[122] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, 2018, pp. 699–706.

[123] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1242–1255, Apr.–Jun. 2021.

[124] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 136, 2018.

[125] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and efficient data accessibility in blockchain based healthcare systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 206–212.

[126] Z. Xiao et al., "EMRShare: A cross-organizational medical data sharing and management framework using permissioned blockchain," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, 2018, pp. 998–1003.

[127] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Jan. 2018.

[128] B. Toshniwal, P. Podili, R. J. Reddy, and K. Kataoka, "PACEX: PAtient-centric EMR eXchange in Healthcare systems using blockchain," in *Proc. IEEE 10th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, 2019, pp. 954–960.

[129] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020.

[130] M. Y. Jabarulla and H.-N. Lee, "Blockchain-based distributed patient-centric image management system," 2020, *arXiv:2003.08054*.

[131] "Ipfs." 2022. [Online]. Available: https://ipfs.io/

[132] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[133] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data," in *Proc. Norwegian Inf. Secur. Conf.*, Oslo, Norway, 2017, pp. 100–111.

[134] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-Health data access management with privacy protection," in *Proc. IEEE 24th Int. Workshop Comput.-Aided Model. Design Commun. Links Netw. (CAMAD)*, 2019, pp. 1–7.

[135] M. Hanley and H. Tewari, "Managing lifetime healthcare data on the blockchain," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, pp. 246–251.

[136] T. Rupasinghe, F. Burstein, and C. Rudolph, "Blockchain based dynamic patient consent: A privacy-preserving data acquisition architecture for clinical data analytics," in *Proc. ICIS*, 2019, pp. 1–9.

[137] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system," *IEEE Access*, vol. 7, pp. 88012–88025, 2019.

[138] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, 2017, pp. 1–5.

[139] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.

[140] A. Dubovitskaya et al., "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, 2020, Art. no. e13598.

[141] J. Xu et al., "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[142] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, "MediChain TM: A secure decentralized medical data asset management system," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Physical Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1533–1538.

[143] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *J. Med. Syst.*, vol. 43, no. 2, p. 26, 2019.

[144] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[145] K. M. Hossein, M. E. Esmaeili, T. Dargahi, and A. Khonsari, "Blockchain-based privacy-preserving healthcare architecture," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, 2019, pp. 1–4.

[146] M. S. Rahman, I. Khalil, P. C. M. Arachchige, A. Bouras, and X. Yi, "A novel architecture for tamper proof electronic health record management system using blockchain wrapper," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, 2019, pp. 97–105.

[147] A. Bayle, M. Koscina, D. Manset, and O. Perez-Kempner, "When blockchain meets the right to be forgotten: Technology versus law in the healthcare industry," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, 2018, pp. 788–792.

[148] M. T. de Oliveira et al., "Towards a blockchain-based secure electronic medical record for healthcare applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–6.

[149] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y.-C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," in *Proc. 18th IEEE Int. Conf. Trust, Security Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, 2019, pp. 594–601.

[150] Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, "Blockchain-based multi-role Healthcare data sharing system," in *Proc. IEEE Int. Conf. E-Health Netw., Appl. Services (HEALTHCOM)*, 2021, pp. 1–6.

[151] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, "Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT," in *Proc. IEEE Global Commun. Conf.*, 2020, pp. 1–6.

[152] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A Decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021.

[153] J. Vora et al., "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–6.

[154] M. Koscina, D. Manset, C. Negri, and O. Perez, "Enabling trust in healthcare data exchange with a federated blockchain-based architecture," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Compan. Vol.*, 2019, pp. 231–237.

[155] H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, *Blockchain and Clinical Trial: Securing Patient Data*. Cham, Switzerland: Springer, 2019.

[156] "Gem." [Online]. Available: https://gem.co/

[157] C. Wood, B. Winton, K. Carter, S. Benkert, L. Dodd, and J. Bradley, "How blockchain technology can enhance EHR operability," ARK Invest, New York, NY, USA, White Paper, 2016.

[158] "Guardtime." Accessed: Jun. 15, 2021. [Online]. Available: https://www.guardtime.co/

[159] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, 2016, pp. 1–3.

[160] "Burstiq." 2022. [Online]. Available: https://www.burstiq.com/

[161] "Medicalchain." 2022. [Online]. Available: https://medicalchain.com/en/

[162] "Pokitdoc." Accessed: Sep. 15, 2021. [Online]. Available: https://www.pokitdok.com/

[163] "Cortex network." Accessed: Sep. 15, 2021. [Online]. Available: https://www.crtx.app

[164] J. Robinson and L. Kish. "Cortex white paper." 2016. [Online]. Available: https://www.crtx.app/crtx.whitepaper.pdf

[165] "Modum." 2022. [Online]. Available: https://modum.io/

[166] "Isolve." 2022. [Online]. Available: https://isolve.io/

[167] A. Albeyatti. "Medicalchain." 2018. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[168] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[169] N. Deepa et al., "A survey on blockchain for big data: Approaches, opportunities, and future directions," 2020, *arXiv:2009.00858*.

[170] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Banking Financ. Technol.*, vol. 3, no. 1, pp. 1–17, 2019.

[171] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2521–2549, 4th Quart., 2020.

[172] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[173] R. El-Gazzar and K. Stendal, "Blockchain in health care: Hope or hype?" *J. Med. Internet Res.*, vol. 22, no. 7, 2020, Art. no. e17199.

[174] T. Abdullah and A. Jones, "eHealth: Challenges far integrating blockchain within healthcare," in *Proc. IEEE 12th Int. Conf. Global Security, Safety Sustainability (ICGS3)*, 2019, pp. 1–9.

[175] J. Yang, H. Bi, Z. Liang, H. Zhou, and H. Yang, "A survey on blockchain: Architecture, applications, challenges, and future trends," in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData) IEEE Congr. Cybermatics (Cybermatics)*, 2020, pp. 749–754.

[176] S. Megha et al., "Survey on blockchain applications for Healthcare: Reflections and challenges," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.*, 2021, pp. 310–322.
[177] T. Hardin and D. Kotz, "Blockchain in health data systems: A survey," in *Proc. 6th Int. Conf. Internet Things Syst., Manage. Security (IOTSMS)*, 2019, pp. 490–497.
[178] D. Kumari, B. Rajita, and S. Panda, "Blockchain: A survey on healthcare perspective and its challenges," in *Proc. Int. Conf. Inf. Commun. Technol. Intell. Syst.*, 2020, pp. 111–119.
[179] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and smart healthcare security: A survey," *Procedia Comput. Sci.*, vol. 175, pp. 615–620, Jan. 2020.
[180] K. Wilber, S. Vayansky, N. Costello, D. Berdik, and Y. Jararweh, "A survey on blockchain for healthcare informatics and applications," in *Proc. 7th Int. Conf. Internet Things Syst., Manage. Security (IOTSMS)*, 2020, pp. 1–9.
[181] E. N. Arnesen and B. A. Larsen, "Kritisk informasjon i kjernejournal," *Tidsskrift Den norske legeforening*, vol. 134, no. 20, pp. 1927–1928, 2014. [Online]. Available: https://doi.org/10.4045/tidsskr.14.1085
[182] "National health service (NHS) digital, summary care records (SCR)." 2022. [Online]. Available: https://digital.nhs.uk/services/summary-care-records-scr
[183] "Australian digital health agency, my health record, your health information securely in one place." Accessed: Nov. 10, 2021. [Online]. Available: https://www.myhealthrecord.gov.au
[184] D. P. J. Woudstra, "Towards a national implementation of the electronic locum record: Analysis of a regional approach in the Netherlands," in *Proc. 3rd IBA Bachelor Thesis Conf.*, 2014, pp. 1–14.
[185] "Health information and quality authority, international review of national summary care records." Accessed: Nov. 10, 2021. [Online]. Available: https://www.hiqa.ie/sites/default/files/2017-02/International-Review-Summary-Care-Records.pdf
[186] "The Norwegian summary care record." Accessed: Nov. 10, 2021. [Online]. Available: https://www.nhn.no/nasjonale-e-helselosninger/kjernejournal/hva-er-kjernejournal/_/attachment/download/101a522b-8031-4223-a4eb-0d959ab6c18f:eb2d84c6eb914d5f10e1262ef67cb8735f22b1fc/the-norwegian-summary-care-record.pdf
[187] "What is a summary care record?" 2021. [Online]. Available: https://www.helsenorge.no/en/summary-care-record/kjernejournal-for-safer-healthcare/
[188] "Helsenorge: Public healthcare website for residents of Norway." Accessed: Nov. 10, 2021. [Online]. Available: https://www.helsenorge.no
[189] K. Dyb and L. L. Warth, "The norwegian national summary care record: A qualitative analysis of doctors' use of and trust in shared patient information," *BMC Health Services Res.*, vol. 18, no. 1, pp. 1–10, 2018.
[190] P. T. Pons, J. S. Haukoos, W. Bludworth, T. Cribley, K. A. Pons, and V. J. Markovchick, "Paramedic response time: Does it affect patient survival?" *Acad. Emerg. Med.*, vol. 12, no. 7, pp. 594–600, 2005.
[191] "Norwegian board of health, 2017 annual report." 2017. [Online]. Available: https://www.helsetilsynet.no/globalassets/opplastinger/Publikasjoner/tilsynsmelding/tilsynsmelding2017.pdf/
[192] "Lov om helsepersonell mv (helsepersonelloven)." Helse-og omsorgsdepartementet. 1999. [Online]. Available: https://lovdata.no/dokument/NL/lov/1999-07-02-64
[193] "Sykepleien, healthcare professionals snoop in medical records (original: Helsepersonell snoker i journaler)." 2018. [Online]. Available: https://sykepleien.no/2018/03/helsepersonell-snoker-i-journaler
[194] "Nrk, two health workers have confessed to having snooped illegally in patient records (original: To helsetilsette har tilstått å ha snoka ulovleg i pasientjournal)." 2022. [Online]. Available: https://www.nrk.no/vestland/pasient-melde-fra-om-snoking-1.8183704
[195] "Employee caught snooping on patient records (original: Ansatt tatt for snoking i pasientjournaler: Dette er svært alvorlig)." Tv2. Accessed: Nov. 10, 2021. [Online]. Available: https://www.tv2.no/a/11197624/
[196] S. P. Ahuja, S. Mani, and J. Zambrano, "A survey of the state of cloud computing in healthcare," *Netw. Commun. Technol.*, vol. 1, no. 2, p. 12, 2012.
[197] L. O. Gostin, L. A. Levit, and S. J. Nass, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, Nat. Acad. Press, Washington, DC, USA, 2009.
[198] V. Abazi, "Truth distancing? Whistleblowing as remedy to censorship during COVID-19," *Eur. J. Risk Regulation*, vol. 11, no. 2, pp. 375–381, 2020.
[199] G. Karabulut, K. F. Zimmermann, M. H. Bilgin, and A. C. Doker, "Democracy and COVID-19 outcomes," *Econ. Lett.*, vol. 203, Jun. 2021, Art. no. 109840.
[200] R. Armitage, "Online 'anti-vax' campaigns and COVID-19: Censorship is not the solution," *Public Health*, vol. 190, p. e29, Jan. 2021.
[201] R. Mühlberger et al., "Foundational oracle patterns: Connecting blockchain to the off-chain world," in *Proc. Int. Conf. Bus. Process Manage.*, 2020, pp. 35–51.
[202] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, "Astraea: A decentralized blockchain oracle," in *Proc. IEEE Int. Conf. Internet Things (IThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Physical Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1145–1152.
[203] J. Heiss, J. Eberhardt, and S. Tai, "From oracles to trustworthy data on-chaining systems," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, 2019, pp. 496–503.
[204] N. Narula, W. Vasquez, and M. Virza, "ZKledger: Privacy-preserving auditing for distributed ledgers," in *Proc. 15th USENIX Symp. Netw. Syst. Design Implement.*, 2018, pp. 65–80.
[205] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "FastFabric: Scaling hyperledger fabric to 20 000 transactions per second," *Int. J. Netw. Manage.*, vol. 30, no. 5, p. e2099, 2020.
[206] S. Latif, J. Qadir, S. Farooq, and M. A. Imran, "How 5G wireless (and concomitant technologies) will revolutionize healthcare?" *Future Internet*, vol. 9, no. 4, p. 93, 2017.
[207] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.
[208] M. H. Adnan and Z. A. Zukarnain, "Device-to-device communication in 5G environment: Issues, solutions, and challenges," *Symmetry*, vol. 12, no. 11, p. 1762, 2020.
[209] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115876–115904, 2020.
[210] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," R3 CEV, New York, NY, USA, White Paper, Aug. 2016.
[211] R. Vitenberg, "Debunking blockchain myths," in *Proc. 11th Norwegian Inf. Secur. Conf.*, 2018.
[212] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.
[213] M. Di Angelo and G. Salzer, "A survey of tools for analyzing Ethereum smart contracts," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, 2019, pp. 69–78.
[214] K. Zhang, R. Vitenberg, and H.-A. Jacobsen, "Deconstructing blockchains: Concepts, systems, and insights," in *Proc. 12th ACM Int. Conf. Distrib. Event-based Syst. (DEBS)*, 2018, pp. 187–190.

Mohammad Salar Arbabi received the B.S. degree in information technology engineering from the Sharif University of Technology, Tehran, Iran, in 2016, the M.S. degree in information technology engineering with specialization in electronic commerce from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, in 2019. He is currently pursuing the Ph.D. degree with the University of Oslo, Oslo, Norway, where he is a member of Blockchain Lab. His research focuses on distributed systems, blockchain technology, smart contracts, and applications of mentioned domains in healthcare systems.

Chhagan Lal received the Ph.D. degree in computer science and engineering from the Malaviya National Institute of Technology, Jaipur, India, in 2015. During his Ph.D., he has been awarded with the Canadian Commonwealth Scholarship under the Canadian Commonwealth Scholarship Program to work in University of Saskatchewan, Saskatoon, SK, Canada. He is currently working as a Senior Researcher with the Department of Intelligent Systems, Cybersecurity Group, TU Delft, Netherlands. Previously, he was a Postdoctoral Research Fellow with Simula Research Laboratory, Norway. Before Simula, he was a Postdoctoral Fellow with Department of Mathematics, University of Padua, Italy, where he was part of the SPRITZ Research Group. His current research areas include applications of blockchain technologies and smart contracts, network security, software-defined networking, and securing Internet of Things networks.

Narasimha Raghavan Veeraragavan is currently a Special Adviser with the Cancer Registry of Norway. He is a key player in delivering technical architecture and innovative solutions to continuously strengthen the security and privacy of cancer patients' datasets in Norway. Additionally, as part of his role, he is involved in several national and international research projects and collaborates with many reputed national and international partners. Before, he led several technical initiatives in global companies. He has four patents and a few peer-reviewed research papers in reputed conferences and journals. His initiatives resulted in large-scale software products launched globally with millions of users worldwide. His research interests lie in data privacy, secure computing, machine learning, and decentralized systems.

Dusica Marijan is a Senior Research Scientist with the Department of Validation Intelligence for Autonomous Software Systems, Simula Research Laboratory, Oslo, Norway. Prior to Simula, she worked as a Senior Software Engineer in the consumer electronics industry. She has coauthored over 50 referred articles in the software engineering and artificial intelligence communities, and developed several software tools for testing critical software systems. Her research interests lie at the intersection of software engineering and machine learning for improving the trustworthiness (e.g., security, privacy, and robustness) of complex software systems.

Jan F. Nygård received the engineering degree in cybernetics from the Oslo College of Engineering, a minor in political science, and the Ph.D. degree in epidemiology from the University of Oslo in 1991, 1998, and 2005, respectively. He worked with the Institute of Community Medicine, University of Oslo from 1992 to 1998. He has been with the Cancer Registry of Norway since 1999, the Head of the IT/Registry Informatics Department since 2007, and an Adjunct Associate Professor with the Machine Learning Group, Department of Physics and Technology, UiT The Arctic University of Norway since 1 July 2021. From July to December 2017, he was a Visiting Scientist with the Institute for Applied Scientific Computing, Lawrence Livermore National Laboratory. He has published 80 original research papers in peer-reviewed journals, and supervised M.Sc. and Ph.D. students from informatics and medical faculties. His research interest lies in the cross-section between big data analytics/machine learning, data privacy, secure computing, and epidemiology. He serves on several reference and steering committees.

Roman Vitenberg (Member, IEEE) is a Professor with the Department of Informatics, University of Oslo, where he is heading the Blockchain Lab. He has over 80 publications in peer-reviewed venues and five filed patents. His research interests lie broadly in the area of distributed applications, middleware and algorithms, including specification, design, analysis, implementation, performance evaluation, and software engineering. In particular, he has been working on large-scale communication, privacy and security, data storage, distributed event-based systems, fault-tolerant distributed computing, and more recently, blockchain. He is an Associate Editor for the EAI Transactions on Cloud Computing and a Steering Committee Member for ACM/IFIP/USENIX Middleware. His papers were presented Best Paper Awards at ACM/IFIP/USENIX Middleware, ACM SAC, and ACM DEBS conferences.