Improving security and efficiency in IoT data management using BC based solutions

Ruben Couwenberg

Supervisor(s): Mauro Conti, Chhagan Lal

EEMCS, Delft University of Technology, The Netherlands

A Thesis Submitted to EEMCS Faculty Delft University of Technology,
In Partial Fulfilment of the Requirements
For the Bachelor of Computer Science and Engineering
January 29, 2023

Name of the student: Ruben Couwenberg
Final project course: CSE3000 Research Project
Thesis committee: Mauro Conti, Chhagan Lal , Jorge Martinez

Abstract

The Internet of Things (IoT) consists out of billions of devices. This vast size magnifies the security and efficiency challenges the IoT faces. Blockchain (BC) features like decentralisation, immutability and smart contracts can negate these IoT challenges. In this paper we discuss how BC based solutions can significantly increase the security and efficiency of data management in IoT networks.

To this end we provide reviews of existing related surveys that focus on the privacy and performance of BC solutions in IoT. State-of-the-art research papers on this topic are reviewed and discussed. We create summaries that categorize and compare all reviews in this paper. These comparisons include consensus algorithms, performance, security, privacy, pros and cons. Finally, we discuss the reviewed papers and present potential future research directions that we found in this field based on the discussed research papers and surveys.

***Index terms*—Blockchain, Internet of Things, consensus, performance, security, privacy**

1 Introduction

As the Internet of Things (IoT) domain grows larger every day, the amount of data used by the IoT scales in conjunction with this IoT expanse. The IoT is a network that consists of billions of physical objects. Juniper Research projects the IoT to contain 50 billion connected devices in 2023 [1]. This rapid exponential growth simultaneously makes the efficiency and security of IoT data management more important. The existing threats the IoT faces are broad and can be complicated to create countermeasures for.

The blockchain (BC) is an adequate candidate to make IoT data management more secure and efficient while also being applicable to plenty of IoT networks [2]. Recent papers have shed light on the threats that the IoT networks face and proposed corresponding countermeasures using BC while also highlighting the existing research gaps [3], [4].

The gap that this research will fill is to provide a review of the research direction on using BC-based solutions to improve the IoT data management process in different IoT applications. The cornerstones of these improvements that the state-of-the-art BC approaches provide for IoT data management are security, privacy and performance. The main question this paper will answer is how we can improve security and efficiency in IoT data management using BC-based solutions.
This main question will be subdivided into the following subquestions:

- How does BC improve IoT data management?
- What are the pros and cons of using BC to improve IoT data management?
- What solutions exist to negate the cons of using BC to improve IoT data management?

The following sections will be divided as follows. Section 2 will discuss the relevant background and related work used to answer the research question while also going over related work. Section 3 will contain the survey of related work. In section 4 the proposed study will discuss state-of-the-art research papers and will, together with the previous section, partially answer the first and second sub-question. Section 5 will discuss the evaluation metrics used in categorizing the surveys and research papers. Section 6 will feature the discussion together with an investigation of the sub-questions and recommendations for future works. In section 7 the ethical aspects of the research will be discussed together with the thoughts that went into making the research responsible and reproducible. Finally, section 8 will discuss the conclusions of this paper.

2 Background

Additional background on BC and IoT will be provided in the following subsections to get a better grasp of this research.

2.1 Internet of Things

The IoT consists of devices that can be connected to each other via a potentially local network, but often the internet, and are able to communicate with each other to exchange data. Common devices such as kitchen appliances and smart thermostats belong to the IoT as well as more advanced technological applications such as cars, healthcare services and power grids. Due to the widespread use of the IoT in critical infrastructures, the importance of the security of the data management of these networks can not be overstated. Attacks that compromise and take down these critical infrastructures and services have great consequences [4]. Devices that are included in the IoT can often be cheaply made but are lacking in processing power and memory. This opens the IoT up to more simple attacks like Denial of Service (DoS). The IoT devices that are deployed in private and public networks will gather and use data to create added value. This data gathering and exchanging, however, can be a weak link in the security of the IoT network.

2.2 Blockchain

BC is a technology where users are able to collectively track transactions using a distributed ledger. In the past, a ledger was used for accounting in the financial world to keep track of all the transactions the company completed. The first BC was Bitcoin. In fact, Nakamoto [5, p. 1] noted in his Bitcoin white paper, Bitcoin was to be used as a "purely peer-to-peer version of electronic cash allows online payments to be sent directly from one party to another without going through a financial institution". Without the intermediary involvement of a financial institution, Bitcoin users did not have to worry about this financial institution not acting in the users' best interest.

To have the BC network consolidate to a consensus for the ledger a consensus algorithm is used. This algorithm is also used to safeguard the integrity and security of the distributed system. Bitcoin uses a Proof of Work algorithm (PoW) by solving complicated math problems to achieve a consensus.

Moreover, the PoW algorithm in Bitcoin is used for confirming transactions in the network and creating new blocks. PoW is considered very secure and reliable. However, due to the number of calculations necessary and the energy-consuming nature of this type of algorithm, it is not effectively scalable or suitable for an IoT application.

Recently in 2022 Ethereum however switched from PoW to Proof of Stake (PoS) specifically to consume less energy while being more secure [6]. In this new version validator nodes stake ETH on the Ethereum BC as collateral to destroy if the node misbehaves. Of these two most well-known consensus algorithms PoS has the edge over PoW in regards to IoT and BC integration as it consumes less processing power and battery.

Today BC is used for a wide variety of purposes and industries. Recently BC has been integrated with IoT-based healthcare systems. This integration safeguards patient data by creating a system that protects the security and privacy of electronic health records and ensures no manipulation can be performed [7].

3 Related Work

In the following section, we will present clear and concise reviews of various relevant surveys that are beneficial for researchers in this field. In addition, we present a clear and concise summary and comparison of these surveys in table 1.

The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial
This survey [8] focuses on forging a performance evaluation applicable to a wide variety of BC-based security and privacy systems. 13 consensus algorithms and nine evaluation parameters are discussed and thoroughly evaluated. Security analysis techniques to analyse the security of BC-based systems for IoT networks using Burrows, Abadi, and Needham Logic, game theory and theory analysis are explained that can be used to verify experimental results. The attention is focused on 17 different security requirements, including integrity, tractability, anonymity, access control, data auditability and unforgeability. The authors believe and justify that these requirements are fundamental for every BC security and privacy system. Then the authors go into moderate detail on what performance metrics are used in analysing the performance of BC-based security and privacy systems for the IoT networks. These performance metrics include the consensus delay, communication costs, computation costs, average throughput and transaction generation time. The backbone of this survey is the excellent tables and figures supporting all the sections to deliver a detailed yet easily understandable comparison.

The datasets that are used to evaluate the performance of BC-based security and privacy systems for IoT networks are inspected in conjunction with the cryptography libraries. The authors show what BC testbeds are used for the performance evaluation of BC-based security and privacy systems as well as the BC network type, IoT application and focus of the works. Experimental environments, hyper ledger groups and open-source BC platforms are discussed as well. When finishing the survey the authors mention that consensus algorithms can be of great impact on the performance of the BC-based systems for the IoT. Creating consensus algorithms that are tailored to the IoT are important and the authors point in the direction of DAG based consensus algorithms.

Ferrag and Shu have created a thorough survey focused on showcasing a variety of performance evaluation methods of BC-based security and privacy systems. They touch upon a plethora of related consensus algorithms and evaluated them based on various metrics with most importantly including latency, throughput, computation/storage/communication costs, scalability and pros/cons of the consensus algorithm. Security and performance evaluation techniques are thoroughly explained as well. This gives a solid overview and guides researchers on how the performance evaluation of BC-based security and privacy systems for the IoT can be executed.

Embedding Blockchain Technology into IoT for Security: A Survey
Xu et al. focus with this survey [9] on the major security risks that the IoT faces and how the characteristics of a BC-embedded IoT network can solve these problems. The authors first introduce what the IoT is and what the major security risks are that the IoT faces. They then bring the characteristics of a BC-embedded IoT network to light while going into moderate technical detail. The taxonomy of BC-based IoT security together with the structural and functional security are comprehensively explained. For structural security, the sensor, network and application layer are inspected. To complete all the security facades of BC in IoT the focus is then shifted toward how attackers can exploit the characteristics BC introduces in IoT networks such as DoS, link and modification attacks. To support the sketched security benefits possible scenarios where BC-based IoT can be useful are briefly covered. The authors go into detail about technical challenges and critically reflect on the challenges and issues the IoT network currently faces. These challenges include the lacking performance of IoT devices, sub-optimal consensus algorithms and unreliable wireless communication of IoT devices. Lastly, future research trends together with a strong and concise conclusion are presented.

The authors take a critical approach when analysing the issues that are still present and will be present in the future, so as not to see BC as a fix-all solution. This approach makes the survey excellent to get a good starting grasp of the security risks present in IoT networks and how BC can effectively be used to mitigate these risks, while also keeping in mind the BC-specific attacks that should be given thought about. Figures and tables compare the centralized and decentralized systems, taxonomy of BC-based IoT security, security issues of the sensor, network, application layer and BC-related access control models conveniently support the survey and its contents. The survey combines the topics of IoT security with BC-based IoT security into an understandable but broad study. This ensures the reader with more knowledge and also provides papers for future reading directions to delve deeper into this topic.

Survey	Description	Consensus Algorithms	Performance	Security	Privacy	(+) Pros (-) Cons
2021 Ferrag et al. [8]	Thorough survey focused on showcasing a variety of performance evaluation methods of BC-based security and privacy systems.	+++	++	+++	+++	+ Thorough + Varied
2021 Xu et al. [9]	Survey showcasing the major security risks that the IoT faces and how the characteristics of a BC-embedded IoT network can solve these problems.	– –	N/A	+++	+	+ Broad + Critical - Superficial sections
2019 ALi et al. [10]	Comprehensive survey showing the applications that BC has in the IoT.	++	+	++	+++	+ Broad + Monetization - Aged
2021 Yanez et al. [11]	Comprehensive survey methodologically discussing a wide variety of BC IoT integration tactics.	+	++	+	+	+ Comprehensive + Methodological
2020 Lao et al. [12]	Proposes a new traffic model and a five layer architecture for IoT BC while surveying various other research papers.	++	+	–	– –	+ Varied + Traffic models - Poor privacy discussion

Table 1: Summary of evaluated surveys
(– –) poor, (–) insufficient, (+) sufficient, (++) good, (+++) excellent

However, consensus algorithms are only superficially touched upon, while making these algorithms a central part of this paper would translate into a greater understanding of the discussed attacking mechanisms and security techniques. The authors state in the abstract that BC has the potential to increase the performance of IoT security, however they virtually omit any discussion about this in the paper. They only touch upon this increase in performance in a useful way as a future challenge.

Applications of Blockchains in the Internet of Things: A Comprehensive Survey Ali at al. have created a very comprehensive survey [10] on the applications that BC has on the IoT. The authors first familiarize the readers with the features of BC and its structure. As well as how transactions are performed by a BC and what smart contracts and consensus algorithms are. Both permissionless and permissioned modeled BCs are discussed together with the performance and scalability of the used consensus algorithms. The IoT is explained together with how it can be integrated with and decentralized by using BC to mitigate its issues and challenges. The authors draw attention to privacy concerns inherent to a centralized IoT network to then highlight different researches and frameworks that focus on BC-based decentralization for IoT privacy. The same is done for the inherent trust and security issues of IoT. How BC can be used for IoT identity and data management is discussed while proposed solutions are listed that ensure data integrity.

This survey has a pleasant, and at the time, novel section about how IoT devices, data and it's resources can be monetized. The authors even mention various startups that try to successfully monetize the BC and IoT integration. The use of a Directed Acyclic Graph (DAG) as an alternative approach to increase the scalability of decentralized ledgers is also touched upon. Issues and future research directions are discussed where the authors discuss the challenges the use of BC has in the IoT. In this survey this future work an challenges discussion is quite in-depth and due to four years passing since its publishing, some directions they suggested have indeed been explored.

The survey gives indeed a nice and comprehensive overview of the various applications of BC in the IoT. Due to the field of IoT and BC advancing quickly, one can feel that the survey has aged. However, due to the fact that the survey is comprehensive, well put together and quite advanced at its publishing it is still relevant to researchers in this field.

Architecting Internet of Things Systems with Blockchain: A Catalog of Tactics This survey [11] systematically discusses different tactics on the possibilities of implementing the architecture of an IoT system with BC and what design choices have to be made. To report on these tactics the authors make use of the template proposed by Lewis and Lago [13]. The template consists of providing a summary, motivation, description, constraints, example, related tactics and optionally variations of the tactic. The validity of this study is also critically discussed. In this discussion the authors categorise the potential risks to the validity of the study and how they have tackled these. The identified risk categories include external validity, internal validity, construct validity and conclusion validity.

The authors did an excellent job of showcasing different design tactics for the integration of BC in the IoT in this survey. They concretely show what the effects of these design choices are by making use of a well-organized template including thought-out pros and cons. This gives researchers in this field a solid catalog of the possible designs, their effects and examples.

A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling This survey [12] presents the architecture of IoT, BC and BC-based IoT in compact yet informative sections supported by clear figures. The architecture of IoT networks is divided into the physical, network, application, middleware and business layer. This is a more specific separation of layers than most surveys as the authors propose this five-layer architecture for IoT BC. Figures support this division and let the reader get a solid overview of the architecture.

The BC architecture is divided into the usual full and light

nodes. The current and integrated architecture of IoT-BC networks are discussed and shown. The authors discuss consensus algorithms and, as one of the few, also incorporate Ripple in this discussion. The inclusion of Ripple highlights a capable consensus mechanism with high scalability and transaction speed. The discussed consensus algorithms are compared with various characteristics and summarized.

Current traffic models and protocols of existing distributed systems are compared and analysed with several metrics including performance and power consumption by the survey. These models are divided into the following categories i) Gossip protocol ii) Kademlia algorithm ii) Direct Acyclic Graph. They propose a new traffic model as well. A solid understanding of traffic models used in BC-based IoT systems creates the opportunity to increase IoT BC performance by making educated decisions.

Security and, in particular, privacy could have been covered better. These topics should certainly be discussed when a paper proposes a new data traffic model. However, the survey is varied and well supported by explaining tables and figures. The inclusion of traffic models and comparisons in the survey's content makes this a solid and useful work.

4 State-of-the-art: A study

This section will review research papers that are the state-of-the-art of IoT data management using BC-based solutions. We will then compare these research papers on different metrics as well as provide pros and cons to give a good overview of the differences. Table 2 contains these comparisons and pros cons.

ConSenseIoT: A Consensus Algorithm for Secure and Scalable Blockchain in the IoT context This paper [14] proposes the consensus algorithm ConSenseIoT that would not impact the performance of the IoT network while ensuring distributed consensus among the IoT devices. As IoT networks often are computationally and energy-limited devices this proposal is useful. ConSenseIoT is a Proof of Trust (PoT) algorithm, meaning that the trust score of a node is used when deciding if an updated BC state proposed by a node is accepted. PoT in turn also decreases the computational demand on the IoT device.

Decentralized Identifiers (DID) [20] and verifiable credentials (VC) [21] are used to support the functioning of the algorithm. Niavia and Loupos explain that "DIDs are used to encrypt the channel between the devices identity agent while the latter ones are used to exchange identity proofs as well as messages of the algorithm itself" (2022, p. 4). DIDs have also been designed with privacy at the center. This makes it not only more private, but more secure as well. Couple this with the fact that authors claim that this approach does not impact the performance of the network and consumes less energy, ConSenseIoT is a promising and exciting new consensus algorithm.

Blockchain-based Security for Heterogeneous IoT Systems With this paper [15], Yuzik and Makaroff aim to solve one of the IoT's core problems of different resource-constrained devices. They research, test and discuss a security-improving BC implementation for heterogeneous IoT systems with devices that vary in resources. This implementation is based on Ethereum, as this allows for scripting and looping by making use of smart contracts. The authors use the GO Ethereum client (Geth) with a Proof of Authority (PoA) implementation. Using PoA as opposed to PoW ensures that more devices can participate as it is less computationally demanding.

They tested the concept on a network consisting of 3 different types of Raspberry Pis and an AdaFruit Feather M0. The AdaFruit Feather M0 has low memory capacity and networking bandwidth and thus is incapable of running Geth locally. The authors use this to simulate the often lacking abilities of IoT devices in networks. These devices can make use of a proxy and still participate in the network by using LoRa to communicate with IoT devices that do run an Ethereum client locally and act as a gateway. Devices that are capable of running Geth in full sync mode will do so, lesser capable devices will run Geth in light sync mode. Full sync mode devices store the entirety of the BC on the device and verify all created blocks and transactions. Light sync nodes do not store the BC and are thus less resource-demanding, but do need full sync nodes to get the BC information. This architecture can be seen in Figure 1.

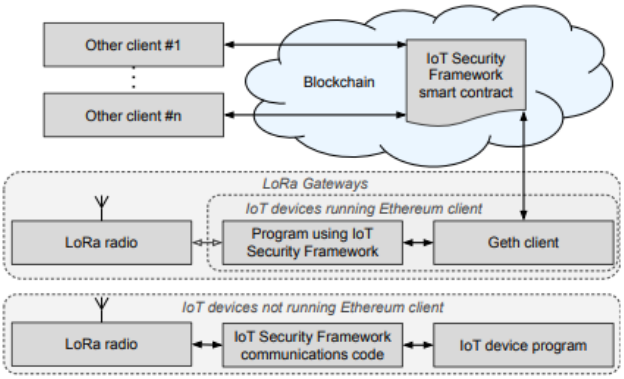

Figure 1: Architecture of the proposed network (yuzik, 2020, p. 4)

This framework is tested by measuring the data latency throughout a set period of time. During this period every 5 seconds, a new block was generated on the BC network. The results of the experiment show that it is indeed possible to run this framework with different IoT devices, albeit with periodic latency spikes in some setup cases due to overloaded processors.

Due to a solid background and helpful subsections explaining the process, the proposed system can easily be followed. However, the Ethereum network has been in development in the years after the publishing of this paper and has fully transitioned from a PoW to a PoS protocol. This could mean easier implementation of this proposed BC framework into IoT networks.

Research	Description	Consensus Algorithms	Performance	Security	Privacy	(+) Pros (-) Cons
2022 Niavis et al. [14]	Proposes ConSenseIoT, a distributed PoI concensus algorithm that would not impact the performance of the IoT network	PoI	+	++	+	+ Promising concept - Not tested
2020 Yuzik et al. [15]	Implementation, testing and discussion of a proof-of-concept security improving BC implementation for heterogeneous IoT systems.	PoA	++	++	–	+ Proof-of-concept + Thorough background - Based on outdated Ethereum
2019 He et al. [16]	System is proposed for the verification of over the air firmware updates using smart contracts.	ETH	++	++	–	+ Proof-of-concept - Limited background - Not extensive
2020 Zhoa et al. [17]	Paper proposing a key-derived controllable lightweight secure certificateless signature algorithm.	PoT	+++	++	+	+ Tested + Proof - Scalability not treated
2021 Zeng et al. [18]	DAG based BC scheme for IIoT is proposed that is faster, more secure and energy efficient.	DAG	+++	++	+	+ Tested + Thorough
2021 Putra et al. [19]	Proposes an adaptive decentralized IoT access control mechanism by using a a permissioned private and public BC.	N/A	++	+	+	+ Tested + Critical - Slower

Table 2: Summary of evaluated research papers
(– –) poor, (–) insufficient, (+) sufficient, (++) good, (+++) excellent

Securing Over–The–Air IoT Firmware Updates using Blockchain This paper [16] discusses Over-The-Air (OTA) firmware updates, which are common for wireless devices in the IoT due to its convenience. However, due to the wireless nature of this update, there are vulnerabilities. The attackers do not need physical access to the devices and can potentially perform DoS and Man in the Middle (MitM) attacks. The authors propose a scalable system to verify the integrity of OTA firmware updates of a large number of IoT devices. A smart contract is used to verify if the firmware update is legitimate. The contract rejects the update when there are too many failed attempts, the update time window is expired (set to 60sec) or when the hash code mismatches.

The authors focused on the implementation and testing of this concept to accumulate meaningful results. They performed DoS and MitM attacks on a proof of concept system using a Wemos D1 Mini board functioning as the IoT device to undermine the update process. The results show that the aim of this paper was indeed reached, the smart contract rejected the firmware update as it was outside of the time window due to DoS or was tampered with by MitM attacks. Performance and scalability were evaluated by measuring RESTful API operations. These performance results were promising as well, the proposed system scaled well with the increase in ledger entries. While this implementation is not very extensive, the base is well thought out and implemented.

A Certificateless Consortium Blockchain for IoTs This paper [17] proposes the scheme Controllable Lightweight Secure Certificateless Signature (CLS^2). Current consortium BCs use mostly a Public Key Infrastructure (PKI) to try to create a secure and trusted environment. However, PKI uses certificates to verify data ownership which increases bandwidth usage and risks the certificate leaking information. To reduce the bandwidth usage various certificateless PKI models have been tried, however, the authors state that "the prevailing Certificateless Signature (CLS) algorithm has many performance and security vulnerabilities, and is not suitable for IoTs with limited computation and power capacities".

CLS^2 is implemented on the Hyperledger Fabric network. This proposal is supported by introducing various algorithms, ranging from setting a partial private key to the sign and verify procedures. The authors incorporated a thorough mathematical proof discussing the security analysis of the proposed scheme using the random oracle model. The performance of the proposed scheme is also compared to the native Hyperledger Fabric with PKI-CA mode. In this comparison, the authors show that although the proposed scheme is 6-8% slower than the natively supported scheme, the request and response messages are only 27.0% and 24.8% of the size respectively. This results in a significant decrease in the necessary bandwidth. CLS^2 is also more secure as the researchers focused on mitigating the forgery of signatures and public key replacement.

A Blockchain Scheme Based on DAG Structure Security Solution for IIoT According to the authors this research paper [18] focuses on the data security risks of the Industrial Internet of Things (IIoT). IIoT related replay attacks, network efficiency and privacy are discussed and negated or improved by the authors. They propose a BC network scheme based on a DAG structure. The proposed network scheme consists of lightweight and basic entity nodes. These entity nodes can be production equipment, sensors or gateways. Due to being battery-powered, light nodes do not have the capacity to run the consensus algorithm on the device, however, they can be used in data transfer and verification. The basic nodes however do have this capacity as they do not have limited power, gateways and controllers fall into this category. The proposed scheme has implemented load balancing in the DAG network to minimize energy usage of the nodes that use batteries. This not only extends the network's life cycle but also minimizes the impact of replay attacks focused on draining the batteries. Differential privacy is used to avoid attackers gaining access to the data of other nodes within the network when one of the network nodes is compromised.

The proposed DAG algorithm is compared to a BC scheme based on Sensor-MAC [22] (S-MAC) and BC based on chain

structures like Bitcoin and Ethereum. S-MAC is another protocol that tries to reduce the power consumption of a battery-operated wireless sensor network. The proposed BC architecture outperforms the other schemes on average network delay when increasing the number of nodes or network load. The average transaction time is less than the chain structure BC and more than the S-MAC BC. The proposed scheme never used more energy on average than the other schemes and comparatively used less the higher the network load was.

Trust-Based Blockchain Authorization for IoT Due to the vast size of the IoT the necessity of an access control mechanism to properly guard sensitive data is high. The authors of this paper [19] the usual access control mechanisms for IoT are centralized and non-flexible. They have designed an IoT access control mechanism for networks where service consumers want to access data that service providers have. This mechanism is decentralized and realised by simultaneously making use of a permissioned private BC and public BC. The private BC stores the IoT attributes used for identification and the public BC manages the access control via smart contracts. Off-chain Dedicated Data Storage (DDS) stores the service provider's data which the service consumers can request access to. This makes data management safer and more private. A Trust and Reputation System (TRS) is designed and proposed to create an adaptive system to detect malicious activity as well.

This access control mechanic is tested and compared against other similar access control mechanisms on the public Ethereum network. Note that any BC with support for smart contracts can implement this proposed system. The test network showed that the proposed mechanism is resilient to various attacks such as DoS, bad-mouthing and newcomer attacks. While the authors have created only one DDS node on the network, this did show to be a bottleneck. Furthermore, the latency was consistent and the malicious nature of dishonest nodes quickly got reflected in the trust score ensuring these nodes were quickly blacklisted to revoke access to the data.

5 Evaluation metrics

In this section, we discuss what evaluation metrics we have used and how we categorized the papers in section 3 and 4. We also underline the difference between the categorization of the surveys and research papers.

We categorize the research papers and surveys using indicators to show how well a topic has been discussed. These indicators are (– –) for poor coverage, (–) for insufficient, (+) for sufficient and (++) for good. When a survey discussed something exceptionally well we use (+++) to show this exceeding of expectation. When an evaluation metric is not applicable we note (N/A).

When the authors have sufficiently covered a metric we will categorize it with a (+) sufficient. However, it is difficult to judge when this metric is adequately discussed. To aid us in making this decision we look at how many references the authors used when discussing a particular metric. Also, it is taken into account when the authors point towards further research instead of discussing the metric themselves. We expect surveys to have more about consensus algorithms than research papers. This is because most of the papers that the survey will compare/review will be in contact in at least some way with consensus algorithms. For the research papers, we will also take into account what the paper is focusing on and proposing. As to not judge a paper focused solely on security on privacy. The metrics we are using to categorize the surveys in are the following.

1) Consensus algorithms: These algorithms are an integral part of BC-based solutions. As such, they should also be an integral part of surveys covering BC-based solutions. When consensus algorithms are discussed, the other survey parts are better understood. Specifically when talking about security and privacy. For the state-of-the-art research papers, we instead note on what consensus algorithm the work is based.

2) Performance: Devices in the IoT often lack good components that enhance performance. This can hinder the performance of said device if BC is used in the network this device is connected to. It is thus necessary to discuss the performance of BC-based solutions and to keep the performance capabilities of the underlying IoT devices in mind. Often performance is also efficiency related.

3) Security: BC can be very beneficial in improving the security of IoT data management. As security is part of the subject of this paper we include this as a metric.

4) Privacy: In IoT data management, privacy is important. BC can help to provide users with more privacy for their data. It is thus an important aspect of using BC-based solutions.

6 Discussion and Future Work

In this section we will discuss our survey and state-of-the-art research paper reviews as well as outline potential future research directions.

6.1 Discussion

The surveys we have reviewed each focused on different parts of integrating BC with the IoT. What all the surveys have in common is the focus on privacy when using BC for the IoT. Ferrag et al. created a survey that was the most comprehensive and useful for researchers in this field [8]. BC-based solutions can be very beneficial to the IoT. The characteristics of BC translate to increased fault tolerance, resilience and transparency.

BC can also help in the management of data storage as seen in [19]. The authors talked about data extensively. They proposed an access control mechanism that consisted of a permissioned private and a public BC. This makes data management more secure and private as sensitive data can be stored on the permissioned private BC. The sensitive data can then be accessed if deemed necessary by the access control mechanism. The needed details of these requests can be retrieved from the public BC.

BC can also provide protection against DOS attacks. [16] proposed a scalable system to protect OTA firmware updates of IoT devices. This system rejects an OTA update when a DOS attack is occurring so the update can be tried again

at a later time without endangering the IoT device's update. Moreover, [19] has created an access control mechanism resilient to DoS attacks.

As there is a wide range of BCs available for BC-based solutions in the IoT network, the implementation can be quite flexible. A BC can be specifically chosen on its capabilities so they align with the needs of a specific IoT network.

However, BC is not the see-all fix-all technology for IoT. There are drawbacks, [9] took a critical approach not only to their own survey but to BC in general as well. They list that most BC needs enough computation power to function properly, something that can be lacking in IoT devices. One should also exercise caution for the amount of bandwidth that is needed when using BC solutions in an IoT network. When the number of devices sharply increases, so does the bandwidth usage. BC-based solutions in IoT can also introduce BC-based weaknesses into the network. Various BCs and their underlying consensus algorithms can be vulnerable to attacks including equipment injection, modification, node abandonment and various reputation-based attacks [8], [9].

6.2 Future work

During our study the following future research directions came to light.

1) Consensus algorithms tailored to the IoT: The IoT consists of devices that can lack in performance and throughput. While PoW is secure, it has low efficiency and high computational costs this popular consensus algorithm should not be used for IoT. DAG is suitable for the IoT due to its high throughput and highly scalable nature. However, the communication costs are relatively high, making it less useful for IoT devices that communicate with a higher frequency [8], [10] - [12], [18]. However, due to the benefits we emphasise DAG-based consensus algorithms to be explored further in the future. It should be considered that BC-based solutions for the IoT benefit greatly from high scalability, high throughput and low communication cost consensus algorithms. Depending on the situation, low latency could also be required in the IoT network. Ideally, benefits of different consensus algorithms should be combined.

2) Individual IoT device security: Important steps have been taken in the reviewed state-of-the-art research papers to improve the IoT security. Future research directions should continue the pursuit of improving the IoT network security, while simultaneously focusing on the individual device's security. IoT networks can often be vulnerable to attacks due to vulnerable and resource constrained connected devices. As there is a vast amount of different kind of devices connected, this challenge is hard to tackle. However, BC is a strong technology to support future research works in this aspect.

7 Responsible Research

In this section we will outline how we responsibly created this research. We reflect on how we selected papers and the reproducibility of our work.

As we have reviewed papers there need to be safeguards in place to ensure credible and trusted papers are chosen to review. In the early stages of this paper, we discussed where we should search for papers with our supervisor and how we can adequately judge the validity of papers. This gave us excellent tools to ensure we choose solid sources for this review in consultation with our supervisor. The ACM Digital Library and IEEE Xplore were used in the search for sources.

7.1 Reproducibility

The reproducibility of this study is difficult to judge as there are no experiments done by this paper. The papers we have addressed have done experiments, however, these papers each included detailed descriptions to aid reproducibility. The specific search for sources is hard to reproduce as it was not done in a rigid systematic way. We tried various search queries while the supervisor suggested sources as well. These search queries specifically included combinations of the terms IoT, data management, BC, security and privacy. However, all the sources we used are accessible either in IEEE Xplore or the ACM Digital Library.

8 Conclusions

In this paper, we have reviewed surveys and state-of-the-art research papers that focused on the area of research that uses BC-based solutions to improve the security and efficiency of IoT data management. We analysed and categorized the related surveys and research papers on the metrics of consensus algorithms, performance, security and privacy. This gives a good overview of the reviewed papers and highlights their strengths and shortcomings.

We discussed how BC can improve the security and efficiency of the IoT by providing increased fault tolerance, resilience and transparency. We also reflect that BC can not immediately fix all the problems IoT has and can even introduce new vulnerabilities to IoT networks. Based on our findings we discussed directions that are to be taken in future works focusing on this area. We included how we performed this research in a responsible and reproducible way.

References

[1] S. Sorrel, "The internet of things: Consumer, industrial & public services 2018-2023," jun 2018.

[2] 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 Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[3] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in iot using machine learning and blockchain: Threats and countermeasures," *ACM Comput. Surv.*, vol. 53, dec 2020.

[4] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system [white paper]," white paper, Bitcoin.org, 2019.

[6] C. Smith, "Proof-of-stake (pos)," nov 2022.

[7] R. Mohammed, R. Alubady, and A. Sherbaz, "Utilizing blockchain technology for iot-based healthcare systems," *Journal of Physics: Conference Series*, vol. 1818, p. 012111, mar 2021.

[8] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17236–17260, 2021.

[9] L. D. Xu, Y. Lu, and L. Li, "Embedding blockchain technology into iot for security: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10452–10473, 2021.

[10] 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 Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[11] W. Yánez, R. Bahsoon, Y. Zhang, and R. Kazman, "Architecting internet of things systems with blockchain: A catalog of tactics," *ACM Trans. Softw. Eng. Methodol.*, vol. 30, apr 2021.

[12] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, feb 2020.

[13] G. Lewis and P. Lago, "Architectural tactics for cyber-foraging: Results of a systematic literature review," *Journal of Systems and Software*, vol. 107, pp. 158–186, 2015.

[14] H. Niavis and K. Loupos, "Consenseiot: A consensus algorithm for secure and scalable blockchain in the iot context," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, (New York, NY, USA), Association for Computing Machinery, 2022.

[15] K. Yuzik and D. Makaroff, "Blockchain-based security for heterogeneous iot systems," in *Proceedings of the 30th Annual International Conference on Computer Science and Software Engineering*, CASCON '20, (USA), p. 63–72, IBM Corp., 2020.

[16] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing over-the-air iot firmware updates using blockchain," COINS '19, (New York, NY, USA), p. 164–171, Association for Computing Machinery, 2019.

[17] X. Guo, Q. Guo, M. Liu, Y. Wang, Y. Ma, and B. Yang, "A certificateless consortium blockchain for iots," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pp. 496–506, 2020.

[18] P. Zeng, X. Wang, L. Dong, X. She, and F. Jiang, "A blockchain scheme based on dag structure security solution for iiot," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 935–943, 2021.

[19] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, "Trust-based blockchain authorization for iot," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1646–1658, 2021.

[20] "Decentralized identifiers (dids) v1.0," Jul 2022. https://w3c.github.io/did-core/.

[21] "Verifiable credentials data model v2.0," Jan 2023. https://w3c.github.io/vc-data-model/.

[22] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," Tech. Rep. ISI-TR-2001-543, USC/Information Sciences Institute, Sept. 2001.