A systematic literature review of blockchain cyber security

Taylor, PJ, Dargahi, T, Dehghantanha, A, Parizi, RM and Choo, KKR

http://dx.doi.org/10.1016/j.dcan.2019.01.005

Digital Communications and Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

A systematic literature review of blockchain cyber security

Paul J. Taylor [a], Tooska Dargahi [a], Ali Dehghantanha [b], Reza M. Parizi [c], Kim-Kwang Raymond Choo [d,*]

[a] School of Computing, Science & Engineering, University of Salford, Manchester, UK
[b] Cyber Science Lab, School of Computer Science, University of Guelph, Ontario, Canada
[c] Department of Software Engineering and Game Development, Kennesaw State University, Marietta, GA, 30060, USA
[d] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, 78249, USA

ARTICLE INFO

Keywords:
Blockchain
Smart contracts
Cyber security
Distributed ledger technology
IoT
Cryptocurrency
Bitcoin

ABSTRACT

Since the publication of Satoshi Nakamoto's white paper on Bitcoin in 2008, blockchain has (slowly) become one of the most frequently discussed methods for securing data storage and transfer through decentralized, trustless, peer-to-peer systems. This research identifies peer-reviewed literature that seeks to utilize blockchain for cyber security purposes and presents a systematic analysis of the most frequently adopted blockchain security applications. Our findings show that the Internet of Things (IoT) lends itself well to novel blockchain applications, as do networks and machine visualization, public key cryptography, web applications, certification schemes and the secure storage of Personally Identifiable Information (PII). This timely systematic review also sheds light on future directions of research, education and practices in the blockchain and cyber security space, such as security of blockchain in IoT, security of blockchain for AI data, and sidechain security,etc.

1. Introduction

As a cryptographic-based distributed ledger, blockchain technology [1,2] enables trusted transactions among untrusted participants in the network. Since the introduction of the first Bitcoin blockchain in 2008 [3], various blockchain systems, such as Ethereum [4,5] and Hyperledger Fabric [6], have emerged with public and private accessibility outside of existing fiat currencies and electronic voucher systems. Recently, blockchain technology has also been the subject of an increasing number of scientific researches [7–10], and has raised significant interest among researchers, developers, and industry practitioners due to its unique trust and security characteristics.

There is no doubt that the popularity of blockchain has increased worldwide. More than simply becoming popular, it has made a lasting impact on the world [11]. For example, it has been commercially adopted [12], influenced world currency markets [13], facilitated the proliferation of illicit dark web marketplaces. It also has been a significant factor affecting the proliferation of financially driven cyber-attacks [14], such as ransomware [15] and denial of service [16] against retailers and other online organizations. In fact, the implementation and use of blockchain have far surpassed its original purpose as the backbone to the world's first decentralized cryptocurrency. The value of a trustless, decentralized ledger that carries historic immutability has been recognized by other industries looking to applying the core concepts to the existing business processes. The unique properties of the blockchain technology make its application an attractive idea for many business areas, such as banking [17], logistics [18], the pharmaceutical industry [19], smart contracts [20,21], and most importantly, in the context of this paper, cyber security [22,23].

Most notably, there is an emerging trend beyond cryptocurrency payments: the blockchain could enable a new breed of decentralized applications without intermediaries and serve as the foundation for key elements of Internet security infrastructures. Hence, it is important to identify the exsiting researches specifically related to the application of blockchain to the problem of cyber security, in order to address how emerging technologies can offer solutions to mitigate emerging threats. To identify what research has already been conducted in relation to blockchain and cyber security, it is necessary to systematically map out relevant papers and scholarly works. This paper seeks to focus on existing literature concerning the use of blockchain as a supporting technology for cyber security applications, including areas of business related to privacy, security, integrity and accountability of data, as well as its use in securing

* Corresponding author.
E-mail addresses: Paul.Taylor_Titan@titan.police.uk (P.J. Taylor), T.Dargahi@Salford.ac.uk (T. Dargahi), Ali@cybersciencelab.org (A. Dehghantanha), rparizi1@kennesaw.edu (R.M. Parizi), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

https://doi.org/10.1016/j.dcan.2019.01.005
Received 19 June 2018; Received in revised form 13 January 2019; Accepted 21 January 2019
Available online xxxx

networked devices, such as Internet of Things (IoT). Our overarching goal is to provide a community-driven initiation for a better study of blockchain and cyber security that explores the interplay between the two frequently discussed fields. Toward this goal, we will critically examine existing works and studies on blockchain cyber security and use our insights to develop new directions.

1.1. Prior research

Specifically in relation to the application of blockchain to the problem of cyber security, to the best of our knowledge, there appears to be very limited Systematic Literature Reviews (SLRs). One of the most recent survey papers in the realm of blockchain and cyber security was performed by Salman et al. [22]. In this study, the authors highlight the challenges and problems associated with the use of security services in the centralized architecture in various application domains, and provide a comprehensive review of current blockchain-enabled methods for such security service applications in areas of authentication, confidentiality, privacy, access control, data and resource provenance, and integrity assurance in distributed networks. In our view, this study gives a valuable start to fellow researchers who might be interested in blockchain-based network and service security. Apart from it, a small number of studies in relation to blockchain and its wider impact have also been published and we will discuss them below to examine the differences between the topics selected by the authors and our research.

Yli-Huumo et al. conducted an SLR in 2016 to determine what research results had been published in relation to the general concept of blockchain technology [24]. They excluded legal, economic and regulatory research from their review and focused on papers about blockchain technology. They found 80% of the research papers focus on Bitcoin projects, in particular on a common theme of security and privacy. Since 2016 the applications for blockchain have diversified, so our research looks to investigate what research works exist specifically in regard to cyber security and blockchain applications.

Towards the end of 2016, Conoscenti et al. conducted an SLR concerning the use and adaptability of blockchain specifically in relation to IoT and other peer-to-peer devices [25]. Interestingly, they highlighted that the blockchain could be used for data abuse detection without the need of a central reporting mechanism. However, they did not look at the wider impact of blockchain on cyber security in general. Seebacher et al. provided an SLR in 2017 that highlighted the increasing impact of blockchain on service systems [26]. They recommended future work to include a review of real world applications, which is the basis of our research as we look to see how blockchain can affect cyber security problems.

All the previous studies mentioned above answer questions related to the wider use of blockchain technology, but they do not examine specifically its use in improving cyber security solutions. The field of research in relation to blockchain has a relatively short history and is advancing quickly. Therefore, it is necessary to provide a fresh summary of the more recent research works, in particular in the realm of blockchain and cyber security, so as to guide new research activities.

1.2. Research goals

The purpose of this research is to analyze existing studies and their findings and to summarize the efforts of research in blockchain applications for cyber security. To make the work more focused, we developed three research questions as shown in Table 1.

1.3. Contributions and layout

This SLR is complementary to existing research and provides the following contributions for those having an interest in blockchain and cyber security to further their work:

Table 1
Research questions.

Research Questions (RQ)	Discussion
RQ1: What are the latest blockchain applications focused on security?	Use cases for blockchain have diversified away from solely cryptocurrency. A review of the latest practical applications will help with understanding the full impact of blockchain technology on cyber security.
RQ2: How is blockchain used to improve cyber security?	Blockchain features can be deployed to solve problems related to the security of devices, networks and their users. This will provide an understanding of the methods used to implement blockchain in digital infrastructure for the purpose of security.
RQ3: What methods are available for blockchain solutions to manage security without requiring a cryptocurrency token?	Cryptocurrency blockchains are commonly maintained through a Proof-of-Work (PoW) mechanism whereby miners can show to the rest of the network that they have invested significant resources in order to assist in the validation of transactions. This question will look at research that addresses how a blockchain can be maintained without the requirement to incentivize miners for transaction validation.

- We identify 42 primary studies related to blockchain and cyber security up to early 2018. Other researchers can use this list of studies to further their work in this specific field.
- We further select 30 primary studies that meet the criteria we set for quality assessment. These studies can provide suitable benchmarks for comparative analysis against similar research.
- We conduct a comprehensive review of the data contained within the subset of 30 studies and present the data to express the research, ideas and considerations in the fields of blockchain and cyber security.
- We present a meta-analysis of the state of play in regard to methods in which blockchain can be implemented to improve security of existing and emerging cyber technologies.
- We make representations and produce guidelines to support further work in this area.

This paper is structured as follows: Section 2 describes the methods with which the primary studies were systematically selected for analysis. Section 3 presents the findings of the analysis of all the primary studies selected. Section 4 discusses the findings related to the research questions presented earlier. Section 5 concludes the research and offers some suggestions for future research.

2. Research methodology

To achieve the objective of answering the research questions, we conducted the SLR in accordance with the guidance published by Kitchenham and Charters [27]. We sought to move through the planning, conducting and reporting phases of the review in iterations to allow for thorough evaluation of the SLR.

2.1. Selection of primary studies

Primary studies were highlighted through passing keywords to the search facility of a particular publication or search engine. The keywords were selected to promote the emergence of research results that would assist in answering the research questions. The Boolean operators were restricted to AND and OR. The search strings were:

("blockchain" OR "block-chain" OR "distributed ledger") AND "security"

("blockchain" OR "block-chain" OR "distributed ledger") AND ("cyber security" OR "cybersecurity" OR "cyber-security")

The platforms searched were:

- IEEE Xplore Digital Library
- ScienceDirect
- SpringerLink
- ACM Digital Library
- Google Scholar

The searches were run against the title, keywords or abstract, depending on the search platforms. The searches were conducted on 30th April, 2018 and we processed all studies that had been published up to this date. The results from these searches were filtered through the inclusion/exclusion criteria, which are to be presented in Section 2.2. The criteria allowed us to produce a set of results that could then be run through the snowballing process as described by Wohlin [28]. Forward and backward snowballing iterations were conducted until no further papers meeting the inclusion criteria were detected.

2.2. Inclusion and exclusion criteria

Studies to be included in this SLR must report empirical findings and could be papers on case studies, new technical blockchain applications and commentaries on the development of existing security mechanisms through blockchain integration. They must be peer-reviewed and written in English. Any results from Google Scholar will be checked for compliance with these criteria as there is a possibility for Google Scholar to return lower-grade papers. Only the most recent version of a study will be included this SLR. The key inclusion and exclusion criteria are shown in Table 2.

2.3. Selection results

There were a total of 742 studies identified from the initial keyword searches on the selected platforms. This was reduced to 665 after removing duplicate studies. After checking the studies under the inclusion/exclusion criteria, the number of papers remaining for reading was 72. The 72 papers were read in full with the inclusion/exclusion criteria being re-applied, and 32 papers remained. Forward and backward snowballing identified an additional 4 and 6 papers respectively, giving a final figure for the number of papers to be included in this SLR as 42.

2.4. Quality assessment

An assessment of the quality of primary studies was made according to the guidance set by Kitchenham and Charters [27]. This allowed for an assessment of the relevance of the papers to the research questions, with consideration for any signs of research bias and the validity of experimental data. The assessment process was based on the process used by Hosseini et al. [29]. Five randomly selected papers were subjected to the following quality assessment process to check their effectiveness:

Table 2
Inclusion and exclusion criteria for the primary studies.

Criteria for Inclusion	Criteria for Exclusion
The paper must present empirical data related to the application and the use of blockchain.	Papers focusing on economic, business or legal impacts of blockchain applications.
The paper must contain information related to blockchain or associated distributed ledger technologies.	Grey literature such as blogs and government documents.
The paper must be a peer reviewed product published in a conference proceeding or journal.	Non-English papers.

Stage 1: **Blockchain.** The paper must be mainly focused on the use of blockchain or the application of blockchain technology to a specific problem well-commented.
Stage 2: **Context.** Enough context must be provided for the research objectives and findings. This will allow for accurate interpretation of the research.
Stage 3: **Blockchain application.** There must be enough details in the study to make an accurate presentation for how the technology has been applied to a specific problem, which will assist in answering research questions RQ1 and RQ2.
Stage 4: **Security context.** The paper must provide an explanation for the security problem, in an effort to assist in answering RQ3.
Stage 5: **Blockchain performance.** Assessing the performance of blockchain in the environment for which it is applied will allow for comparisons of different blockchain applications.
Stage 6: **Data acquisition.** Details about how the data was acquired, measured and reported must be given to determine accuracy.

This checklist for quality assessment was then applied to all other primary studies identified. It was found that 11 studies did not meet one or more of the checklist items and therefore were removed from the SLR, as shown in Table 3.

2.5. Data extraction

All papers that had passed the quality assessment then had their data extracted to assess the completeness of data to test the accurate recording of information contained within the papers. The data extraction process was tried on an initial five studies before being expanded to include the full set of studies that have passed the quality assessment phase. The data from each study were extracted, categorized and then stored in a spreadsheet. The categories given to the data were as follows:

Context data: Information about the purpose of the study.
Qualitative data: Findings and conclusions provided by the authors.
Quantitative data: When applicable to the study, data observed by experimentation and research.

Fig. 1 shows the number of papers selected at each stage of the process and the attrition rate of papers got from the initial keyword searches on each platform down to the final selection of primary studies.

2.6. Data analysis

To meet the objective of answering the research questions, we compiled the data held within the qualitative and quantitative data categories. Additionally, we conducted a meta-analysis of those papers that were subjected to the final data extraction process.

2.6.1. Publications over time

Despite the fact that the concept of blockchain, entwined with Bitcoin, was published in 2008, there were no final primary study papers published before 2015. This may highlight the newness of the ideas concerning cyber security applications for blockchain. Fig. 2 is a chart showing the number of primary studies published each year. As can be

Table 3
Excluded studies.

Checklist for the Criteria Stages	Excluded Studies
Stage 1: Blockchain	[S26] [S37]
Stage 2: Context	[S5] [S23]
Stage 3: Blockchain application	[S6]
Stage 4: Security context	[S17] [S28] [S32]
Stage 5: Blockchain performance	[S40]
Stage 6: Data acquisitionn	[S18] [S31]

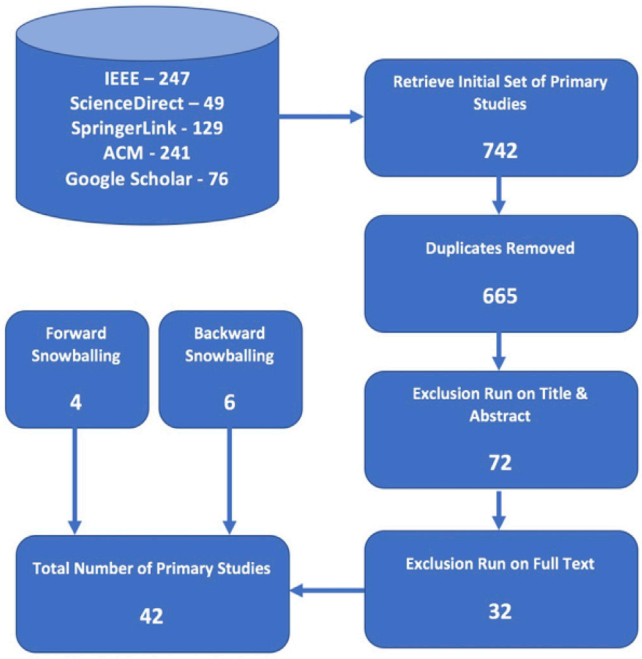

Fig. 1. Attrition of papers through processing.

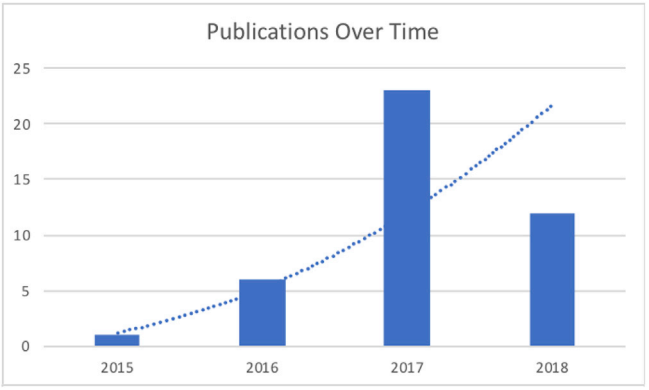

Fig. 2. Number of primary studies published over time.

seen in the figure, there is an upward trend in the usage of blockchain in the cyber security context. We envisage that in the future we will see a significant number of research studies regarding the adoption of blockchain in real world applications, as the number of publication up to April 2018 is only half of the whole number of publications in 2017.

2.6.2. *Significant keyword counts*

In order to summarize the common themes amongst the selected primary studies, an analysis of keywords was performed across all 42 studies. Table 4 shows the number of times some specific words appeared in all of the primary studies. As can be seen in the table, excluding the key words selected by the author, i.e., "blockchain" and "security", the third keyword appearing most frequently in our dataset is "IoT", after "network" and "transaction". This shows an increasing interest in the adoption of blockchain in the context of IoT, as we will discuss further in Section 3.

3. Findings

Each primary research paper was read in full and relevant qualitative and quantitative data was extracted and summarized in Table 5. All the primary studies had a focus or theme in relation to how blockchain was dealing with a particular problem. The focus of each paper is also recorded below in Table 5.

Table 4
Counts of the keywords in the primary studies.

Keywords	Count
blockchain	2389
network	1528
security	1404
transaction	1105
IoT	1041
transactions	773
information	693
smart	669
control	582
devices	552
bitcoin	544
privacy	543
distributed	533
internet	482
systems	473
protocol	450
consensus	450
technology	430
networks	391
applications	333
attacks	320
encryption	222
ethereum	156

Each paper's focus was further grouped into broader categories to allow for a simplified classification of the themes of the primary studies. Studies that had a focus concerning virtual machines, networking and virtual network management were grouped together into the *networks* category. Studies that had a focus related to peer-to-peer sharing, encrypted data storage and searching were grouped into the category of *data storage and sharing*.

Fig. 3 shows the percentages of different themes of the 30 primary studies which had made them pass the quality assessment to be included in the data analysis.

The themes identified in the primary studies highlight that almost half (45%) of all studies on cyber security applications of blockchain are concerned with the security of IoT devices. *Data storage and sharing* is the second most popular theme, with a percentage of 16%. The studies include blockchain applications for searching encrypted cloud-based data and for preventing the tampering of file names and data contained within. Networks are the third commonest theme, accounting for 10%, and are mostly concerned with how blockchain can provide security and authenticity to virtual machines and containers. Data privacy and public key infrastructure are the fourth commonest theme, each with a proportion at 7%. The blockchain applications allow for end users to authenticate in some way with another entity or service so that they do not need to rely on a vulnerable central server of information. The fifth commonest theme is about Domain Name Systems (DNSs) and how blockchain can effectively host DNS records in a distributed environment to prevent malicious changes and denial of service attacks. The last common themes on our list are related to Wi-Fi, web and malware, each accounting for 3%.

4. Discussion

The initial keyword searches show that there are a substantial number of papers related to blockchain. The technologies of blockchain and truly distributed decentralized systems have only been developed for ten years and are clearly still in their infancy. A sizeable portion of the selected primary studies are experimental proposals or concepts for solutions to today's problems, and they have little quantitative data and few practical applications. Some of the more practical security solutions offered in the remaining primary studies display innovative techniques for solving a

Table 5
Key findings and themes of the primary studies.

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Security Applications
[S1]	Data between users and applications can be secured and remain untampered by being stored and passed through a blockchain. Rather than proof-of-work, trusted nodes are rewarded instead by their level of calculated trust assigned by the network.	Personal Data
[S2]	DNS can be secured with blockchain using proposed "D3NS". Proposal for backwards compatible new DNS.	DNS
[S3]	Proof of concept pseudonymous protocol for secure communications between IoT devices using bitcoin blockchain for case study.	IoT
[S4]	Experimental project for immutable naming and storing of data, called "BlockStack". Recognition for previously utilized Namecoin blockchain not offering security and reliability of bitcoin blockchain.	Data Storage
[S7]	Broad look at benefits of IoT devices utilizing blockchain. For example, IoT devices from one manufacturer are on the same blockchain and then distribute firmware upgrades peer to peer rather than pushing from the center. Recognition of requirement for token. Possible solutions offered.	IoT
[S8]	Proposal for a distributed ledger of Public Key Infrastructure (PKI) to avoid potential failure of central repository of PKI's. Recognition for token. New token named Cecoin proposed.	Public Key Infrastructure
[S9]	Blockchain based system for providing authenticity for Docker images, without relying on central service such as Notary (provides defense against denial of service). Recognition of the necessity of a robust blockchain. Using bitcoin for experiment.	IoT/Docker
[S10]	Bitcoin blockchain-based proposal for securing smart home IoT devices on a local blockchain. Assessment of network overheads when utilizing blockchain.	IoT (Specifically Smart Home)
[S11]	Multi-level network of IoT devices utilizing blockchain. Managing security of the blockchain through communication between layers rather than fully decentralized nodes and miners.	IoT
[S12]	Suggestion for how low-power IoT devices could communicate with a more sufficient gateway to enable node communication on the ethereum blockchain.	IoT
[S13]	Proposal for securely sharing big data and preventing tampering. Utilizes the ethereum blockchain.	Big Data
[S14]	Blockchain based distribution of hashed search indices to allow for keyword searching of encrypted data. Integrity maintained by obtaining value deposit from a joining user and if they act maliciously, this deposit is shared to the rest of the nodes.	Encrypted Data Storage & Searching
[S15]	Proposal for the use of blockchain to secure file sharing between nodes within a Software Defined Network (SDN). Utilizing the ethereum platform.	Networking
[S16]	Securing virtual machines in networked environments utilizing private blockchain; IBM's Hyperledger Fabric demonstrated sufficient properties to allow for the researchers' proposals.	Virtual Machines
[S19]	Proposing "ControlChain", a blockchain based solution for IoT device access control. Utilizing the same principles as the bitcoin blockchain and proposing that multiple blockchains could be used to handle different aspects of the IoT control.	IoT
[S20]	Proposal for "ConsortiumDNS". Furthering the work of BlockStack from Ref. [S8] and dealing with storage limits.	DNS
[S21]	Focusing on IoT data trading, access and privacy. Proposing a blockchain solution for each to provide privacy solutions. Utilizing the ethereum platform.	IoT
[S22]	Presenting a scheme for securing access to Wi-Fi hotspots utilizing the bitcoin blockchain. Users authenticate with credentials that are stored on the blockchain as signed transactions. Digital signatures prove that credentials are held for the access point. Anonymity is provided using existing CoinShuffle protocol.	Wi-Fi
[S24]	Discussion on strengths of blockchain in improving security, particularly with IoT. Highlighting security benefits of IoT supply chain from manufacturer to end-user.	IoT
[S25]	Position paper highlights increasing importance of blockchain application to IoT in homes, battlefields and healthcare. Conceiving a way for IoT to install secure firmware updates.	IoT
[S27]	Proposing a Distributed Ledger Based Access Control (DL-BAC) for web applications. Distributed ledger refers to a generic blockchain similar to bitcoin.	Web Applications
[S29]	Using an MIT research data privacy concept to explore differences between blockchain proof-of-work and proof-of-credibility consensus mechanisms. Nodes are given a score to determine their credibility dependent on number of connections to other trusted nodes.	Data Privacy
[S30]	Proposing their own blockchain for managing Public Key Infrastructure and mining is incentivized not through currency tokens but data payloads labelled *approval*, *auth*, *renew*, *blame*, *ban* and *revoke*, which builds trust across nodes.	Public Key Infrastructure
[S33]	Proposing a blockchain gateway between IoT devices, specifically wearable devices, and their end-users in order to protect data privacy. User device preferences are encrypted and stored on the blockchain for retrievable only by that user.	Data Privacy
[S34]	Utilizes a consortium blockchain, where there are specified *N* members to detect hashed malware on Android devices.	Malware (Android)
[S35]	Provides an application of blockchain in the form of securing historic IoT connections and sessions and detecting malicious behavior. Suggested architecture is that the blockchain protocol sits between the application and transports layers of the network. Utilizing token rewards similar to bitcoin but treating them as units of voting power.	IoT
[S36]	Proposing pricing strategies for blockchain-based distributed peer to peer transactions. Blockchain concepts and incentivization based on bitcoin.	Peer to Peer Data Sharing
[S38]	Substantial review of IoT security and how blockchain could meet the challenges of reducing the existing security threats against such devices. Mentioning ethereum as a potential platform to allow for smart contracts to be developed in endless ways.	IoT
[S39]	Proposal to develop "IoTChain" for utilizing blockchain to allow for secure access and authentication to IoT devices. Evaluation of the feasibility of their proposal was conducted on the ethereum platform. Researchers utilize three full nodes: clients, key servers and authentication servers. The	IoT

(*continued on next page*)

Table 5 (*continued*)

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Security Applications
	latter acts as the miner of the transactions and stores data on the blockchain using either proof-of-work or proof-of-stake consensus mechanisms. For IoTChain the researchers conceptualize their own Proof-of-Possession mechanism.	
[S41]	Thorough review of how blockchain works, current Proof-of-X concepts and their advantages and disadvantages. Discussing useful applications of blockchain with IoT security, for example, access control. Quantifying the risk of selfish mining nodes.	IoT
[S42]	Discussing the security of Virtual Network Functions and associated datacentre management. Proposing a consensus blockchain solution using a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. Hard disk sector size impacts on blockchain information retrieval speeds; larger sectors deliver faster speeds. Experimentation indicated write speeds on the PBFT system are 10–20 times the speed of what would be obtained on ethereum and bitcoin platforms.	Virtual Network Management

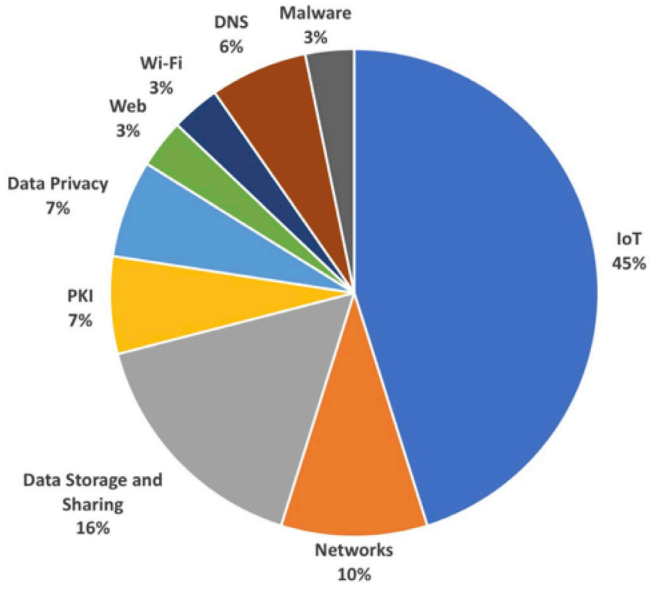

Fig. 3. Chart of themes of primary studies.

wide range of problems concerning data security, mutability and authentication of users. The solutions often depend on a significant change to that system's infrastructure, for example, a change in the network architecture or a reliance on a particular blockchain or platform over a single, centralized server. Due to the labour involved with changing or moving an existing system, it is difficult for some of the practical concepts to be run in an experimental environment for a certain length of time to determine the effectiveness of the blockchain application over conventional security. Notable exceptions included IoTChain [S39] and their experimentation of different consensus mechanisms. They utilized the well-established Ethereum platform to conduct their development and experimental analysis. It seemed that the most practical and ready-to-deploy solutions were those that had been tested on Ethereum or Bitcoin platforms.

The researchers used established platforms, such as Ethereum and Bitcoin for a few different reasons. Ethereum allows for very customisable programming of smart contracts and blockchain applications in the language Solidity, which is not too far removed from Javascript and Python and as such makes it attractive to developers. The Bitcoin blockchain is the most established, invested in and decentralized blockchain [30] available and it provides a useful testbed for experimental concepts. However, it can suffer high latency and fees during times of high network demand with the current protocols being employed [31].

The current proof-of-work mechanisms adopting Ethereum or Bitcoin for achieving consensus can prove to be detrimental to lightweight IoT infrastructures, as they need to use resource intensive processes and networking to hash blocks of transactions to a point where they achieve a predetermined level of difficulty. This mechanism may not be best suited to IoT devices as they are typically designed to have the minimal hardware and power required to perform the task in hand. To address this, several primary studies concerned with IoT have proposed their own solutions, such as the Proof-of-Possession in the IoTChain proposal [S39].

The Proof-of-Credibility blockchain [S29] achieved a consensus by assigning a credibility score to individual nodes [32]. It was proposed in Ref. [S29] that a hybridized blockchain showed that a blockchain utilizing both proof-of-stake and [33] proof-of-credibility could be more resistant to attacks than Proof-of-Work (PoW). This suggests that security does not have to solely rely on PoW mechanisms.

The strength, robustness and trustless appeal of a blockchain come from its "democratic" system [S9]. And due to this, the primary studies in general have showed a recognition that the use of existing blockchains is a necessity. The more participating nodes there are and the better the mechanism to regulate behavior of mining nodes are, the better the decentralization and need for trust of individual nodes will be, which leads to improvements in blockchain security and reliability.

4.1. RQ1: what are the latest blockchain applications focused on security?

It is important to stress that this systematic literature review intends to just focus on *cyber security* applications of blockchain but no other potential or existing applications such as healthcare and logistics.

With that in mind, it should be noted that, during the process of attrition to select the primary studies, the researchers noted that studies regarding finance and healthcare were plentiful. Each of these may have addressed security issues in their own right, however, the selection process concentrated on studies which were focused on security at their cores.

The opportunities to improve the security of IoT are clearly abundant when consideration is given to the fact that almost half of all published cyber security blockchain applications concerned IoT. This may be because of the proliferation of IoT in our homes, military and healthcare, and the ever increasing demand for IoT solutions [34]. Similarly, demand for solutions to security threats to IoT may be spawned from well covered media reports of attacks orchestrated through exploiting such devices [35].

The latest studies suggested that the most security-focused blockchain applications were as follows:

- IoT — authentication of devices to the network and authentication of end users to the devices [S10] [S19] [S21]. Secure deployment of firmware through peer-to-peer propagation of updates [S7] [S24] [S25]. Threat detection and malware prevention [S34] [S35].
- Data storage and sharing — ensuring that data stored in the cloud remains resistant to unauthorized change, that hash lists allow for searching of data which can be maintained and stored securely, and that data exchanged can be verified as being the same from dispatch to receipt [S4] [S13] [S14].
- Network security — due to increasingly utilized visualized machines, software-defined networks and the use of containers for application deployment, blockchain allows for authentication critical data to be stored in a decentralized and robust manner [S15] [S16] [S42].

- Private user data — including end user settings for wearable Bluetooth devices and the protection of personal identifiable information being exchanged with other parties [S29] [S33].
- Navigation and utility of the World Wide Web — ensuring the validity of wireless Internet access points connected to Ref. [S22], navigating to the correct web page through accurate DNS records [S2] [S20], safely utilizing web applications [S27] and communicating with others through secure, encrypted methods [S8] [S39].

4.2. RQ2: how is blockchain used to improve cyber security?

Blockchain and the related technologies offer no silver bullet for cyber security issues. If anything, they simply bolster existing efforts for secure networks, communications and data. Blockchain utilizes encryption and hashing to store immutable records and many of the existing cyber security solutions utilize very similar technology as well. The majority of existing security measures rely on a single trusted authority to verify information or store encrypted data. This leaves the system vulnerable to attack, and many bad actors could focus their efforts on a single target to commit denial of service attacks, inject malicious information and extort data through theft or blackmail. Blockchains have the upper hand over current security measures in that true blockchains are decentralized and do not require the authority or trust of an individual member of the group or network. The system does not require trust because each node, or member, has a complete copy of all the historic information available and just through achieving consensus of the majority will more data be added to the chain of previous information. As outlined in other sections of this paper, this is achieved in many different ways, but the bottom line is this: many members of a group who have access to the same information will be able to secure that group far better than a group made up of one leader and a host of members who rely on the leader for their information, particularly when bad actors could come in the form of group members or even as the leaders themselves.

Based on the most security-focused blockchain applications identified in RQ1, we discuss how blockchain was applied to improve cyber security in IoT, data storage and sharing, network security, private user data, navigation and utility of World Wide Web:

- IoT — main private blockchains (such as Hyperledger Fabric) are applied to implement permitted access control for devices (nodes) in the network [S10] [S19] [S21] to securely track data management and prevent any malicious access. In another class of work, blockchain is used to improve the security of firmware deployment through peer-to-peer propagation of updates [S7] [S24] [S25] to provide IoT device identification, authentication and seamless secure data transfer. An application of blockchain in the form of securing historic IoT connections and sessions and detecting malicious behavior is provided in Ref. [S34] [S35]. In these works, the suggested architecture is that: the blockchain protocol sits between the application and transport layers of the network, and utilizes token rewards similar to bitcoin but treats them as units of voting power.
- Data storage and sharing — both public and private distributed ledgers are used to eliminate a single source of failure within a given storage ecosystem, protecting its data from tampering. That is, blockchain helps to ensure that data stored in the cloud remains resistant to unauthorized changes, hash lists allow for searching of data that can be maintained and stored securely, and data exchanged can be verified as being the same from dispatch to receipt [S4] [S13] [S14]. In a nutshell, blockchain improves data storage and sharing security by creating a decentralized network that uses client-side encryption in which data owners will have full traceable control of their data.
- Network security — the majority of works in this category use blockchains to improve Software Defined Networks (SDNs) and use containers for authentication critical data to be stored in a decentralized and robust manner [S15] [S16] [S42]. In such works, blockchain-enabled architecture of SDN controllers using a cluster structure is used. The architecture uses public and private blockchains for P2P communication between nodes in the network and SDN controllers to make the blockchain appropriate for addressing network security issues.
- Private user data — comparing with other categories, the application of blockchain for improving data privacy has been less discussed in the literature. The reason could be due to the irreversibility nature of blockchain (everybody has a copy of the ledger), which makes it hard to be used for privacy purposes, particularly in data protection. In current approaches [S29] [S33], typical user device preferences are encrypted and stored on the blockchain to be retrieved only by that user. Also, they explore differences between blockchain PoW and proof-of-credibility consensus mechanisms, where nodes are given a score to determine their credibility dependent on the number of connections to other trusted nodes.
- Navigation and utility of the World Wide Web — Blockchain is used to improve the validity of the wireless Internet access points connected to Ref. [S22], by storing and monitoring the access control data on a local ledger. Also, blockchain is used to help navigating to the correct web page through accurate DNS records [S2] [S20], safely utilizing web applications [S27] and communicating with others through secure, encrypted methods [S8] [S39]. To implement these solutions, the idea of consortium blockchain has been used, in which the consensus process is controlled by a preselected set of nodes in the network.

4.3. RQ3: what methods are available for blockchain solutions to manage security without requiring a cryptocurrency token?

A substantial number of primary studies accept that token incentivization of miners [36,37], such as in the reward of bitcoin, is a well-established and robust method for achieving consensus of the longest chain [S8,S9,S13,S14,S21,S22,S29,S30,S36,S38]. That says, novel approaches to token distribution suggest that there are options outside of paying miners currency tokens [S30]; tokens hold value in allowing recipient nodes more voting power; and the more a node contributes to mining, the more voting power it will have over the process of the chain going forward.

The proposal of [S7] suggests the possibility of each IoT automatically charging other devices a token amount for pushing firmware upgrade.

IBM's Hyperledger Fabric [S16] utilizes their own chaincode to secure transactions within the blockchain and achieve consensus. Tokens of currency are optional in the application.

One study [S11] even explores the possibility of relying on multiple blockchain layers for trust and authentication of transaction between hierarchical layers.

Some of the studies propose blockchain as a particular security solution but make no reference to whether an existing blockchain should be used or a new one should be developed. Equally, some papers avoid mentioning of the use of tokens entirely. [S25] is an example that proposes some interesting security solutions without specifying particulars in relation to the blockchain itself.

There is no evidence available in the primary studies to suggest that any system other than a PoW consensus mechanism awarding miners a token of value has been able to scale securely with the levels of network traffic the Bitcoin and Ethereum networks are subjected to.

5. Future research directions of blockchain cyber security

Based on the results of this survey and our observations, we present the following research directions of blockchain for cyber security that worth further investigation:

Blockchain for IoT security: security in IoT networks has been claimed as a pressing need of the industry and has gotten the utmost priority for improvement and enforcement, despite current research

shows the fact that almost every article on blockchain cyber security in the literature points out that the security of IoT systems could be revitalized if it is supported with blockchain technology. Yet, little is known and discussed about factors related to decisions about and feasibility to adopt this technology, and how and where it can be systematically put into use to remedy current IoT security risks/threats in a clear context, allowing for the imagination and then creation of future vectors in this specific domain. Thus, it is important for future research to develop some quantifiable guidelines and tools that can help fill this blank in the literature. Furthermore, proposing lightweight blockchain-based solutions for resource constrained IoT devices (running on the edge of network) could be another area of further research.

Blockchain for AI data security: in modern computing ecosystem, data is captured from various sources and transmitted among devices (e.g., IoT) through the networks. Artificial Intelligence (AI) and its derivatives have been used as powerful tools to analyze and process the captured data to achieve effective reasoning in addressing security issues. Although AI is powerful and can be engaged with distributed computing, deceptive analysis would be generated when corrupted or dishonest data is intentionally or unintentionally integrated by a malicious third-party based on adversarial inputs. Blockchain as a popular ledger technology has the potential to be leveraged in different areas of the cyber space. Blockchain attempts to reduce transaction risks and financial fraud, owing to its characteristics such as decentralization, verifiability and immutability for ensuring the authenticity, reliability and integrity of data. When the cedibility and reliability of data can be ensured, more secure and trustworthy outcomes can be produced by AI. A future research direction could be the exploration of blockchain for the security of AI data in B2B and M2M environments.

Sidechain security: The sidechain technology [38,39] has most recently emerged as a separate chain attached to the main chain, in parallel with transactions, to alleviate the challenges (mainly performance) related to main blockchains. In the near future, we envision a distributed multi-blockchain ecosystem, in which different main chains and sidechains work to collaborate with each other in various scenarios. However, the practical aspects of sidechains remain poorly understood, and many fundamental research questions are still to be debated. For example,

1. How do these sidechains establish security defaults to prevent attacks?
2. How could blockchain customers be assured of the integrity and confidentiality of their data through sidechains?

Answering these questions is vital for the future investigations to have a more sustained blockchain cyber security research [40].

Releasing open-source software and dataset, and engaging with community: blockchain cyber security research is fractured between academia and the developer community. To bridge this gap, efforts are required by academic researchers to release more open-source applications, tools, and dataset to be engaged by the industry community and start-ups. In fact, there is a large community who are interested in blockchain analysis (evidenced by the popularity of open-source tools such as bitcoin-abe [41] or BlockBench [42] for instance), so academic researchers should actively involve the community in the development, validation, and maintenance of their research results.

6. Conclusion and future work

This research has identified available recent research on how blockchain solutions can contribute to cyber security problems. The initial keyword searches for this research and current media reports [43] highlight blockchain as a standalone technology that brings with it an exorbitant array of possible solutions for finance, logistics, healthcare and cyber security. This research has focused solely on cyber security. Undoubtedly, there are worthy applications for blockchain, however, a decentralized, trustless system cannot by itself solve all problems one may uncover in the field of cyber security. Blockchain applications for cyber security have evolved and bolstered the existing efforts to enhance security and to deter malicious actors.

This research highlights opportunities available for future research to be conducted in areas of cyber security outside the realm of IoT. As the World Wide Web moves towards a mass adoption of *https* encryption and the end users are increasingly using some forms of encryption for everyday communication [44], there is an ever increasing need to securely manage the surrounding cryptography and certification schemes.

Potential research agenda 1: the research concerning IoT security using blockchain applications often made comment on network latency and power consumption to maintain the distributed network. For the purpose of this paper, it was not possible to quantify such data due to the variability in solutions employed by each group of researchers. Future work could include an *assessment of network latency, power consumption and data packet flows of blockchain-based IoT networks*, and standardization of data presented in the primary studies.

Potential research agenda 2: several of the primary studies [20,43,45] opted to use the Ethereum platform and smart contracts to find solutions to their security problems. Further future work could include a *review of the various ways in which Ethereum and/or other permissionless/-permissioned blockchain platforms have been, or can be, used to develop innovative cyber security solutions*.

Potential research agenda 3: The more distributed, investable and decentralized cryptocurrency tokens have the more robust and secure blockchains to support the applications proposed by researchers, and for that reason, cryptocurrencies will grow alongside the adoption of blockchain security technologies. While Bitcoin remains the most successful decentralized cryptocurrency with the lengthiest, most robust blockchain, there has been increasing interest in *designing a forensically-friendly cryptocurrency architecture*, which will facilitate lawful (forensic) investigation of suspicious cryptocurrency transactions, such as those used in cybercriminal activities (e.g., ransomware and terrorism financing).

Potential research agenda 4: It is known that permissionless blockchain frameworks, such as Bitcoin and Ethereum, generally take minutes to reach consensus. However, such latency may not be acceptable for time and delay-sensitive applications such as Internet of Battlefield Things (IoBT). Hence, a potential research agenda is to *design blockchain-based solutions, for example, in combination with hardware-based approaches, which have reduced latency and are therefore suited for time and delay-sensitive applications*.

Declarations of interest

None.

Acknowledgement

K.-K. R. Choo is funded by the Cloud Technology Endowed Professorship.

References

[1] T. Aste, P. Tasca, T. Di Matteo, Blockchain technologies: the foreseeable impact on society and industry, Computer 50 (9) (2017) 18–28.
[2] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), 2017, p. 557564.
[3] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008. Www.Bitcoin.Org. https://bitcoin.org/bitcoin.pdf [Online]. Available:.
[4] G. Wood, Ethereum: a Secure Decentralized Generalized Transaction Ledger Yellow Paper, Ethereum Project. Yellow Pap., 2014, p. 132.
[5] V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Etherum, 2014 [Online]. Available: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf.

[6] E. Androulaki, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 30:130:15.
[7] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, H. Kai, A multiple blockchains architecture on inter-blockchain communication, in: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018, p. 139145.
[8] D. Miller, Blockchain and the internet of Things in the industrial sector, IT Professional 20 (3) (2018) 1518.
[9] J. Fiaidhi, S. Mohammed, S. Mohammed, EDI with blockchain as an enabler for extreme automation, IT Professional 20 (4) (2018) 6672.
[10] M. Samaniego, R. Deters, Blockchain as a service for IoT, in: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, p. 433436.
[11] M.E. Peck, Blockchains: How They Work and Why Theyll Change the World, IEEE Spectrum, 2017.
[12] Bitcoin Could Be Accepted at 300,000 Japanese Stores in, 2017.
[13] S. Chen, C.Y.-H. Chen, W.K. Hrdle, T.M. Lee, B. Ong, Chapter 8 - Econometric Analysis of a Cryptocurrency Index for Portfolio Investment BT - Handbook of Blockchain, Digital Finance, and Inclusion, vol. 1, Academic Press, 2018, p. 175206.
[14] K.-K.R. Choo, Cryptocurrency and virtual currency, in: Handbook of Digital Currency, Elsevier, 2015, p. 283307.
[15] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence, in: IEEE Trans. Emerg. Top. Comput., 2017, p. 11.
[16] O. Osanaiye, H. Cai, K.-K.R. Choo, A. Dehghantanha, Z. Xu, M. Dlodlo, Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing, EURASIP J. Wirel. Commun. Netw. (1) (2016) 2016.
[17] Five ways banks are using blockchain.
[18] How Blockchain Will Transform the Supply Chain and Logistics Industry.
[19] K. Megget, Securing the supply chain, 2018.
[20] R.M. Parizi, Amritraj, A. Dehghantanha, Smart contract programming languages on blockchains: an empirical evaluation of usability and security, in: International Confernce on Blockchain, Seattle, USA, 2018, pp. 75–91.
[21] Smart Contracts on the Blockchain: Can Businesses Reap the Benefits.
[22] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: a state of the art survey, in: IEEE Communications Surveys & Tutorials, 2018, https://doi.org/10.1109/COMST.2018.2863956.
[23] Convergence of Blockchain and Cybersecurity - IBM Government Industry Blog.
[24] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on Blockchain technology? - a systematic review, PLoS One 11 (10) (2016) 127.
[25] M. Conoscenti, A. Vetr, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, p. 16.
[26] S. Seebacher, R. Schritz, Blockchain technology as an enabler of service systems: a structured literature review, in: Exploring Services Science, 2017, p. 1223.
[27] B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, in: Engineering, vol. 2, 2007, p. 1051.
[28] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proc. 18th Int. Conf. Eval. Assess. Softw. Eng. - EASE 14, 2014, p. 110.
[29] S. Hosseini, B. Turhan, D. Gunarathna, A systematic literature review and meta-analysis on cross project defect prediction, IEEE Trans. Softw. Eng. 45 (2) (1 Feb 2019) 111–147.
[30] Bitcoin price, charts, market cap, and other metrics — CoinMarketCap.
[31] What are Blockchains Issues and Limitations? - CoinDesk.
[32] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: securing a blockchain applied to smart contracts, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016, p. 467468.
[33] The challenge of providing heavyweight security for lightweight IoT devices — Mbed Blog.
[34] Global Cellular IoT Market (2017-2023): Increasing Demand for Long Range Connectivity - Research and Markets — Business Wire.
[35] IoT Botnets & DDoS Attacks: What you need to know.
[36] R.M. Parizi, A. Dehghantanha, On the understanding of gamification in blockchain systems, in: 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, 2018, pp. 214–219.
[37] R.M. Parizi, On the gamification of human-centric traceability tasks in software testing and coding, in: 2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA), Towson, MD, 2016, pp. 193–200.
[38] A. Back, et al., Enabling blockchain innovations with pegged sidechains [Online]. Available: http://www.blockstream.com/sidechains.pdf, 2014.
[39] P. Robinson, Requirements for Ethereum Private Sidechains, arXiv Prepr. arXiv1806.09834, 2018.
[40] Q. Zhang, R.M. Parizi, K.K.R. Choo, A Pentagon of Considerations Towards More Secure Blockchains, IEEE Blockchain Technical Briefs, 2018.
[41] Bitcoin-abe, https://github.com/bitcoin-abe/bitcoin-abe.
[42] T.T.A. Dinh, J. Wang, G. Chen, R. Liu, B.C. Ooi, K.-L. Tan, BLOCKBENCH: a framework for analyzing private blockchains, in: Proceedings of the 2017 ACM International Conference on Management of Data, 2017, p. 10851100.
[43] Blockchain is this year's buzzword - but can it outlive the hype? — Technology — The Guardian.
[44] Use of WhatsApp in NHS 'widespread', say doctors - BBC News.
[45] R.M. Parizi, A. Dehghantanha, K.K.R. Choo, A. Singh, Empirical vulnerability analysis of automated smart contracts security testing on blockchains, in: 28th ACM Annual International Conference on Computer Science and Software Engineering (CASCON18), IBM, Canada, 2018, pp. 103–113.

Primary Studies

[S1] G. Zyskind, A.S. Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015.
[S2] B. Benshoof, A. Rosen, A.G. Bourgeois, R.W. Harrison, Distributed decentralized domain name service, in: Proc. - 2016 IEEE 30th Int. Parallel Distrib. Process. Symp. IPDPS 2016, 2016, p. 12791287.
[S3] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, FairAccess: a new blockchain-based access control framework for the Internet of Things, Secur. Commun. Networks 9 (18) (2016) 59435964.
[S4] M. Ali, et al., Blockstack: A global naming and storage system secured by blockchains, in: USENIX Annu. Tech. Conf., 2016, p. 181194.
[S5] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and solutions, 2016.
[S6] J. Filipek, L. Hudec, Advances in distributed security for mobile ad hoc networks, in: Proc. 17th Int. Conf. Comput. Syst. Technol. 2016 - CompSysTech 16, no. June, 2016, p. 8996.
[S7] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, IEEE Access, 4, 2016, p. 22922303.
[S8] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, W. Shi, Cecoin: A decentralized PKI mitigating MitM attacks, Futur. Gener. Comput. Syst. (2017).
[S9] Q. Xu, C. Jin, M.F.B.M. Rasid, B. Veeravalli, K.M.M. Aung, Blockchain-based decentralized content trust for docker images, Multimed. Tools Appl. 126 (2017).
[S10] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work., PerCom Work., 2017, p. 618623.
[S11] C. Li, L.J. Zhang, A blockchain based new secure multi-layer network model for internet of things, in: Proc. - 2017 IEEE 2nd Int. Congr. Internet Things, ICIOT 2017, 2017, p. 3341.
[S12] K.R. zylmaz, A. Yurdakul, Integrating low-power IoT devices to a blockchain-based infrastructure, in: Proc. Thirteen. ACM Int. Conf. Embed. Softw. 2017 Companion - EMSOFT 17, 2017, p. 12.
[S13] L. Yue, H. Junqin, Q. Shengzhi, W. Ruijin, Big data model of security sharing based on blockchain, in: 2017 3rd Int. Conf. Big Data Comput. Commun., 2017, p. 117121.
[S14] C. Cai, X. Yuan, C. Wang, Hardening distributed and encrypted keyword search via blockchain, in: 2017 IEEE Symp. Privacy-Aware Comput., 2017, p. 119128.
[S15] S. Ram Basnet, S. Shakya, BSS: Blockchain Security over Software Defined Network, Ieee Iccca, 2017, p. 720725.
[S16] N. Bozic, G. Pujolle, S. Secci, Securing virtual machine orchestration with blockchains, in: 2017 1st Cyber Secur. Netw. Conf., 2017, p. 18.
[S17] F. Dai, Y. Shi, N. Meng, L. Wei, Z. Ye, From Bitcoin to cybersecurity: a comparative study of blockchain application and security issues, in: 2017 4th Int. Conf. Syst. Informatics, no. 61471129, 2017, p. 975979.
[S18] N. Rifi, E. Rachkidi, N. Agoulmine, N.C. Taher, Towards using blockchain technology for IoT data access protection, in: 2017 IEEE 17th Int. Conf. Ubiquitous Wirel. Broadband, 2017, p. 15.
[S19] O.J.A. Pinno, A.R.A. Gregio, L.C.E. De Bona, Controlchain: Blockchain as a central enabler for access control authorizations in the IoT, in: GLOBECOM 2017 - 2017 IEEE Glob. Commun. Conf., 2017, p. 16.
[S20] X. Wang, K. Li, H. Li, Y. Li, Z. Liang, ConsortiumDNS: A distributed domain name service based on consortium chain, in: 2017 IEEE 19th Int. Conf. High Perform. Comput. Commun. IEEE 15th Int. Conf. Smart City; IEEE 3rd Int. Conf. Data Sci. Syst., 2017, p. 617620.
[S21] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, L. Xie, A decentralized solution for IoT data trusted exchange based-on blockchain, in: 2017 3rd IEEE Int. Conf. Comput. Commun., 2017, p. 11801184.
[S22] Y. Niu, L. Wei, C. Zhang, J. Liu, Y. Fang, An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain, in: 2017 IEEE/CIC Int. Conf. Commun. China, no. Iccc, 2017, p. 16.
[S23] H. Gupta, A security framework for IOT devices against wireless threats, 2017.
[S24] N. Kshetri, Blockchains roles in strengthening cybersecurity and protecting privacy, Telecomm. Policy 41 (10) (2017) 10271038.
[S25] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to internet of things security: A position paper, Digit. Commun. Networks 4 (3) (August 2018) 149–160 .
[S26] F. Buccafurri, G. Lax, S. Nicolazzo, A. Nocera, Overcoming limits of blockchain for IoT applications, in: Proc. 12th Int. Conf. Availability, Reliab. Secur. - ARES 17, 2017, p. 16.
[S27] L. Xu, L. Chen, N. Shah, Z. Gao, Y. Lu, W. Shi, DL-BAC: Distributed ledger based access control for web applications, in: Proc. 26th Int. Conf. World Wide Web Companion, 2017, p. 14451450.
[S28] J. Spasovski, P. Eklund, Proof of stake blockchain, in: Proc. 9th Int. Conf. Manag. Digit. Ecosyst. - MEDES 17, no. November, 2017, p. 251258.
[S29] D. Fu, F. Liri, Blockchain-based trusted computing in social network, in: 2016 2nd IEEE Int. Conf. Comput. Commun. ICCC 2016 - Proc., 2017, p. 1922.

[S30] A. Moinet, B. Darties, J.-L. Baril, Blockchain based trust & authentication for decentralized sensor networks, 2017, p. 12.
[S31] D. Li, Z. Cai, L. Deng, X. Yao, H.H. Wang, Information security model of block chain based on intrusion sensing in the IoT environment, Cluster Comput. 1 (2018) 118.
[S32] Y. Zhao, Y. Li, Q. Mu, B. Yang, Y. Yu, Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems, IEEE Access 6 (2018) 1229512303.
[S33] S.C. Cha, J.F. Chen, C. Su, K.H. Yeh, A blockchain connected gateway for BLE-based devices in the internet of things, IEEE Access 3536 (2018) no. c.
[S34] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, Z. Wang, Consortium blockchain-based malware detection in mobile devices, IEEE Access 6 (2018) 1211812128.
[S35] Y. Gupta, R. Shorey, D. Kulkarni, J. Tew, The applicability of blockchain in the Internet of Things, in: 2018 10th Int. Conf. Commun. Syst. Networks, 2018, p. 561564.
[S36] Y. He, H. Li, X. Cheng, Y.A.N. Liu, C. Yang, L. Sun, A blockchain based truthful incentive mechanism for distributed P2P, IEEE Access xx (2018) no. c.
[S37] J.H. Jeon, K. Kim, J. Kim, Block chain based data security enhanced IoT Server Platform, 2018, p. 941944.
[S38] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018) 395411.
[S39] O. Alphand, et al., IoTChain: A Blockchain Security Architecture for the Internet of Things, in: IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6 .
[S40] C. Dukkipati, Decentralized , BlockChain Based Access Control Framework for the Heterogeneous Internet of Things, 2018, p. 6169.
[S41] E.F. Jesus, V.R.L. Chicarino, C.V.N. De Albuquerque, A.A.D.A. Rocha, A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack, 2018, 2018.
[S42] I.D. Alvarenga, Securing Configuration, Management And Migration Of Virtual Network Functions Using Blockchain, 2018.