Blockchain-based Application Security Risks: A Systematic Literature Review

Mubashar Iqbal[0000-0003-0543-613X] and
Raimundas Matulevičius[0000-0002-1829-4794]

Institute of Computer Science, University of Tartu, Tartu, Estonia
{mubashar.iqbal,raimundas.matulevicius}@ut.ee

Abstract. Although the blockchain-based applications are considered to be less vulnerable due to the nature of the distributed ledger, they did not become the *silver bullet* with respect to securing the information against different security risks. In this paper, we present a literature review on the security risks that can be mitigated by introducing the blockchain technology, and on the security risks that are identified in the blockchain-based applications. In addition, we highlight the application and technology domains where these security risks are observed. The results of this study could be seen as a preliminary checklist of security risks when implementing blockchain-based applications.

Keywords: Blockchain · Blockchain-based applications · Decentralized applications · Security risks

1 Introduction

Blockchain is a distributed immutable ledger technology [34]. It gives participants an ability to share a ledger by peer-to-peer replication and updates every time when a transaction occurs. A ledger contains a certain and verifiable record of every single transaction ever made [22]. Security engineering is concerned with lowering the risk of intentional unauthorized harm to valuable assets to that level which is acceptable to the systems stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks [14]. Security plays an important role in blockchain-based applications. Those applications are acknowledged to be less vulnerable because the use of a decentralized consensus paradigm to validate the transactional information. They also backed by cryptography technology. However, the blockchain technology is continuously penetrating various fields and the involvement of the monetary assets raised the security concerns, mainly when the attackers stole the monetary assets or damage the system. For example, the reentrancy attack on the Ethereum based decentralized autonomous organization (DAO) smart contracts when an adversary gained control on \$60 million Ethers [4, 26].

Blockchain technology promises to overcome the security challenges, enhance the data integrity and to transform the transacting process into a decentralized, transparent and immutable manner. The recent progression of blockchain technology captured the interest of various sectors to transform their business processes by using blockchain-based applications. Hence, the security challenges are debatable and there is no comprehensive (or standardized) overview of security risks which can potentially damage the blockchain-based applications. There exist few studies reporting on security challenges in the blockchain platforms [4, 24], but there is still a lack of focus on the blockchain-based applications security.

In this paper, we present a systematic literature review (SLR) following the guidelines of [20]. Our research objectives are twofold. Firstly, we explain what security risks of centralized applications are mitigated by introducing blockchain-based applications. Secondly, we report the security risks of the blockchain-based applications which appear after introducing the blockchain technology. The main contributions of our study are: (1) a list of security risks in the blockchain-based applications which mitigate or inherit by incorporating the blockchain technology/platform, (2) aggregate a list of possible countermeasures and (3) an overview of the prominent research domains which are nourishing by the blockchain. The results of this study could be seen as a preliminary checklist of security risks when implementing blockchain-based applications.

The rest of the paper is structured as follows: Section 2 provides an overview of the blockchain and related work. Section 3 presents the contributions which explain the SLR process and Section 4 discuss its results. In Section 5, conclusion and future research directions are conferred.

2 Background

In this section, first, we introduce the blockchain technology. Second, we present an overview of related work.

2.1 Overview of Blockchain Technology

Blockchain forms a chain by a sequence of blocks that replicates over a peer-to-peer (P2P) network. In the blockchain, each block is attached to the previous block by a cryptographic hash, a block contains block header and a list of transactions as a Merkle tree. Blockchain is classified as a permissionless or permissioned [31]. In permissionless blockchain, anyone can join or leave the network and transactions are publicly available. In permissioned blockchain only predefined verified nodes can join the network and transactions visibility is restricted [2, 31].

In the blockchain, a smart contract (SC) is a computer program [4, 7] which constitutes a digital contract to store data and to execute functions [28] when certain conditions are met. In the ethereum platform, developers use *Solidity* programming language to write a smart contract and to build decentralized applications [7]. In Hyperledger Fabric, a smart contract is called chaincode. Similarly, other blockchain platforms introduce smart contracts to perform contractual agreements in a digital realm. The smart contracts are the high-level programming language-based programs and those can be error-prone where security flaws could be introduced (e.g. the reentrancy bug [26]).

Blockchain eliminates the trusted intermediary and follows the decentralized consensus mechanism to validate the transactional information. Different blockchains use various consensus mechanism. Proof of Work (PoW) is a widely used computational rich energy-waste consensus strategy where special nodes called miners validate transactions by solving the crypto puzzle. Proof of Stake (PoS) is an energy-efficient consensus strategy [42] where miners become validators [12] and lock a certain amount of cryptocurrency to show ownership to participate in the consensus process. There are other consensus mechanisms, for example, Delegated Proof of Stake (DPoS), Proof of Authority (PoA), Proof of Reputation (PoR) and Proof of Spacetime (PoSt).

The number of blockchain platforms is rapidly growing and thus, security becomes an important factor of the successful blockchain-based applications. In this paper, we focus on three frequently used blockchain platforms (Bitcoin, Ethereum, Hyperledger fabric). In addition, we also look at customised permissioned & permissionless platforms (see Table 3). Our goal is to learn which security risks and threats are considered in the applications of these platforms.

2.2 Related Work

There exist a few surveys, which consider blockchain platforms security risks. For instance, Li et al. [24] overview the security attacks on the blockchain platforms & summarise the security enhancements. In our work, we consider the security risks on the *blockchain-based applications* and their countermeasures.

Another related study [4] is conducted on Ethereum *smart contracts* security. It reports on the major security attacks and presents a taxonomy of common programming pitfalls, which could result in different vulnerabilities. This study focuses on the security risks in the Ethereum smart contracts, further investigation is required to explore possible security risks in *smart contracts based decentralized applications* and their viable countermeasures.

The main attributes of blockchain are integrity, reliability and security [21] which are also important in the IoT systems. The conventional approaches and reference frameworks of IoT network implementation are still unable to fulfil the requirements of security [19]. Minhaj et al. [19] survey major security issues of IoT and discuss different countermeasures along with the blockchain solution. This study, however, does not detail security challenges in the *blockchain-based IoT applications*. Our study reviews the different blockchain-based IoT applications, discusses their security risks and potential countermeasures.

3 Survey Settings

In [20], a comprehensive approach is presented to perform a SLR. In this section, we apply it to conduct a SLR on the security risks in the blockchain-based applications.

3.1 Review Method

In order to achieve the objectives of this study, we consider four research questions: (i) What are the domains where blockchain solutions are applied? (ii) What security risks are mitigated by the blockchain solutions? (iii) What do security risks appear within the blockchain-based applications? (iv) What are the countermeasures to mitigate security risks in the blockchain-based applications?

Selection of databases. The selection of electronic databases and literature search is carried out by consulting with the experts of software security. Literature studies are collected from ACM digital library, IEEE digital library, ScienceDirect, SpringerLink and Scopus. The **search queries** (including some alternative terms and synonyms) are formulated as follows:

Blockchain applications security (risks, threats, gaps, issues, challenges), permissioned blockchain applications security, permissionless blockchain applications security, public blockchain applications security

Relevance and Quality Assessment. The inclusion and exclusion criteria listed in Table 1. In this study, we only include the peer-reviewed literature because most of the grey literature is based on assumptions, abstract concepts and prejudices towards the security of their applications. Based on these shreds of evidence the grey literature could lead to the publication bias and erroneous results, so in order to eliminate these concerns only peer-reviewed literature is considered.

Table 1. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Only the peer-reviewed literature	Literature that does not subject to peer review
Literature studies that discuss security risks in the blockchain-based applications	Grey literature or informal studies with no concrete evidence

The selection of the studies was made after reading the paper *title, abstract, introduction and conclusion* sections. Finally, following the quality guidelines of [20] and research scope of our study we have assessed the quality of studies using the following questions:

- Are the goals and purpose of a study is clearly stated?
- Is the study describes security risks on the blockchain-based applications?
- Is the study provide the countermeasures to mitigate security risks?
- Is the study answered the defined research questions?
- How well the research results are presented?

The answers to the above questions are scored as follows: 1=Fully satisfy, 0.5=Partially satisfy, 0=Not satisfy. The studies with 2.5 or more points are included.

3.2 Screening Results

Table 2. Literature studies.

Database	Total	Excl.	Incl.
ACM	21	11	10
IEEE	31	9	22
ScienceDirect	22	15	7
SpringerLink	23	12	11
Scopus	44	26	18
Total	141	73	68

Table 2 presents the screening results. Initially, a total of 141 studies was collected. Later 73 studies were excluded by applying inclusion/exclusion and quality assessment criteria. Finally, 68 studies remained[1]. The extracted information outlines the study identification, research problem, security risks and countermeasures.

4 Results and discussion

Table 3. Statistics of literature studies as per year.

	Permissionless			Permissioned			
	Bitcoin	Ethereum	CPL	HLF	CP	Generic	Total
2016	2	0	0	0	0	0	2
2017	7	3	8	1	2	1	22
2018	9	15	3	8	8	1	44
Total	18	18	11	9	10	2	68

In this section, we present the SLR results. Table 3 shows how the field of blockchain-based applications is emerging every year. We observe that *Ethereum-based* applications are gaining popularity among others. Also, permissioned blockchain platforms (*Hyperledger Fabric (HLF)* & *Customised Permissioned (CP)*) are arising because of those support various industry-based use cases beyond cryptocurrencies. Practitioners also presented various *Customised Permissionless (CPL)* platforms to achieve customised tasks and to overcome the limitations of other platforms. The term *Generic* refers to studies where the blockchain type and platform is not mentioned.

4.1 Applications Domains

Table 4 presents the quantity of *applications domains & technology solutions* based on the different blockchain platforms. It shows *Healthcare* is mostly studied

Table 4. Research areas based on different blockchain platforms.

	Permissionless			Permissioned			
	Bitcoin	Ethereum	CPL	HLF	CP	Generic	Total
Applications domains where blockchain is used.							
Healthcare	0	3	1	2	4	1	11
Resource monitoring & Digital rights management	1	3	2	0	2	1	9
Financial	2	1	1	1	0	0	5
Smart vehicles	1	0	1	1	2	0	5
Voting	1	1	0	2	0	0	4
Technology solutions where blockchain is used.							
Security layer	6	7	1	0	1	0	15
IoT	2	2	1	2	2	0	9
Total	13	17	7	8	11	2	58

application domain and *security layer* as a technology solution. Also, it indicates that Ethereum is widely used blockchain platform for building the decentralized applications.

[1] Here is a list of these SLR studies: http://datadoi.ut.ee/handle/33/89

4.2 Security Risks

Security risks result in harm to the system and its components [18]. In our study, the identified security risks are classified into two categories. (i) Security risks which are mitigated by introducing the blockchain-based applications (see Table 5), and (ii) Security risks which appear within the blockchain-based applications (see Table 6). Table 5 presents the most common security risks which show that the researchers are utilizing the blockchain-based applications to overcome the limitations of centralized applications. For example, *data tampering attack* is mitigated in *Healthcare* applications and DDoS attack/Single point failure is resisted by decentralized distributed property of blockchain.

Table 5. Security risks which are mitigated by introducing blockchain applications.

	Permissionless			Permissioned			
	Bitcoin	Ethereum	CPL	HFL	CP	Generic	Total
Data tampering attack	7	8	4	7	5	1	32
DoS/DDoS attack	7	7	5	3	2	1	25
MitM attack	3	6	2	2	0	1	14
Identity theft/Hijacking	1	0	3	0	0	1	5
Spoofing attack	2	0	1	0	1	0	4
Other risks/threats	6	4	2	1	2	2	17
Total	26	25	17	13	10	6	97

In addition to risks in Table 5, other risks (found once or twice in the studies) are: Side-channel attack, Impersonation attack, Phishing attack, Password attack, Cache poisoning, Arbitrary attack, Dropping attack, Appending attack, Authentication attack, Signature forgery attack, Keyword guess attack, Chosen message attack, Audit server attack, Inference attack, Binding attack and Bleichenbach-style attack

Table 6 represents the most common security risks which appear within the blockchain-based applications after introducing the blockchain technology. The table indicates the security risks, which have a high probability to make the blockchain-based applications vulnerable to attack.

Table 6. Security risks which appear within the blockchain applications.

	Permissionless			Permissioned			
	Bitcoin	Ethereum	CPL	HLF	CP	Generic	Total
Sybil attack	5	1	1	4	1	1	13
Double spending attack	4	1	2	2	0	1	10
51% attack	3	3	1	0	0	1	8
Deanonymization attack	2	1	3	0	0	1	7
Replay attack	2	4	1	0	0	0	7
Quantum computing threat	0	1	1	2	0	1	5
Selfish mining attack	1	0	2	1	0	0	4
SC reentrancy attack	0	2	0	0	0	1	3
Other risks/threats	6	1	6	3	1	3	20
Total	23	14	17	12	2	9	77

Hence the *Sybil attack*, *Double spending attack* and *51% attack* are the most appeared security risks after incorporating the blockchain technology. Other security risks which are appeared once or twice in the studies are: Eclipse attack, BWH attack, 25% attack, Stake grinding attack, Block Discarding attack, Difficulty Raising attack, Pool-hopping attack, Node masquerading attack, Timestamp attack, Balance attack, Signature forgery attack, Confidentiality attack, Private keys compromise, Overspending attack, Collusion attack and Illegal activities.

In Table 7 we encompass the security risks along with the blockchain-based applications research areas to show which security risks are more frequently occurring on different blockchain-based applications. Most frequently the security risks expose in *Resource monitoring and digital rights management* applications, followed by the *Financial*, *Healthcare*, *Smart vehicles* and *Voting* applications. Also, blockchain is presented as a technology solution where researchers incorporated the blockchain as a security layer to protect against the listed security risks. However, Table 7 shows 34 different security risks *(combining both security risks which are mitigated and appear by introducing the blockchain solution)*. Furthermore, a blockchain technology solution for IoT based applications is rapidly increasing because it provides integrity, reliability and security [19] and these are important for IoT based solutions to reach high requirements of security. By the results, the most common security risks in IoT based applications are mitigated by implementing the blockchain-based solution and only 3 different security risks are inherited after introducing the blockchain solution. The *other* column represents the generic blockchain-based applications and blockchain technology solutions where no specific domain is studied.

Table 7. Security risks based on the research areas.

Security risks which are mitigated by introducing blockchain applications.									
	Applications					Technology			
	Healthcare	Resource monit.	Financial	Smart vehicles	Voting	Security layer	IoT	other	Total
Data tampering attack	6	5	1	4	3	2	5	6	32
DoS/DDoS attack	0	5	1	3	1	7	3	5	25
MitM attack	1	4	1	1	1	2	2	2	14
Identity theft/Hijacking	1	2	0	0	0	0	1	1	5
Spoofing attack	0	0	0	0	1	0	1	2	4
Other risks/threats	2	0	1	0	1	5	5	3	17
Security risks which appear within the blockchain applications.									
Sybil attack	1	1	1	1	2	1	1	5	13
Double spending attack	0	4	2	0	0	2	0	2	10
51% attack	0	4	0	0	1	1	0	2	8
Deanonymization attack	0	2	1	1	1	1	1	0	7
Replay attack	0	2	1	0	0	4	0	0	7
Quantum comp. threat	1	0	0	0	0	2	0	2	5
Selfish mining attack	0	1	1	0	0	2	0	0	4
SC reentrancy attack	0	0	0	0	0	3	0	0	3
Other risks/threats	0	11	5	0	0	2	1	1	20
Total	12	41	15	10	11	34	20	31	174

4.3 Countermeasures

In this section, we overview countermeasures to mitigate the security risks listed in Table 5 and 6.

Countermeasures introduced with blockchain solution. The security risks presented in Table 5 are mitigated by implementing the blockchain-based applications together with the techniques to mitigate these risks. For instance, *Data tampering attack* poses a threat to data-sensitive applications. In [40, 41] authors implement the smart contract to mitigate votes tampering. In [35, 40] authors encrypt information and associate a unique hash. Lei et al. [9] propose a random oracle model with strong RSA. And Li et al. [23] introduce an elliptic curve digital signature algorithm (ECDSA) based signature scheme for anonymous data transmission along Merkle hash tree based selective disclosure mechanism. Han et al. [16] propose to use permissioned blockchain where only the authorized nodes are able to access the data as well as generate a cypher-text by using digital signatures.

DoS/DDoS attack is another exploitable cyber-attack, it is resisted by a distribution of service on different nodes [40]. The [25, 11] authors implement an access control scheme to prevent unauthorized requests. Androulaki et al. [3] propose a block-list to track suspicious requesting nodes and the authors of [3, 32] incorporate the transaction fee to resist it. In order to resist the *MitM attack*, authors suggest to encrypt an information [10, 40] and publish on the blockchain [40]. In [25, 38] research studies, an authentication scheme is introduced to verify each communication node. *Identity theft/Hijacking* based risks are mitigated by information authentication and message generation time-stamping [13]. Mylrea et al. [30] suggest a permission-based solutions (e.g. KSI). *Spoofing attack* is mitigated by introducing an anonymous communication among nodes [8] and Keyless Signature Infrastructure (KSI) based distributed & witnesses trust anchor [30].

Countermeasures to mitigate security risks of blockchain solutions. The blockchain solution comes with a few trade-offs and inherits several security risks (see Table 6) of blockchain technology which are mitigated by implementing the various techniques, those techniques are listed below as countermeasures. In order to mitigate the *Sybil attack*, in [15, 41] authors suggest the permissioned blockchain-based application. Bartolucci et al. [5] incorporate the transaction fee & identification system to allow only authorized users to perform different operations. In [32], authors use the PoR scheme and Liu et al. [27] implement the customised blockchain to control the computing power. *Double spending attack* is mitigated by the transaction verification based on unspent transaction state [3]. In [1] authors resisted this attack by PoA scheme and in [6] by PoW complexity. Also, the Muzammal et al. [29] append the nonce with each transaction. Another frequent security risk on the blockchain-based applications is *51% attack* which is resisted by implementing trusted authorities control [43] and Hjalmarsson et al. [17] customised the Ethereum blockchain to permissioned blockchain.

In order to mitigate *Deanonymization attack*, in [25] authors propose a solution to obtain identity information only after authorization. Bartolucci et al. [5] propose the mixer for mixing the position of output addresses. In [33, 37] authors propose another solution to mitigate this attack by using the fresh key for each transaction. *Selfish mining attack* is mitigated by PoR scheme [32] and by raising the threshold [37]. No countermeasure is found for *Replay attack*. In order to overcome the *Quantum computing threats*, Yin et al. [39] implement the lattice cryptography and in [6] authors suggest an additional digital signature or a hard fork in the post-quantum era. Decusatis et al. [11] propose a need of quantum blockchain. To eliminate the chances of *Smart contract reentrancy attack*, authors of [26] present the automation tool to detect smart contract bugs via run-time trace analysis and in [36] authors built a static analysis tool that detects reentrancy bugs in a smart contract and translates solidity source code into an XML-based intermediate representation and checks it against XPath patterns.

5 Conclusion and Future Work

In this paper, we present a systematic literature review on the blockchain-based applications security risks to explain what security risks are mitigated by introducing the blockchain-based applications, and what security risks are reported in the blockchain-based applications. Our result is a preliminary checklist to support developers' decisions while developing blockchain-based applications.

Our current study has a few limitations: (i) Applications which are built on the blockchain platforms are mostly in the prototype phase. Thus the research studies present only the conceptual illustrations of different security risks and their countermeasures but not the real-life applications. (ii) The field of decentralized applications is relatively new but continuously evolving. Not all the possible security risks are researched in the blockchain-based applications which show the possibility that a wide range of security risks will emerge in upcoming years. (iii) This study found that a lot of security risks and their countermeasures are either obscure or the practical implementation is still not available. Overcoming these limitations could possibly result in the interesting insights and contribute to the explaining the blockchain-based application security risks, their vulnerabilities and the countermeasures for more in-depth.

As a part of the future work, our aim is to build a comprehensive reference model for security risk management to systematically evaluate the security needs. This model would explain the protected assets of the blockchain-based applications, and countermeasures to mitigate their risks.

Acknowledgement. This research has been supported by the Estonian Research Council (grant IUT20-55).

References

1. Alcarria, R., Bordel, B., Robles, T., Martín, D., Manso-Callejo, M.Á.: A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. In: Journal of Sensors (Switzerland) **18**(10) (2018)
2. Ali, S., Wang, G., White, B., Cottrell, R.L.: A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. In: Proceedings of 17th IEEE

International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 pp. 1303–1308 (2018)
3. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J.: Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In: Proceedings of EuroSys '18 Thirteenth EuroSys Conference Article No.30 (2018)
4. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on Ethereum smart contracts (SoK). In: Proceedings of 6th International Conference on Principles of Security and Trust - Volume 10204 Pages 164-186 April 22 - 29, 2017 (2017)
5. Bartolucci, S., Bernat, P., Joseph, D.: SHARVOT: secret SHARe-based VOTing on the blockchain. In: Proceedings of ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (2018), 30–34 (2018)
6. Buchmann, N., Rathgeb, C., Baier, H., Busch, C., Margraf, M.: Enhancing Breeder Document Long-Term Security Using Blockchain Technology. In: Proceedings of International Computer Software and Applications Conference **2**, 744–748 (2017)
7. Buterin, V.: A Next-Generation Smart Contract and Decentralized Application Platform (2014), https://github.com/ethereum/wiki/wiki/White-Paper
8. Cebe, M., Erdin, E., Akkaya, K., Aksu, H., Uluagac, S.: Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. In: Journal of IEEE Communications Magazine (Volume: 56 , Issue: 10 , OCTOBER 2018) (October), 50–57 (2018)
9. Chen, L.: EPBC : Efficient Public Blockchain Client for Lightweight Users. In: Proceedings of SERIAL '17 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers Article No. 1
10. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. In: Journal of Sustainable Cities and Society **39**(December 2017), 283–297 (2018)
11. Decusatis, C., Lotay, K.: Secure, Decentralized Energy Resource Management Using the Ethereum Blockchain. In: Proceedings of 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 pp. 1907–1913 (2018)
12. Fabian Vogelsteller, V.B.: Proof of Stake FAQs (2018), https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs
13. Fan, K., Wang, S., Ren, Y., Yang, K., Yan, Z., Li, H., Yang, Y.: Blockchain-based Secure Time Protection Scheme in IoT. In: Journal of IEEE Internet of Things **PP**(c), 1 (2018)
14. Firesmith, D.G.: Cite this column as follows: Donald Firesmith: Engineering Security Requirements. In: Journal of Object Technology, Published by ETH Zurich, Chair of Software Engineering JOT, 2003 **2**(1), 53–68 (2003)
15. Gallo, P., Quoc Nguyen, U.: BlockSee: Blockchain for IoT video surveillance in smart cities Suporn Pongnumkul NECTEC Thailand. In: Proceedings of IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe) pp. 1–6 (2018)

16. Han, H., Huang, M., Zhang, Y.: An Architecture of Secure Health Information Storage System Based on Blockchain Technology. In: Proceedings of International Conference on Computer and Communication Systems (ICCCS) 2018, LNCS 11064, pp. 578588, 2018 (2018)
17. Hjalmarsson, F.P., Hreioarsson, G.K., Hamdaqa, M., Hjalmtysson, G.: Blockchain-Based E-Voting System. In: Proceedings of IEEE 11th International Conference on Cloud Computing (CLOUD) pp. 983–986 (2018), https://ieeexplore.ieee.org/document/8457919/
18. Jouini, M., Rabai, L.B.A., Aissa, A.B.: Classification of security threats in information systems. In: Proceedings of Procedia Computer Science **32**(October 2017), 489–496 (2014)
19. Khan, M.A., Salah, K.: IoT security: Review, blockchain solutions, and open challenges. In: Journal of Future Generation Computer Systems **82** (2018)
20. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. Engineering **45**(4ve), 1051 (2007)
21. Koteska, B., Mishev, A.: Blockchain Implementation Quality Challenges: A Literature Review. In: Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications (September), 11–13 (2017)
22. Lewis, A.: Blockchain Technology Explained (2015), http://www.blockchaintechnologies.com/blockchain-definition
23. Li, H., Lu, R., Misic, J., Mahmoud, M.: Security and Privacy of Connected Vehicular Cloud Computing. In: Journal of IEEE Network (Volume: 32 , Issue: 3 , May/June 2018) **32**(3), 4–6 (2018)
24. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. In: Journal of Future Generation Computer Systems (2017)
25. Lin, C., He, D., Huang, X., Choo, K.K.R., Vasilakos, A.V.: BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. In: Journal of Network and Computer Applications **116**(February), 42–52 (2018)
26. Liu, C., Liu, H., Cao, Z., Chen, Z., Chen, B., Roscoe, B.: ReGuard: Finding reentrancy bugs in smart contracts. In: Proceedings of International Conference on Software Engineering pp. 65–68 (2018)
27. Liu, M., Shang, J., Liu, P.: VideoChain : Trusted Video Surveillance Based on Blockchain for Campus. In: Proceedings of ICCCS 2018: Cloud Computing and Security pp 48-58 (2018)
28. Macrinici, D., Cartofeanu, C., Gao, S.: Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study. In: Journal of Telematics and Informatics (October), 0–1 (2018), https://linkinghub.elsevier.com/retrieve/pii/S0736585318308013
29. Muzammal, M., Qu, Q., Nasrulin, B.: Renovating blockchain with distributed databases: An open source system. In: Journal of Future Generation Computer Systems **90**, 105–117 (2018)
30. Mylrea, M., Gourisetti, S.N.G.: Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In: Proceedings of 2017 Resilience Week, RWS 2017 pp. 18–23 (2017)
31. Pradeepkumar, D.S., Singi, K., Kaulgud, V., Podder, S.: Evaluating complexity and digitizability of regulations and contracts for a blockchain application design. In: Proceedings of 2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (1), 25–29 (2018)

32. Qin, D., Wang, C., Jiang, Y.: RPchain: A Blockchain-Based Academic Social Networking Service for Credible Reputation Building, vol. 10974. In: Proceedings of ICBC 2018: Blockchain pp 183-198 (2018), http://link.springer.com/10.1007/978-3-319-94478-4
33. Saritekin, R.A., Karabacak, E., Duray, Z., Karaarslan, E.: Blockchain based secure communication application proposal: Cryptouch. In: Proceedings of 6th International Symposium on Digital Forensic and Security, ISDFS 2018 **2018-Janua**, 1–4 (2018)
34. Sato, T., Himura, Y.: Smart-Contract Based System Operations for Permissioned Blockchain. In: Proceedings of 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 **2018-Janua**, 1–6 (2018)
35. Sylim, P., Liu, F., Marcelo, A., Fontelo, P.: Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. In: Journal of Medical Internet Research **20**(9) (2018)
36. Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., Alexandrov, Y.: SmartCheck: Static Analysis of Ethereum Smart Contracts. In: Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain - WETSEB '18 (October), 9–16 (2018)
37. Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A., Njilla, L.: Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack. In: Proceedings of 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017 pp. 458–467 (2017)
38. Yao, H., Wang, C.: A novel blockchain-based authenticated key exchange protocol and its applications. In: Proceedings of IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018 pp. 609–614 (2018)
39. Yin, W.E.I., Wen, Q., Li, W., Zhang, H.U.A., Jin, Z.: An Anti-Quantum Transaction Authentication Approach in Blockchain. In: Journal of IEEE Access (Volume: 6) **6** (2018)
40. Yu, B., B, J.K.L., Sakzad, A., Steinfeld, R., Rimba, P., Au, M.H.: Platform-Independent Secure Blockchain-Based Voting System, vol. 2433. In: Proceedings of ISC 2018: Information Security pp 369-386 (2018)
41. Zhang, W.: A Privacy-Preserving Voting Protocol on Blockchain. In: Proceedings of IEEE 11th International Conference on Cloud Computing (April), 401–408 (2018)
42. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang. In: International Journal of Web and Grid Services **14**(4), 1–24 (2016), http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf
43. Zhu, L., Wu, Y., Gai, K., Choo, K.K.R.: Controllable and trustworthy blockchain-based cloud data management. In: Journal of Future Generation Computer Systems **91**, 527–535 (2018), https://linkinghub.elsevier.com/retrieve/pii/S0167739X18311993