Blockchain Implementation Quality Challenges: A Literature Review

BOJANA KOTESKA, ELENA KARAFILOSKI and ANASTAS MISHEV, University SS. Cyril and Methodius, Faculty of Computer Science and Engineering, Skopje, Macedonia

Blockchain is a public digital and distributed database solution providing decentralized management of transaction data. Since the introduction of Bitcoin cryptocurrency, which was the first implementation of the Blockchain technology in 2008, the interest in Blockchain technology has been constantly increasing. Blockchain is not applicable only in financial transaction systems but it is transforming our society from the way we use our cars, smartphones, healthcare, vote, and even personal identification. As such when we discuss the Blockchain implementation we are really discussing three different things: Blockchain ledger, Blockchain network and clients. Modern Blockchain implementations have to adapt to some technical challenges and limitations required for Blockchain technology. For example, security, privacy, throughput, size and bandwidth, performance, usability, data integrity and scalability are just some of the attributes required for high quality Blockchain implementation. In this paper, we aim to analyze the current quality issues in the Blockchain implementation and to identify the Blockchain quality attributes. A literature review is conducted to investigate the current quality requirements for Blockchain implementation. Findings show that the research on quality requirements for Blockchain implementation is still in its early stage. The conclusions of this study could be used for further analysis of the quality attributes required for the Blockchain implementations and improvement of the quality of the Blockchain systems.

Categories and Subject Descriptors: D.2.4 [**Software Engineering**]: Software/Program Verification —*Validation*; K.6.4 [**System Management**] Quality Assurance

General Terms: Reliability, Security

Additional Key Words and Phrases: Blockchain, quality requirements, software quality.

1. INTRODUCTION

Blockchain is a technology that redefines trust in the new generation systems. It spreads the idea of processing any type of transaction without a mediator. Mediators, like corporations and governments, almost always come as central entities that receive, process and store the transactions. All the trust we put as users in any system is trust in the mediators who are obliged to process the transactions using correct business logic. Mediators are fully in control of data security and data privacy too. In a case of Blockchain systems, the trust is decentralized. Users just need to trust the system and the smart code that is shared between all the participants. From technical point of view, Blockchain is a distributed database that exists on a P2P network (Fig. 1). This P2P network is a backbone of the system because every node in the network is on the same level as all the other nodes. Although nodes can come in many forms, there is no central node that is an authority. Every node stores a local copy of the Blockchain. If consensus of nodes agrees upon transaction's validity, then the transaction is considered valid [Pilkington 2015].

The Blockchain database can be a simple file that just stores minimum required data about the encrypted transactions. All the transactions are grouped in timestamped blocks (Fig.2). Once the transaction is in the block, it is

Author's address: Bojana Koteska, FCSE, Rugjer Boshkovikj 16, P.O. Box 393 1000, Skopje; email: bojana.koteska@finki.ukim.mk; Elena Karafiloski, FCSE, Rugjer Boshkovikj 16, P.O. Box 393 1000, Skopje; email: elena.karafiloski@gmail.com; Anastas Mishev, FCSE, Rugjer Boshkovikj 16, P.O. Box 393 1000, Skopje; email: anastas.mishev@finki.ukim.mk.

In: Z. Budimac (ed.): Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia, 11-13.9.2017, Also published online by CEUR Workshop Proceedings (http://ceur-ws.org, ISSN 1613-0073)

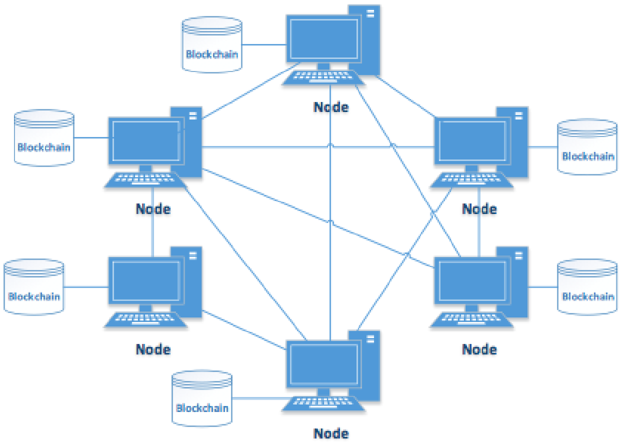

Fig. 1. Blockchain P2P Network.

irreversible. All the nodes can access the transactions, but cannot change or delete a transaction from the Blockchain. The business logic by which the nodes operate is often defined in so called "smart contracts". Smart contracts specify all the conditions that must be met before a transaction is executed. They come together as programmed rules for writing and reading from the Blockchain database. The smart contracts are installed on every node too.

The Blockchain is constantly growing. In a case of Bitcoin, there is new block every ten minutes. The last block in the Blockchain contains the latest executed transactions. Every block has a header and a body. The header contains metadata like time of block's creation and a link to the previous block. That is how the blocks are linked. All the transactions with the addresses of the parties included in the transactions are listed in the block's body.

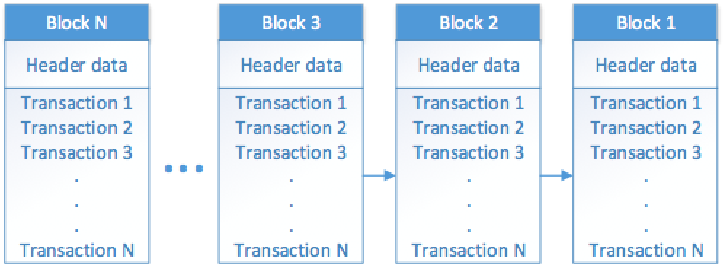

Fig. 2. Blocks in Blockchain.

There are public and private Blockchains. Bitcoin is a public Blockchain because it was designed to be completely open, decentralized, and permissionless. This means that anyone can participate without establishing an identity and there is no central authority that controls admission. New Blockchain platforms like Hyperledger [News 2017] take a novel approach to the model, in part by managing the admission of participants. In other words, Hyperledger is a permissioned, shared ledger modified to respond to the multitude of industrial use case requirements by providing a secure model for identity. Here, new techniques are replacing the need of block's mining. Because the environment is more controlled and contains smaller number of nodes which are authorized, mining can be avoided and the consensus can be simpler by rule.

All nodes in the network can have a permission to create new transactions. Depending on the application, one end user may be one node, or may connect to one server node using web application. In both cases, the end user creates new transactions. When a transaction is created, it has to go through validation and confirmation stages before it enters the Blockchain and it is broadcasted to the network. P2P nodes share the transaction between themselves almost in a real time. Every node receives the transaction and validates its structure and actions. The validation checklists are defined in the Blockchain system. They may check the transaction's parameters, size, values etc. If valid, the node saves the transaction into its transaction pool. If not, the transaction is immediately removed from the pool.

Some of the nodes are so called "miners". They use special hardware to work on creating the next block. Miners take all the available transactions from the transaction pool and include them in a new candidate block. Mining a block in Bitcoin is done with a proof of work concept [Vukolic 2015]. That is calculating a random hash value using data of the candidate block. To guess a correct hash value there is a need of great processing power that calculates millions of values in a second. The correct hash value must satisfy a defined difficulty target. This number is calculated using all block's metadata including the hash of the previous block. This is the key to Blockchain security. If someone tries to change a transaction from the past, the hash value of the block that contains the transaction must be calculated again. All hash values for the blocks that came afterwards must be calculated again too. This is not feasible, unless more than half of the nodes in a network are malicious. When a new block is created, it is broadcasted to the network. All nodes receive the block, validate it and all the transactions in it. If valid, all nodes put it as the next block in their local Blockchain. Transactions that are included in the created block, are then removed from the pool.

The research has shown that most of the studies have focused on one or several particular aspects connected to Blockchain implementation. To the best of our knowledge, no studies have been investigated in details the quality requirements and solutions for Blockhain implementations. This type of study can help to identify quality requirements that can be taken into account in the new Blockchain implementations. Furthermore, these study could be helpful to understand how different Blockchain characteristics and current issues could affect the quality of Blockchain systems.

In this research, we have conducted a literature review to investigate the level of evidence available in published literature on the quality requirements for Blockchain implementations.

The paper is organized as follows. In Section 2, we research the current quality issues in the Blockchains implementations. Section 3 provides the overview of the quality requirements and solutions. Conclusive remarks are given in the last section, Section 4.

2. CURRENT QUALITY ISSUES IN BLOCKCHAIN IMPLEMENTATIONS

Blockchain technology is still in testing phase and its implementation has some issues that have to be addressed when trying to establish Blockchain free cryptographically secured system. In this section, we summarize the most common Blockshain quality issues found in this research.

Throughput issues. In his book, Swan [Swan 2015] has discussed seven technical future challenges and limitations of the Blockchain technology. One of them is througput. The problem with current Bitcoin network is that it processes 3 to 20 transaction per second (tps) [Xu et al. 2016], with a maximum possible theoretical throughput seven tps. In comparison, VISA transaction network can process 2000 tps (has been stress-tested in 2013 to handle 47,000 transactions per second [Trillo 2013]) and Twitter network 5000 tps.

Latency issues. Time factor is one of the most critical issues in Blockchain implementations. Having the requests processed on Internet almost immediately, it is an obstacle in regards to the universal technology acceptance. [Beck et al. 2016]. In order to provide security the Bitcoin transaction block, the time needed to complete one transaction is about 10 minutes. For a larger transfer amounts, the cost of a double spend attack can last about an hour. VISA transaction completion process takes seconds at most [Swan 2015] [Yli-Huumo et al. 2016].

Size and bandwidth issues. In February 2016, the size of the Blokchain in the Bitcoin network was over 50,000 MB and it could grow 214 PB in each year. Current Bitcoin size is 1MB and a new block is created every 10 minutes. It means that an average 500 transaction can be handled in one block. This is a serious issue if Blockchain needs to handle more transactions [Swan 2015] [Yli-Huumo et al. 2016].

Scalability issues. One of the main challenging problems in Blockchain implementations is scalability. In order to provide the theoretically proved security, the Blockchain implementation must have a large number of full nodes.

Otherwise, the implementation might result in a less decentralized system such in a case with Bitcoin [Beck et al. 2016]. The scalability limits of the Blockchain are connected to the size of the data on Blockchain, the transaction processing rate, and the latency of data transmission. On the other hand, the latency between the transaction submission and confirmation is affected by the consensus protocol. For example, the time between the transaction submission and confirmation on Bitcoin is around 1 hour (10-minute block interval per block and 6-block confirmations), and around 3 minutes on Ethereum (14-second block interval per block and 12-block confirmation) [Xu et al. 2017].

Cost issues. Blockchain use is not free of cost which is a drawback of decentralization and the blockchain technology. The users have to pay for the transactions and computational power. One fact that users will chose centralized solutions is because they will not be constantly reminded that an action has a fee, but the prices will be more hidden [Beck et al. 2016].

Data malleability issues. Data malleability is a potential issue in the Blockchain implementation. The signatures do not provide guarantee the ownership of the Bitconin transferred in a transaction. An attacker can modify and rebroadcasts a transaction which can cause problems with approvement of transaction confirmation. [Decker and Wattenhofer 2014] [Yli-Huumo et al. 2016].

Authentication issues. Another problem connected to the Blockchain transactions is the authentication. An example of incident with the authentication is the well-known case in Mt.Gox [Bos et al. 2014] when the storage of customer private keys was attacked and stolen.

Privacy issues. One issue connected to Blockchain privacy is the problem with multiple addresses. For example, users of the Bitcoin system can create any number of addresses and researchers try to cluster all addresses that belong to the same user [Herrera-Joancomartí and Pérez-Solà 2016]. Address clustering is performed to trace the economic movements of the same users. The goal is to find all addresses included in the transaction that belong to the same user [Reid and Harrigan 2013] [Androulaki et al. 2013]. In [Koshy et al. 2014], the authors found that some of the Bitcoin addresses can be mapped to IP addresses by analyzing the transaction traffic.

Double-spending attacks. Blockchain implementations are susceptible to double-spending attacks. In a case of Bitcoin, a double-spending attack can occur when the attacker keeps his/her bitcoin while receiving services that can be spent again. This happens when the attacker credits an account, receives the service or goods by the account holder and then reorganize the ledger by reverting the transaction that credits the account. Nakamoto [Nakamoto 2008] claims that Bitcoin system is preventing double-spending attacks by modeling the attacker and the set of honest players as to competing actors performing a random walk moving toward a single direction with probabilistic steps. However, it is not claimed that in Bitcoin's decentralized environment the attacker may attempt to introduce disagreement between the honest miners[Garay et al. 2015].

Security issues. A problem with the public distributed legders is the highly speculative nature with a trade-off between the dimension of the network and decentralization [Atzori 2015]. The Bitcoin Blockchain has a possibility of 51% attack. In such a case, one miner can have full control of the majority of the network which is a serious problem. In [Lim et al. 2014], the authors have identified different security breaches that occurred in Bitcoin including DDoS attacks, account hacking using Trojan horses and viruses from ads. According to [Vasek and Moore 2015], a total od $11 million had been contributed to scams by 13000 Bitcoin victims from September 2013 to September 2014.

Wasted Resources. The energy spend of mining in the Bitcoin network is approximately $15 million per day [Swan 2015] . The waste in the Bitcoin is a result on the Proof-of-Work effort. In such a case, the probability of mining a block depends on the work done by the miner [Yli-Huumo et al. 2016].

Usability issues.The Bitcoin API is less user-friendly that the other modern API-s [Swan 2015] [Yli-Huumo et al. 2016].

Versioning, hard forks, multiple chains. Smaller chains with smaller number of nodes are more susceptible to 51% attack. Another issue is the hard merging of split chains for administrative or versioning purposes [Swan 2015] [Yli-Huumo et al. 2016].

3. QUALITY REQUIREMENTS AND SOLUTIONS FOR BLOCKCHAIN IMPLEMENTATIONS

To ensure the trustworthiness of a Blockchain system, the Blockchain implementation must provide high data integrity, security, reliability and node privacy [Porru et al. 2017] [Swan 2015].

A possible solution to the throughput problem is to increase the size of each block, but it can lead to other size problems [Yli-Huumo et al. 2016]. If the same Blockchain is used on a wide variety of applications, more performance is needed [Beck et al. 2016].

An alternative scenario to solve the problem with size and bandwidth is to reduce the number of submitted transactions and to stop recording any voting activity, but to record only the different value of negotiable variables and the final voting result [Xu et al. 2016].

A solution to the scalability problem is to have many blockchains for different purposes. For example, some of them can be used for specific purposes while other for generalized tasks. The benefit of this approach is that the Blockchains can use each other to provide security for one another, no matter what their purpose is. In a such case, a miner can mine Blockchains with a suitable size and also security will be on a satisfactory level [Beck et al. 2016].

One option to solve the authentication issue is the BlueWallet device which is a Bitcoin hardware token which secure and sign Bitcoin transactions and communicates by using Bluetooth Low Energy [Bamert et al. 2014]. Another solution to this problem is the proposed certification system for Bitcoin which offers a guarantee to send and receive Bitcoins only to/ from certified users, and control of the creation of Bitcoins addresses by trusted authorities [Ateniese et al. 2014]. In [Mann and Loebenberger 2017], the authors proposed a two-factor authentication for a Bitcoin wallet by using a smart phone as the second authentication factor.

The privacy of the Blockchain transaction is an essential quality requirement in the Blockchain implementations. Transactions are public and all the data on the Blockchain are visible to all participants, but they must not be linked to identities. A more appropriate solution is a permissioned Blockchain which will allow developers to grant permissions to the participants [Xu et al. 2016]. If Blockchain systems are to operate at a global scale, a new model for privacy-preserving identities is needed. The model must allow entities to verify the security of an identity, to access the independence of an identity from any given authority and to access the source of trust for a digital identity. MIT researches proposed the ChainAnchor system which is designed for permissioned Blockchains and it adds an identity and privacy-preserving layer above the Blockchain [Shrier et al. 2016]. A human resource information management model based on Blockchain that reduces the risk of authenticity of human resource information is presented in [Wang et al. 2017]. This model provides authentic and decision support information to the human resource management in an organization. Consensus mechanism, smart contract, accounting, and payment functions of the Blockchain provides the basic support for human resource information management.

A new scheme for increasing the energy efficiency is presented in [Paul et al. 2014]. Each block of the Blockchain is modified by adding some extra bytes to utilize the timestamp more effectively. An alternative to Proof-of-Work effort is Proof-of-Stake in which the resource that is compared is the amount of Bitcoin a miner holds. If someone is holding 1% of the Bitcoin, he can mine 1% of the "Proof-of-Stake blocks" [Yli-Huumo et al. 2016].

One of the biggest challenges is the data storage capacity limitation in the current Blockchain implementations. Taking into advance the cost efficiency, performance, and flexibility, the real design challenge is to decide what data and computation should be placed on-chain and what data should be stored off-chain [Xu et al. 2016]. A common practice for storing data in the Blockchain ledger is to store raw data off-chain, and to store meta-data, small critical data, and hashes of the raw data only on-chain [Xu et al. 2017].

Security and reliability of the software that implements Blockchain technology can be ensured by continuous testing techniques. Such testing techniques that could improve the quality of Blockchain systems were recently presented by IBM [Ojha 2017].

The testing of the Blockchain implementations takes into consideration several implementation aspects. First, the level of validation depends on the platform implementation (public or private). If the platform is private, then it requires much more effort in testing. Next, if the test platform does not provide replica of the Blockchain implementation, then additional time will be required for setting up the environment. If the Blockchain implementation has connection with other applications, then the consistency must be checked by making integration testing. One of the key issues is performance of the Blockchain implementation. A strategy that will handle a large number of transactions must be applied, so the results from the performance testing are satisfactory. In a case of a real scenario testing, the early involvement of the testing team is very important since the other system components or applications can be affected by the Blockchain implementation. An example of the Blockchain testing process is shown in Fig.3. The system appreciation phase includes the creation of testing plan and strategy that provides detailed view of the impacted components in the system. In the test design assurance phase, the testing team should create a detailed level test strategy and to assign traceability to the requirements. The key components that need to be done in this phase are: building a model of the blocks structure, transactions and contracts, defining use cases for each section and validation end points, specifying non-functional requirements and security testing needs. The result from the test planning phase should be a full test strategy with a specified testing methodology. In order to verify and validate the test plan, the use cases should be mapped to detailed level test cases. In the last phase, the test cases execution and result verification are performed. The execution of test cases can be automated by using frameworks for unit testing. Testing should be done according the test plan and the list of defects needs to be reported along with the test execution status [Sundarraman 2017].

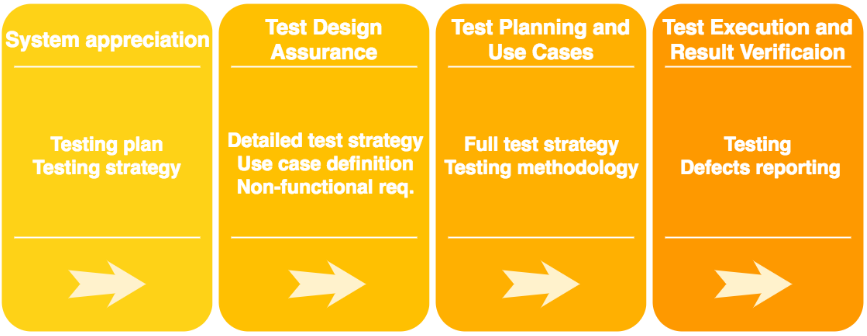

Fig. 3. Testing process of Blockchain implementation.

Software architecture that includes specific design notations, patterns and meta models and also modeling languages that provide designing graph models (UML diagrams) can enhance the quality of software that implements the Blockchain technology. Additionally, specific metrics required to measure complexity, communication capability, resource consumption and performance could be defined and used for evaluating and improvement of the software process [Porru et al. 2017].

If the Blockchain implementations are not tested properly they will likely fail at some point. There are different ways to verify a distributed system such as Blockchain. In [McCaffrey 2015], the authors propose formal verification methods and lineage driven fault injection (random, heuristic..).

The evaluation of the Blockchain performance can be done using a few simple qualitative and quantitative metrics [Kakavand and Kost De Sevres 2016]:

—Submission Throughput: maximum number of transactions submitted per second permitted by each node and by the network.

—Maximum/Average Validation Throughput (processing speed) of the network: parameter that determines the maximum/ average number of transactions validated per second permitted by the network.

—Average Transaction Validation Latency: the average time taken to validate the transaction from the time of its submission. This metric measures the average time of waiting of the users for their transaction to be validated.

—Latency Volatility: measure of the variety of the transaction processing time.

—Security: The evaluation of system security requires a threat model which is able to define the types and scope of adversaries and attacks on the system. The following analysis are required to perform the security evaluation of the Blockchain implementation: Transaction and block immutability, transaction censorship resistance, denial of Service (DoS) resilience, trust requirements of users and oracles, protocol governance and node membership services and transaction confidentiality and user anonymity.

—Confidentiality: ability of Blockchain nodes to hide the contents of the transaction and or the identity as having participated in that transaction.

—Transaction fees: Users pay small transaction fee to the network in order to process transactions or execute smart contracts. These fees are used to cover the maintenance costs or protection of malicious computational tasks.

—Hardware requirements: Memory/storage per node, processor resources needed to validate transactions and blocks, network usage.

—Scalability: Number of nodes, transactions, users, geographic dispersion.

—Complexity: measures the development, maintenance, and operation complexity of Blockchain infrastructure.

—Smart-contract limitations: limitations of the code deployed to the Blockchain caused by smart contract scripting language and the underlying consensus protocols.

The Blockchain implementation into an established supply chain system is not an easy process because the existing supply chains are hard to be changed and adapted. Some companies spend years putting supply chains into the existing systems [Mougayar 2016].

4. CONCLUSION

Blockchain is a distributed database solution providing decentralized transaction and data management. Modern Blockchain implementations have to ensure security, privacy, throughput, size and bandwidth, performance, usability, data integrity and scalability. However, these quality attributes set up a lot of challenges that need to be addressed.

To understand the current research in the field of Blockchain implementation quality, we have analyzed the current quality issues in the Blockchain implementation and identified the Blockchain quality attributes. The research has shown that this topic is still immature. The results indicate that the Blockchain implementations need to be improved in terms of scalability, latency, throughput, cost-effectiveness, authentication, privacy, security, etc. The goal of this study was to investigate the quality requirements and solutions for Blockchain implementation. We provided an overview of the quality recommendations and solutions for Blockchain that could improve the quality of the new Blockchain implementations. This study contributes to the theory by analyzing the Blockchain quality from literature and by providing an integrated view of quality requirements for Blockchain implementations.

REFERENCES

Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, 34–51.

Giuseppe Ateniese, Antonio Faonio, Bernardo Magri, and Breno De Medeiros. 2014. Certified bitcoins. In *International Conference on Applied Cryptography and Network Security*. Springer, 80–96.

Marcella Atzori. 2015. Blockchain technology and decentralized governance: Is the state still necessary? (2015).

Tobias Bamert, Christian Decker, Roger Wattenhofer, and Samuel Welten. 2014. Bluewallet: The secure bitcoin wallet. In *International Workshop on Security and Trust Management*. Springer, 65–80.

Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, and Simon Malone. 2016. Blockchain-the Gateway to Trust-Free Cryptographic Transactions.. In *ECIS*. ResearchPaper153.

Joppe W Bos, J Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. 2014. Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*. Springer, 157–175.

Christian Decker and Roger Wattenhofer. 2014. Bitcoin transaction malleability and MtGox. In *European Symposium on Research in Computer Security*. Springer, 313–326.

Juan A Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The Bitcoin Backbone Protocol: Analysis and Applications.. In *EUROCRYPT (2)*. 281–310.

Jordi Herrera-Joancomartí and Cristina Pérez-Solà. 2016. Privacy in bitcoin transactions: new challenges from blockchain scalability solutions. In *Modeling Decisions for Artificial Intelligence*. Springer, 26–44.

Hossein Kakavand and Nicolette Kost De Sevres. 2016. The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. (2016).

Philip Koshy, Diana Koshy, and Patrick McDaniel. 2014. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*. Springer, 469–485.

Il-Kwon Lim, Young-Hyuk Kim, Jae-Gwang Lee, Jae-Pil Lee, Hyun Nam-Gung, and Jae-Kwang Lee. 2014. The Analysis and Countermeasures on Security Breach of Bitcoin. In *International Conference on Computational Science and Its Applications*. Springer, 720–732.

Christopher Mann and Daniel Loebenberger. 2017. Two-factor authentication for the Bitcoin protocol. *International Journal of Information Security* 16, 2 (2017), 213–226.

Caitie McCaffrey. 2015. The verification of a distributed system. *Queue* 13, 9 (2015), 60.

William Mougayar. 2016. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons.

Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). https://bitcoin.org/bitcoin.pdf

Blockchain News. 2017. Hyperledger Whitepaper. http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf. (2017).

Varun Ojha. 2017. Unit-testing your Blockchain chaincode in Go for Hyperledger Fabric v0.6. (2017). https://www.ibm.com/developerworks/cloud/library/cl-ibm-blockchain-chaincode-testing-using-golang/index.html

Goutam Paul, Pratik Sarkar, and Sarbajit Mukherjee. 2014. Towards a more democratic mining in bitcoins. In *International Conference on Information Systems Security*. Springer, 185–203.

Marc Pilkington. 2015. Blockchain technology: principles and applications. *Browser Download This Paper* (2015).

Simone Porru, Andrea Pinna, Michele Marchesi, and Roberto Tonelli. 2017. Blockchain-oriented software engineering: challenges and new directions. In *Proceedings of the 39th International Conference on Software Engineering Companion*. IEEE Press, 169–171.

Fergal Reid and Martin Harrigan. 2013. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*. Springer, 197–223.

David Shrier, Weige Wu, and Alex Pentland. 2016. *Blockchain & infrastructure (identity, data security)*. Technical Report. Tech. rep. URL: http://cdn. resources. getsmarter. ac/wp-content/uploads/2016/05/MIT_Blockchain_Infrastructure_ Report_Part_Three_May_2016. pdf.

Arvind Sundarraman. 2017. Assuring success in blockchain implementations by engineering quality in validation. (2017). https://www.infosys.com/IT-services/validation-solutions/white-papers/Documents/blockchain-implementations-quality-validation.pdf

Melanie Swan. 2015. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Manny Trillo. 2013. Stress test prepares VisaNet for the most wonderful time of the year. (2013). http://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html

Marie Vasek and Tyler Moore. 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In *International Conference on Financial Cryptography and Data Security*. Springer, 44–61.

Marko Vukolic. 2015. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication.. In *iNetSeC*. 112–125.

Xin Wang, Libo Feng, Hui Zhang, Chan Lyu, Li Wang, and Yue You. 2017. Human Resource Information Management Model based on Blockchain Technology. In *Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on*. IEEE, 168–173.

Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, An Binh Tran, and Shiping Chen. 2016. The blockchain as a software connector. In *Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on*. IEEE, 182–191.

Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. In *Software Architecture (ICSA), 2017 IEEE International Conference on*. IEEE, 243–252.

Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. 2016. Where Is Current Research on Blockchain Technology? - A Systematic Review. *PloS one* 11, 10 (2016), e0163477.