Creative Research Publishers

Journal of Behavioral Informatics
Digital Humanities & Development Research

https://www.crossref.org/06members/50go-live.html

Vol 10, No 2, 20224 Series

On the Security, Vulnerabilities and Attack Surfaces of Blockchain Technologies

[1]Laud Charles Ochei, [2]Aliloulaye Tchaou, [3]Omotosho Seyi & [4]Longe, Olumide
[1]Department of Computer Science, University of Port Harcourt, Port Harcourt, Nigeria
[2]Department of Technology and Innovation, Ghana Institute of Management & Public Administration
[3]Federal School of Statistics, Ibadan, Nigeria
[4]Academic City University College, Accra, Ghana
E-mails: laud.ochei@uniport.edu.ng; tchaou.aliloulaye@st.gimpa.edu.gh;
longeolumide@fulbrightmail.org; seyiblack1@yahoo.co.uk

ABSTRACT

As blockchain technology continues to gain traction in various industries, it is critical to assess and evaluate the security measures of blockchain systems. This paper reviews the existing literature on blockchain security, highlight the potential threats to blockchain systems, and explore the various techniques used to assess and evaluate blockchain security. The research will also examine the strengths and weaknesses of these techniques and suggest best practices for blockchain security assessment and evaluation. Our efforts contributes to the body of knowledge on blockchain security, and provide valuable insights for blockchain developers, auditors, and security professionals.

Keywords: Blockchain, Security, Systems, Techniques, Threats.

Journal Reference Format:
Laud Charles Ochei, Aliloulaye Tchaou, Omotosho Seyi & Longe, Olumide. (2024): On the Security, Vulnerabilities and Attack Surfaces of Blockchain Technologies. Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol. 10.No. 2, Pp 93-102. https://www.isteams.net/behavioralinformaticsjournal. dx.doi.org/10.22624/AIMS/V10N2P8

1. BACKGROUND TO THE STUDY

Blockchain technology has emerged as a revolutionary concept that has transformed the way digital transactions are conducted (Nakamoto, 2008). This decentralized and transparent system records transactions securely and efficiently, without the need for intermediaries like banks (Nakamoto, 2008). The blockchain technology is a public ledger that records all transactions on the network and consists of blocks of transactions that are linked together in chronological order (Nakamoto, 2008). Each block contains a cryptographic hash of the previous block, which ensures the integrity of the blockchain (Nakamoto, 2008). The first implementation of blockchain technology was Bitcoin, which is created and transferred using blockchain technology (Nakamoto, 2008). Bitcoin's blockchain is a public ledger that records all transactions on the network (Nakamoto, 2008). Other blockchain-based cryptocurrencies like Ethereum, Litecoin, and Ripple have also emerged, which have different features and capabilities but share the same fundamental characteristics of blockchain technology (Swan, 2015).

Blockchain technology has found applications in several sectors, such as finance, healthcare, supply chain management, and more (Swan, 2015). This technology has the potential to transform the way transactions are conducted in these sectors by providing a secure and transparent system for recording and verifying transactions (Swan, 2015). However, concerns have been raised about its security vulnerabilities and attack surfaces (Swan, 2015). Attackers have started to target blockchain systems with various types of attacks, such as 51% attacks and double-spending attacks (Swan, 2015). Researchers and developers have been working on improving the security of blockchain systems by using consensus protocols to ensure the validity of transactions on the network (Swan, 2015). Consensus protocols are used to ensure that all nodes on the network agree on the state of the blockchain (Swan, 2015).

There are several types of consensus protocols, such as proof of work, proof of stake, and delegated proof of stake (Swan, 2015). Proof of work is the consensus protocol used by Bitcoin, which requires nodes on the network to solve complex mathematical puzzles to add new blocks to the blockchain (Nakamoto, 2008). Proof of stake is an alternative consensus protocol that requires nodes to stake a certain amount of cryptocurrency to participate in the consensus process (Swan, 2015).

Blockchain Technology

Blockchain technology has revolutionized the way we perceive digital transactions, providing a decentralized and transparent system that records transactions securely and efficiently. The technology has become widely popular and has found applications in several sectors such as finance, healthcare, supply chain management, and more (Zheng et al., 2017). However, with the growing popularity of blockchain technology, there has been an increasing concern about its security vulnerabilities and attack surfaces. Investigating and analyzing the security vulnerabilities and attack surfaces of existing blockchain systems is critical to identify and mitigate security risks in blockchain implementations. To achieve this goal, a range of methods and tools can be used, including penetration testing, vulnerability scanning, and code review.

Penetration testing is a method of identifying and exploiting security vulnerabilities in a system by simulating an attack. This method has been used to identify security vulnerabilities in various blockchain systems. Guo et al. (2019) used penetration testing to identify security vulnerabilities in the Hyperledger Fabric blockchain system, revealing several vulnerabilities such as DoS attacks, data tampering, and privacy breaches. Vulnerability scanning is another method used to identify security vulnerabilities in blockchain systems. Shin et al. (2018) used vulnerability scanning to identify security vulnerabilities in Ethereum smart contracts.

The study revealed that Ethereum smart contracts are vulnerable to various types of attacks such as reentrancy attacks, integer overflow attacks, and denial-of-service attacks. Code review is another important method used to identify security vulnerabilities in blockchain systems. Tschorsch and Scheuermann (2016) used code review to identify security vulnerabilities in the Bitcoin network, revealing that the Bitcoin network is vulnerable to various types of attacks such as selfish mining attacks and Sybil attacks. While these methods have proven effective in identifying security vulnerabilities and attack surfaces in blockchain systems, it is also important to consider the specific characteristics of blockchain technology when conducting security assessments.

Blockchain technology is decentralized and relies on consensus protocols to ensure the validity of transactions, making it more challenging to detect and mitigate attacks on the network (Zhang et al., 2018). In addition to the methods mentioned above, there are other approaches to investigating and analyzing the security vulnerabilities and attack surfaces of existing blockchain systems. Azevedo et al. (2020) used a hybrid approach that combined static analysis, dynamic analysis, and manual code inspection to identify security vulnerabilities in smart contracts. The study revealed that the hybrid approach was more effective in identifying security vulnerabilities in smart contracts than individual approaches.

One of the major concerns regarding blockchain security is the vulnerability of smart contracts. Smart contracts are self-executing contracts that are stored on the blockchain. They are responsible for automating the execution of transactions on the blockchain. However, smart contracts can be vulnerable to various types of attacks such as reentrancy attacks, integer overflow attacks, and denial-of-service attacks. Therefore, it is essential to investigate and analyze the security vulnerabilities of smart contracts in existing blockchain systems.

Several studies have been conducted to investigate and analyze the security vulnerabilities of smart contracts in existing blockchain systems. In a study conducted by Atzei et al. (2017), the authors identified several types of vulnerabilities in Ethereum smart contracts. The vulnerabilities included transaction-ordering dependence, timestamp dependence, and gas limit dependence. The authors concluded that the vulnerabilities in Ethereum smart contracts could lead to significant financial losses for users.

Another important concern regarding blockchain security is the possibility of 51% attacks. A 51% attack occurs when a single entity or group of entities control more than 50% of the computing power in the blockchain network. This gives them the ability to manipulate the blockchain, reverse transactions, and double-spend coins. Therefore, it is important to investigate and analyze the security vulnerabilities of blockchain networks to mitigate the risk of 51% attacks.

Several studies have been conducted to investigate and analyze the security vulnerabilities of blockchain networks. In a study conducted by Zhang et al. (2018), the authors analyzed the security vulnerabilities of the Bitcoin network. The authors identified several types of attacks that could be used to exploit the vulnerabilities in the Bitcoin network. The attacks included double-spending attacks, selfish mining attacks, and Sybil attacks.

The authors concluded that the security vulnerabilities in the Bitcoin network could be exploited to launch various types of attacks. Another important concern regarding blockchain security is the possibility of insider attacks. Insider attacks occur when a malicious actor with access to the blockchain network exploits their privileges to launch attacks on the network. Therefore, it is important to investigate and analyze the security vulnerabilities of blockchain networks to mitigate the risk of insider attacks.

Several studies have been conducted to investigate and analyze the security vulnerabilities of blockchain networks to mitigate the risk of insider attacks. In a study conducted by Kim et al. (2019), the authors proposed a secure blockchain system that prevents insider attacks. The proposed system uses a distributed trust model that distributes trust among the network nodes, thereby preventing any single node from gaining too much control over the network. The authors concluded that the proposed system could effectively mitigate the risk of insider attacks in blockchain networks.

2. EVALUATING THE SECURITY OF BLOCKCHAIN SYSTEMS

2.1 Empirical Literature

A study conducted by Wu et al. (2021) proposed a blockchain security evaluation framework based on the STRIDE model. The framework was designed to identify potential security threats and vulnerabilities in blockchain systems using a threat modeling approach. The authors applied the framework to a real-world blockchain system and identified several potential security threats and vulnerabilities.

Similarly, another study by Xia et al. (2020) proposed a security assessment methodology for blockchain systems based on the PASTA model. The methodology was designed to identify and evaluate potential security threats and vulnerabilities in blockchain systems using a risk-based approach. The authors applied the methodology to a blockchain-based supply chain management system and identified several potential security threats and vulnerabilities.

Blockchain systems are not impervious to security threats, and it is essential to evaluate their security through comprehensive analysis using established methodologies and tools. Several researchers have explored potential vulnerabilities and attack surfaces of blockchain systems and proposed solutions to mitigate these risks. One of the significant security threats to blockchain systems is the 51% attack, where an attacker controls more than 50% of the computing power of the blockchain network.

This attack allows the attacker to modify transactions, double-spend coins, and exclude other users from the network. Karame et al. (2012) proposed a quantitative analysis of the probability of 51% attacks on different blockchain systems, considering various parameters such as network size, hash rate, and difficulty level. They found that smaller blockchain networks are more vulnerable to 51% attacks and suggested increasing the difficulty level or implementing checkpointing mechanisms to prevent these attacks.

Another security vulnerability of blockchain systems is the smart contract vulnerability, where the code of the smart contract contains errors or loopholes that can be exploited by attackers. Atzei et al. (2017) conducted a systematic review of smart contract vulnerabilities and proposed a taxonomy of these vulnerabilities. They categorized smart contract vulnerabilities into four categories: transaction-ordering dependencies, mishandled exceptions and call-stack vulnerabilities, timestamp dependence, and reentrancy vulnerabilities. They also proposed solutions to mitigate these vulnerabilities, such as code reviews, testing, and formal verification.

In addition to the above vulnerabilities, blockchain systems are also vulnerable to privacy attacks, where an attacker can reveal the identity of a user or link transactions to a particular user. Kosba et al. (2016) proposed a privacy-preserving protocol for blockchain systems called Hawk, which uses zero-knowledge proofs to enable secure and private transactions without revealing any sensitive information. The protocol ensures that only authorized users can access the data, and the data is securely encrypted.

Another significant security threat to blockchain systems is the distributed denial-of-service (DDoS) attack, which can cause disruptions to the network's functionality by overwhelming it with traffic (Dinh et al., 2018). To mitigate DDoS attacks, researchers have proposed solutions such as increasing network capacity, implementing load balancing mechanisms, and using anti-DDoS services (Sun et al., 2019).

Blockchain systems are also vulnerable to social engineering attacks, which exploit human vulnerabilities to trick users into revealing sensitive information or transferring funds to unauthorized accounts (Ron et al., 2018). Social engineering attacks can take various forms, such as phishing, baiting, pretexting, and quid pro quo (Chen et al., 2019). To mitigate social engineering attacks, users must be aware of these tactics and adopt security best practices, such as verifying the authenticity of requests, using two-factor authentication, and keeping their private keys secure (Nakamoto, 2008). Lastly, blockchain systems are susceptible to attacks on the underlying cryptography, such as quantum attacks, which can break some of the cryptographic algorithms used in blockchain systems (Zohrevand & Bassoli, 2020).

To mitigate the risk of quantum attacks, researchers have proposed using quantum-resistant cryptography, such as lattice-based cryptography and hash-based cryptography (Zhang et al., 2020). However, implementing these solutions in existing blockchain systems may require significant changes to the network architecture and infrastructure (Conti et al., 2020).

3. ASSESSING THE EFFECTIVENESS OF DIFFERENT SECURITY MEASURES

Several security measures can mitigate the risks associated with blockchain systems, such as double-spending attacks, smart contract vulnerabilities, and privacy issues. Researchers have explored the effectiveness of these security measures in mitigating these risks. One of the significant security measures to prevent double-spending attacks is the consensus mechanism, where the network participants agree on the state of the blockchain ledger. Bitcoin uses the proof-of-work (PoW) consensus mechanism, where network participants compete to solve a mathematical puzzle to validate transactions and add new blocks to the blockchain.

Nakamoto (2008) proposed the PoW consensus mechanism for Bitcoin, which has been widely adopted in various blockchain systems. However, PoW has some limitations, such as high energy consumption, scalability issues, and vulnerability to 51% attacks. To mitigate these issues, alternative consensus mechanisms have been proposed, such as proof-of-stake (PoS), delegated proof-of-stake (DPoS), and practical Byzantine fault tolerance (PBFT).

Smart contract vulnerabilities can be mitigated by implementing security measures, such as code reviews, testing, and formal verification. Testing is a crucial security measure for smart contracts, as it can detect errors and vulnerabilities in the smart contract code. However, manual testing can be time-consuming and may not be able to cover all possible scenarios. Therefore, automated testing tools have been proposed to improve the efficiency and effectiveness of smart contract testing.

For example, Ma et al. (2018) proposed a tool called MAIAN, which uses symbolic execution and constraint solving to generate test cases for smart contracts. The tool can automatically detect vulnerabilities, such as integer overflow and division by zero, and generate exploit payloads to test the smart contract's resilience.

Privacy issues in blockchain systems can be addressed by implementing privacy-preserving protocols, such as zero-knowledge proofs (ZKPs). ZKPs allow users to prove the validity of a statement without revealing any additional information. Several privacy-preserving protocols have been proposed for blockchain systems, such as Zerocoin, Zerocash, and Hawk. However, these protocols have some limitations, such as high computational overhead and limited scalability.

Therefore, researchers have proposed alternative privacy-preserving protocols, such as bulletproofs and zk-SNARKs, which have lower computational overhead and better scalability. In addition to the security measures mentioned, researchers have also explored the effectiveness of other security measures in mitigating risks associated with blockchain systems. For instance, network partitioning has been proposed to prevent 51% attacks. Network partitioning involves splitting the network into multiple sub-networks to reduce the likelihood of a single entity controlling more than 50% of the network's computing power. This method has been proposed by Eyal and Sirer (2018) as a way of mitigating the risk of a 51% attack on blockchain systems.

Furthermore, multi-signature schemes have been proposed to mitigate the risk of funds being lost or stolen due to a single point of failure. Multi-signature schemes require multiple parties to sign off on a transaction before it can be executed, making it more difficult for funds to be misused. This security measure has been proposed by Andrychowicz et al. (2014) as a way of mitigating the risk of theft or fraud in blockchain systems. Secure hardware has been proposed as a security measure to protect private keys used to sign transactions on blockchain systems. Private keys are essential to blockchain systems as they enable users to access their digital assets. If private keys are lost or stolen, digital assets can be lost forever. Therefore, secure hardware, such as hardware wallets or smart cards, has been proposed to protect private keys from theft or loss. This security measure has been proposed by Androulaki et al. (2013) as a way of mitigating the risk of private key theft or loss.

Another security measure that can be implemented to mitigate the risks associated with blockchain systems is multi-factor authentication (MFA). MFA is a security mechanism that requires users to provide two or more authentication factors, such as a password and a fingerprint or a one-time code, to access a system. This can significantly reduce the risk of unauthorized access to a blockchain system, particularly for user-controlled wallets and exchanges. Researchers have suggested the use of MFA in blockchain systems, particularly for high-value transactions, to enhance security (Kshetri, 2018).

In addition to MFA, access control mechanisms can also be used to mitigate the risks associated with blockchain systems. Access control mechanisms can limit the privileges of users and ensure that only authorized users can access specific resources. Role-based access control (RBAC) is a commonly used access control mechanism that assigns users roles based on their responsibilities and permissions. Researchers have proposed the use of RBAC in blockchain systems to control access to smart contracts and other blockchain resources, reducing the risk of unauthorized access and potential damage to the system (Liu et al., 2019).

Finally, continuous monitoring and auditing of blockchain systems can help detect and prevent security breaches. Monitoring and auditing can identify suspicious activities and potential vulnerabilities, allowing for timely intervention to mitigate the risk. Researchers have proposed the use of real-time monitoring and auditing tools in blockchain systems, such as blockchain explorers, to enhance security and prevent security breaches (Liang et al., 2018).

4. IMPROVING THE SECURITY OF BLOCKCHAIN SYSTEMS

Based on the findings of the case studies and the analysis of different security measures, researchers have proposed recommendations for improving the security of blockchain systems. The recommendation to implement a robust consensus mechanism to prevent 51% attacks and ensure the integrity of the blockchain ledger has been proposed by researchers (Chen et al., 2018). Alternative consensus mechanisms, such as PoS, DPoS, and PBFT, have been suggested as having lower energy consumption, better scalability, and higher security than PoW (Lu et al., 2019).

For example, the EOS blockchain uses the DPoS consensus mechanism, which allows network participants to vote for block producers and distribute rewards based on their contributions to the network, resulting in a more decentralized and secure network than the PoW consensus mechanism (Croman et al., 2016). Another recommendation was the implementation of security measures, such as code reviews, testing, and formal verification, to mitigate smart contract vulnerabilities has been proposed by researchers (Atzei et al., 2017). Automated testing tools, such as MAIAN, have been suggested to improve the efficiency and effectiveness of smart contract testing and detect vulnerabilities that may be missed by manual testing (Albert et al., 2018). Formal verification has also been recommended to ensure the correctness of the smart contract code and detect potential vulnerabilities before the contract is deployed (Nikolic et al., 2014).

The recommendation to implement privacy-preserving protocols, such as ZKPs, bulletproofs, and zk-SNARKs, to address privacy issues in blockchain systems has been proposed by researchers (Kosba et al., 2016). These protocols have been suggested to enable secure and private transactions without revealing any sensitive information. However, it has been emphasized that these protocols should be carefully designed and implemented to ensure that they do not compromise the security or scalability of the blockchain system (Bonneau et al., 2015). In addition to the above recommendations, researchers have also proposed the use of multi-layered security measures to enhance the security of blockchain systems (Gai et al., 2018). This approach involves using multiple security layers, such as network security, application security, and physical security, to provide a comprehensive defense against various types of attacks.

Network security measures may include firewalls, intrusion detection and prevention systems, and secure communication protocols. Application security measures may involve access control, encryption, and authentication mechanisms. Physical security measures may include secure data storage and backup systems, secure hardware components, and disaster recovery plans.

Moreover, researchers have suggested the need for continuous monitoring and auditing of blockchain systems to identify and address any security vulnerabilities or breaches in a timely manner (Zhang et al., 2019). This can be achieved through the use of security analytics tools, such as SIEM (Security Information and Event Management) systems, which can analyze network traffic, detect anomalies, and generate alerts for potential security incidents. Regular security audits can also help to identify and address security gaps in the blockchain system.

Finally, researchers have emphasized the importance of user education and awareness in ensuring the security of blockchain systems (Dwyer et al., 2018). Users need to be aware of potential security risks and how to protect themselves against them, such as through the use of strong passwords, two-factor authentication, and secure storage of private keys. User education programs can also help to raise awareness and promote best security practices among blockchain users.

5. CONCLUSION

Blockchain technology offers a promising solution for secure data management, storage, and transaction processing. However, blockchain systems are not impervious to security vulnerabilities and attacks. Therefore, it is essential to evaluate the security of blockchain systems, identify potential vulnerabilities and attack surfaces, and assess the effectiveness of different security measures in mitigating risks. This literature review explored previous academic works related to these research objectives and provided recommendations for improving the security of blockchain systems. By implementing these recommendations, blockchain systems can be more secure, resilient, and trustworthy, enabling their adoption in various industries.

BIBLIOGRAPHY

Androulaki, E., Karame, G. O., & Capkun, S. (2013). Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 441-452).

Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, L. (2014). Secure multiparty computations on bitcoin. In International conference on financial cryptography and data security (pp. 443-452).

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (No. arXiv:1710.06085). arXiv preprint arXiv:1710.06085.

Azevedo, I., Santos, N., Antunes, N., & Vieira, M. (2020). Hybrid analysis for detecting vulnerabilities in smart contracts. Journal of Systems and Software, 169, 110711.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-238. https://doi.org/10.1257/jep.29.2.213

Bryman, A., & Bell, E. (2015). Business Research Methods. Oxford University Press.

Chen, Y., Li, X., Li, Z., Xie, J., & Li, X. (2018). Research on consensus algorithm and its improvement for blockchain. Journal of Physics: Conference Series, 1020(1), 012009.

Creswell, J. W. (2014). Research design: qualitative, quantitative, and mixed methods approaches. Sage publications.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2020). Blockchain for IoT security and privacy: The case study of a smart home. IEEE Communications Magazine, 58(9), 149-155. https://doi.org/10.1109/MCOM.001.2000244

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95-102.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. Qualitative inquiry, 12(2), 219-245.

Guo, J., Chen, H., Chen, X., Wang, X., & Xu, J. (2019). A penetration testing method for blockchain-based applications. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 171-178). IEEE.

Hassan, S., Chang, V., Javaid, Q., Ahmad, J., & Nazir, M. (2020). The blockchain technology for IoT applications: A review. IEEE Internet of Things Journal, 7(3), 2191-2204.

International Association of Trusted Blockchain Applications. (2020). INATBA Blockchain Security Guidelines. https://inatba.org/wp-content/uploads/2020/05/INATBA-Blockchain-Security-Guidelines.pdf

Joshi, A., Bisht, P., & Singh, M. P. (2019). Blockchain and security: a survey. Journal of Network and Computer Applications, 126, 50-67.

Karame, G. O., Androulaki, E., & Capkun, S. (2015). Double-spending fast payments in bitcoin. In Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security (pp. 906-917). https://doi.org/10.1145/2810103.2813677

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2018). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. Journal of Cloud Computing, 7(1), 4.

Liu, J., Zhang, N., & Liu, Z. (2019). Design and implementation of blockchain-based access control model for digital identity management. Security and Communication Networks, 2019, 1-15.

Liu, S., Huang, Y., Zhang, Y., Cheng, Z., & Feng, D. (2021). BASF: A blockchain attack surface framework. Future Generation Computer Systems, 119, 153-166. https://doi.org/10.1016/j.future.2021.06.017

Ma, J., Sun, X., Zhang, K., Zhao, Y., & Deng, R. H. (2018). Maian: A malware-resistant smart contract security framework. IEEE Transactions on Information Forensics and Security, 13(5), 1242-1255.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Shin, Y., Kim, H., & Kim, S. (2018). On Vulnerabilities of Ethereum Smart Contracts. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 658-663). IEEE.

Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media, Inc.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Yin, R. K. (2018). Case study research and applications: Design and methods. Sage publications.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?–a systematic review. PloS one, 11(10), e0163477.

Zerocash. (2018). Zerocash: Decentralized anonymous payments from bitcoin. Proceedings of the IEEE Symposium on Security and Privacy (SP), 459-474.

Zerocoin Electric Coin Company. (2018). Zerocoin Electric Coin Company Whitepapers. Retrieved from https://zerocoin.org/whitepapers/

Zhang, Y., Wen, Q., & Wang, J. (2018). Blockchain-based decentralized trust management in V2X networks. IEEE Communications Magazine, 56(7), 158-165.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 13(4), 352-375.

Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113.