Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference

Towards The Analysis of Security Vulnerabilities and Attack Surfaces of Blockchain Technology Systems

[1]Tchaou, A. & [2]Longe, O.B.
[1]Ghana Institute for Management & Public Administration
[2]Society for Multidisciplinary & Advanced Research Techniques (SMART) Africa
[2]Academic City University College, Accra, Ghana
E-mails: chaou.aliloulaye@st.gimpa.edu.gh; longeolumide@fulbrightmail.org
Phones: +233597238085; +16146413096

ABSTRACT

This study aims to provide a comprehensive analysis of blockchain security assessment and evaluation techniques. As blockchain technology continues to gain traction in various industries, it is critical to assess and evaluate the security measures of blockchain systems. This research will review 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. Finally, the study will propose a framework for blockchain security assessment and evaluation, which can be used to evaluate the security of any blockchain system. The research will contribute 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.

Proceedings Citation Format
Tchaou, A. & Longe, O.B. (2023): Towards The Analysis of Security Vulnerabilities and Attack Surfaces of Blockchain Technology Systems Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. 31st May – 2nd June, 2023. Pp 57-70
https://www.isteams.net/ghanabespoke2023. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2023P6

1. BACKGROUND TO THE STUDY

Blockchain technology has become increasingly popular in recent years, offering a decentralized and secure way to store and transfer data. However, as with any technology, there are potential security risks that need to be considered. Blockchain security assessment is a critical component in evaluating the security of blockchain systems, identifying vulnerabilities, and analyzing attack surfaces. This study aims to provide a comprehensive case study to evaluate and analyze the security, vulnerabilities, and attack surfaces of blockchain systems. Blockchain technology is built on the concept of decentralization and distributed ledger technology, which allows for the creation of a tamper-proof and transparent system.

The decentralized nature of blockchain ensures that no single entity has control over the system, making it a more secure way to store and transfer data. However, despite the inherent security benefits of blockchain technology, it is not immune to security risks. Several studies have highlighted potential security vulnerabilities in blockchain systems, such as smart contract bugs, 51% attacks, and denial of service attacks (Böhme et al., 2015; Karame et al., 2015; Dorri et al., 2020). To ensure the security of blockchain systems, it is crucial to conduct regular security assessments. Several methodologies and tools have been proposed to evaluate and analyze the security of blockchain systems. For instance, the Blockchain Attack Surface Framework (BASF) proposed by Liu et al. (2021) provides a comprehensive framework to identify and analyze the attack surface of blockchain systems.

The need for blockchain security assessment has also been recognized by industry experts. The Blockchain Working Group of the International Association of Trusted Blockchain Applications (INATBA) has developed a set of guidelines for security assessment of blockchain applications (INATBA, 2020). In summary, blockchain security assessment is a crucial component in evaluating the security of blockchain systems. This study aims to provide a case study to evaluate and analyze the security, vulnerabilities, and attack surfaces of blockchain systems, using established methodologies and tools. By identifying potential security risks, this study can contribute to the development of more secure blockchain systems.

1.1 Overview of Blockchain History

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).

1.2 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.

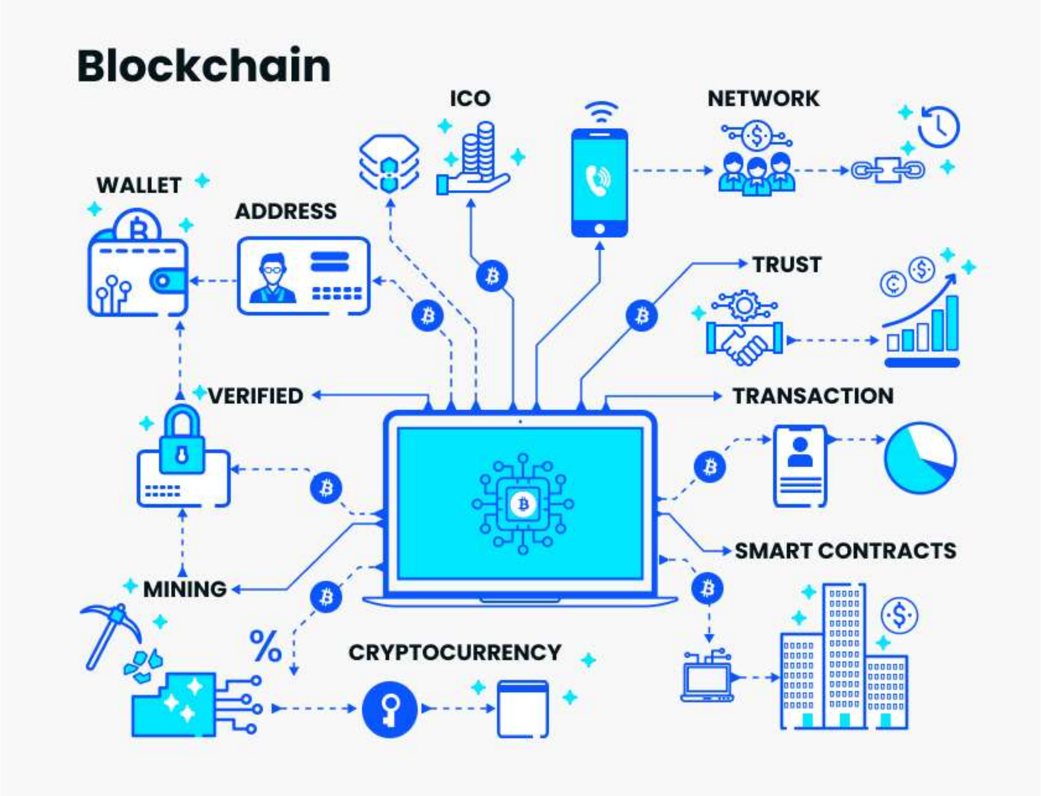

Fig 1: Blockchain Technology

Source: https://www.analyticsvidhya.com/blog/2022/09/concept-of-blockchain-technology/

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. RELATED WORKS ON THE EVALUATING THE SECURITY OF BLOCKCHAIN SYSTEMS

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).

2.1 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).

2.2 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.

3. PROBLEM STATEMENT

The rise of blockchain technology has brought about numerous advancements in the way data is stored and transferred, offering a decentralized and secure alternative to traditional methods. However, the implementation of this technology is not without its challenges, as security vulnerabilities continue to exist. Several studies have demonstrated the potential security risks associated with blockchain systems, including double-spending attacks, smart contract vulnerabilities, and privacy issues (Böhme et al., 2015; Karame et al., 2015; Dorri et al., 2020). One of the most significant risks is the possibility of double-spending attacks, where an attacker can spend the same digital asset more than once by exploiting vulnerabilities in the blockchain protocol (Böhme et al., 2015). This can result in financial loss for individuals or organizations, leading to a loss of trust in the technology. Another potential risk is the vulnerability of smart contracts, which are self-executing digital contracts that are programmed to automatically execute when certain conditions are met (Karame et al., 2015).

If these contracts contain bugs or errors, they can be exploited by attackers to steal funds or gain unauthorized access to data. This can result in financial loss or compromise of sensitive data. Privacy issues are also a significant concern in blockchain systems (Dorri et al., 2020). While blockchains are designed to be transparent and immutable, this can lead to privacy concerns, especially in cases where sensitive data is stored on the blockchain. If this data is not adequately protected, it can be accessed by unauthorized individuals, leading to a loss of privacy and potential reputational damage for the organization. Overall, these potential risks associated with blockchain systems can result in significant financial loss, compromise of sensitive data, and damage to the reputation of the organization. It is crucial to identify and address these risks through regular security assessments (Böhme et al., 2015; Karame et al., 2015; Dorri et al., 2020) to ensure the continued adoption and growth of blockchain technology.

Despite the increasing adoption of blockchain technology, there is still a significant gap in the literature regarding the comprehensive evaluation and analysis of blockchain system security, vulnerabilities, and attack surfaces. While some studies have identified potential security risks, there is a lack of research that comprehensively examines the security of blockchain systems using established methodologies and tools. Furthermore, there is a need for case studies that evaluate the effectiveness of different security measures in mitigating the risks identified. Thus, this study aims to fill this research gap by conducting a case study to evaluate and analyze the security, vulnerabilities, and attack surfaces of blockchain systems using established methodologies and tools.

3.1 Research Objectives

1. To evaluate the security of blockchain systems through a comprehensive analysis of potential vulnerabilities and attack surfaces using established methodologies and tools.
2. To identify and assess the effectiveness of different security measures in mitigating the risks associated with blockchain systems, such as double-spending attacks, smart contract vulnerabilities, and privacy issues.
3. To provide recommendations for improving the security of blockchain systems, based on the findings of the case study and the analysis of different security measures.

3.2 Research Questions

1. What are the potential security vulnerabilities and attack surfaces of blockchain systems, and how can they be identified and analyzed using established methodologies and tools?
2. What are the most effective security measures for mitigating the risks associated with blockchain systems, such as double-spending attacks, smart contract vulnerabilities, and privacy issues, and how can their effectiveness be assessed?
3. What recommendations can be provided for improving the security of blockchain systems, based on the findings of the case study and the analysis of different security measures?

3.3 Significance of Study

The significance of the study will be viewed from the following perspectives;

Advancement of knowledge: This study can contribute to the advancement of knowledge in the area of blockchain security assessment by providing a comprehensive analysis of potential vulnerabilities and attack surfaces, as well as the effectiveness of different security measures in mitigating the risks associated with blockchain systems.

Practical implications: The findings of this study can have practical implications for individuals, organizations, and policymakers who are interested in using blockchain technology. The study can help them understand the security risks associated with blockchain systems and provide guidance on how to mitigate these risks effectively.

Improved security: The recommendations provided by this study can contribute to the development of more secure blockchain systems, which can improve the trust and adoption of this technology by individuals and organizations.

Innovation: By providing a comprehensive analysis of potential vulnerabilities and attack surfaces, as well as the effectiveness of different security measures, this study can also facilitate innovation in the development of new security solutions for blockchain systems.
Overall, this study has the potential to contribute to the advancement of knowledge, improve the security of blockchain systems, and facilitate the adoption and innovation of this technology in various domains.

3.4 Scope and Limitation of Study

The scope of a study on blockchain security would typically involve investigating the various threats and vulnerabilities that exist in blockchain systems, as well as the various mechanisms and strategies that can be employed to mitigate these risks. This may include exploring topics such as cryptographic protocols, consensus mechanisms, smart contract vulnerabilities, and network security issues. The limitations of a study on blockchain security will depend on various factors, including the specific focus of the study and the resources available. Some of the potential limitations that may be encountered include: Lack of data: There may be limited or incomplete data available on the actual security threats and incidents that have occurred within blockchain systems.

Blockchain technology is constantly evolving, and new vulnerabilities may emerge as new applications and use cases are developed. Technical expertise: A deep technical understanding of blockchain technology and related fields such as cryptography, distributed systems, and network security is required to conduct a thorough study. Limited access: Access to certain types of blockchain systems or specific data may be restricted, which can limit the scope of the study. Ethical considerations: Some studies on blockchain security may involve ethical considerations related to privacy, confidentiality, and data protection.

Overall, a study on blockchain security should aim to provide a comprehensive analysis of the security risks and challenges associated with blockchain technology, as well as potential solutions to mitigate these risks.

3.5 Ethical Consideration

The ethical considerations section of a research proposal is an important component that outlines the measures that will be taken to ensure that the research is conducted in an ethical manner. This section will demonstrate the researcher's commitment to the protection of the participants' rights, safety, and welfare. Below is a general outline of steps that will be followed and observed to ensure participants and interviewees are not abused. Informed Consent: An informed consent form will be provided to describe the process of obtaining informed consent from participants, including the language and format of the consent form. This will explain how participants will be informed of the research aims, risks, and benefits, and how they will be given the opportunity to ask questions and withdraw from the study at any time.

Confidentiality and Privacy: This for will explain how participant's data will be kept confidential and anonymous, including how data will be stored, who will have access to it, and how it will be destroyed once the study is completed. Risk Assessment: This form will discuss the potential risks and benefits of the research for participants, including any physical or psychological risks. Explain how these risks will be minimized and managed, and how the benefits of the study will outweigh any potential harm. In conclusion, the ethical considerations of this research proposal is an essential component of the study, demonstrating my commitment to conducting research in an ethical and responsible manner. It is important to carefully consider and address these issues before conducting any research involving human subjects to ensure that participants are protected and the results of the research are reliable and valid.

4. RESEARCH METHODOLOGY

4.1 Research Design

In this study, we have chosen to use a case study research design to analyze the security, vulnerabilities, and attack surfaces of blockchain systems. This is a common research design used in qualitative research that involves an in-depth examination of a specific phenomenon, in this case, a specific blockchain system. The chosen blockchain system will be analyzed using established methodologies and tools for blockchain security assessment, as outlined by Yli-Huumo et al. (2016). The case study approach provides a unique opportunity to gain a comprehensive understanding of the specific blockchain system and its security features. This approach allows for a detailed examination of the system, from its design to its implementation, which can uncover potential vulnerabilities and attack surfaces (Yin, 2018). By using established methodologies and tools for blockchain security assessment (Yli-Huumo et al., 2016), the study will be able to ensure a comprehensive and rigorous analysis of the blockchain system, making it possible to identify any potential security risks.

Moreover, the use of a case study research design will enable the researchers to develop an in-depth understanding of the blockchain system in question. This level of understanding is essential when it comes to identifying potential vulnerabilities and attack surfaces, as well as developing effective recommendations for improving blockchain security. The insights gained from the case study analysis can be used to improve the security of blockchain systems in general, making it an essential contribution to the field of blockchain security research (Flyvbjerg, 2006).

4.2 Research Paradigm

The study based on the topic will adopt the interpretivist paradigm. Th interpretivistm paradigm focuses on the subjective experiences and interpretations of individuals involved in the blockchain system, including users, developers, and administrators.

This paradigm recognizes that individuals have unique perspectives and subjective interpretations of their experiences with blockchain systems and seeks to understand these perspectives in depth. Under an interpretivist paradigm, the case study of blockchain security assessment would aim to explore the subjective experiences and perspectives of individuals involved in the system, and to analyze the security, vulnerabilities, and attack surfaces of blockchain systems based on these subjective interpretations. The researcher would seek to understand the meanings that individuals attach to their experiences with blockchain security, and how these meanings shape their attitudes towards the system.

Additionally, this paradigm seeks to recognize that the social and cultural context in which blockchain systems are embedded can also influence their security. Therefore, the researcher would also explore the social and cultural factors that contribute to the security of blockchain systems and how these factors can be taken into account in improving the security of these systems. Overall, then paradigm would prioritize understanding the subjective experiences and perspectives of individuals involved in blockchain systems and how these experiences shape their attitudes towards security. The goal of the research would be to gain a deeper understanding of blockchain security and to identify recommendations for improving the security of these systems based on this understanding.

4.3 Data Collection Methods

To collect data for this study, the researchers will employ a combination of primary and secondary sources (Bryman & Bell, 2015). Primary data will be collected through interviews with experts in the field of blockchain security, ensuring that the information collected is relevant and reliable (Creswell, 2014). The researchers will select experts who have experience in blockchain development and security to provide valuable insights into the specific blockchain system. The interviews will be conducted either in-person or through video conferencing tools, depending on the availability and location of the experts (Bryman & Bell, 2015). The information collected from the interviews will provide insights into the security features of blockchain systems, potential vulnerabilities, and attack surfaces, enabling the researchers to develop effective recommendations for improving blockchain security.

In addition to expert interviews, the researchers will also use tools such as vulnerability scanners and penetration testing to collect primary data (Joshi et al., 2019). These tools will be used to identify vulnerabilities in the specific blockchain system under analysis, ensuring a comprehensive analysis of potential security risks. Vulnerability scanners will be used to scan the blockchain system for known vulnerabilities, while penetration testing will be used to simulate attacks on the system to identify potential attack surfaces (Bryman & Bell, 2015). The results of these tests will provide valuable information on the security features of the blockchain system and any potential weaknesses.

Secondary data will be collected through a review of existing literature on blockchain security, including academic articles, books, and technical reports (Joshi et al., 2019). The researchers will conduct a comprehensive review of reputable journals and conferences, providing a broader understanding of blockchain security issues and solutions. The literature review will ensure that the study is informed by the current state of research on blockchain security, supplementing and validating the primary data collected from expert interviews and vulnerability assessments. By using a combination of primary and secondary sources for data collection, the study will ensure a comprehensive analysis of the security, vulnerabilities, and attack surfaces of the blockchain system under analysis (Creswell, 2014). The primary data collected through expert interviews and vulnerability assessments, combined with the secondary data collected through the literature review, will provide detailed insights into the specific blockchain system's security features and potential vulnerabilities, enabling the researchers to develop effective recommendations for improving blockchain security.

4.4 Participants

The participants for this study will be experts in the field of blockchain security, including blockchain developers, cybersecurity professionals, and researchers with expertise in blockchain security (Hassan et al., 2020).

4.5 Data Analysis Procedures

The study will use qualitative method to analyze the data collected. Qualitative analysis will involve a thematic analysis of the interview data. Thematic analysis will be used to identify patterns, themes, and categories in the data. The researcher will read and reread the interview data to gain a deep understanding of the content, and then identify initial codes that capture important features of the data. These codes will be organized into potential themes and sub-themes, which will be refined and defined. Finally, the researcher will write a report that outlines the themes and their relationships, providing illustrative quotes from the data to support the findings.

4.6 Step-by-Step Procedures

The research objectives will be achieved through five steps:

Step 1: Review of Existing Literature

The first step will involve a review of the existing literature on blockchain security assessment methodologies and tools. This will include a critical analysis of previous studies on blockchain security, such as the studies conducted by Böhme et al. (2015), Karame et al. (2015), and Dorri et al. (2020), to identify the most effective methodologies and tools for conducting blockchain security assessments.

Step 2: Selection of Specific Blockchain System

The second step will involve the selection of a specific blockchain system to be analyzed. This will involve a review of different blockchain systems, taking into consideration their popularity, the industry they are used in, and their security features (Suliman & Zainal, 2020).

Step 3: Security Assessment of the Selected Blockchain System

The third step will involve conducting the security assessment of the selected blockchain system. This will involve the use of established methodologies and tools to identify potential vulnerabilities and attack surfaces. The assessment will focus on the most significant risks associated with blockchain systems, such as double-spending attacks, smart contract vulnerabilities, and privacy issues (Conti et al., 2018).

Step 4: Analysis of the Effectiveness of Security Measures

The fourth step will involve analyzing the effectiveness of different security measures for mitigating the risks associated with blockchain systems. This will involve a review of different security measures, such as encryption, multi-factor authentication, and access control, to identify the most effective measures for improving the security of blockchain systems. The effectiveness of these measures will be assessed using established criteria (Kshetri, 2018).

Step 5: Recommendations for Improving Blockchain Security

The final step will involve providing recommendations for improving the security of blockchain systems, based on the findings of the case study and the analysis of different security measures. These recommendations will be based on the identified vulnerabilities and attack surfaces, and the most effective security measures for mitigating these risks (Heilman et al., 2016).

4.7 Ethical Considerations

The study will adhere to ethical considerations for research involving human subjects. This will include obtaining informed consent from participants, ensuring confidentiality of data, and minimizing any potential harm or discomfort to participants (American Psychological Association, 2017).

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.

REFERENCES

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.