A Comprehensive Analysis of the Blockchain Threat Landscape: Security Attacks, Impacts & Countermeasures

Name: Deepa Ujjwal Mishra [1] Dr. Shraddha Phansalkar[2]
Affiliation[1]: Research Scholar, Dept. of Computer Science & Engineering MIT Art, Design and Technology University, Pune,
Affiliation[2]: Professor , Dept. of Computer Science & Engineering MIT Art, Design and Technology University, Pune,
Email id[1]: deepa.mishra@mituniversity.edu.in Email id[2]: shraddha.phansalkar@ mituniversity.edu.in

***Abstract*— Blockchain Technology has gained enormous market acceptance with its unique features like decentralization, anonymity, autonomy, integrity, immutability, verification, auditability, and transparency. This study conducts a comprehensive investigation of blockchain security, exploring its fundamental elements, public/private keys, consensus mechanisms, and smart contracts. It then focuses on common threats prevalent in Blockchain such as Double spending, Sybil attack, Liveness attack, 51% Vulnerability their impact and how to defend against them. It looks at hazards that exist in the actual world and offers risk assessment and mitigation techniques. The paper concludes with the importance of addressing Blockchain security to improved market adaptability and future research directions.**

Keywords*— Blockchain Security, Consensus, Smart Contracts, Blockchain attacks.

I. INTRODUCTION

In the realm of blockchain, information is stored within a distributed ledger. The primary function of blockchain technology is to ensure integrity and availability, enabling participants in the network to write, read, and verify transactions recorded in the distributed ledger[1,2]. Notably, this technology imposes restrictions on deletion and modification operations for transactions and other ledger data.

The security of the blockchain system is underpinned by cryptographic primitives and protocols, including digital signatures and hash functions. These cryptographic elements ensure that recorded transactions in the ledger maintain integrity, authenticity, and non-repudiation. Moreover, as a decentralized network, blockchain requires a consensus protocol, a set of rules adhered to by all participants to establish a globally unified view.

Operating in a trust less environment, blockchain offers users key features such as decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency, garnering significant attention from both academic and industrial spheres in recent years due to its advanced capabilities.

As blockchain implementations extend their reach into various sectors such as finance, healthcare, and supply chain, the imperative for security becomes fundamental to protect sensitive information, digital assets, and automated workflows. The importance of blockchain security manifests in its ability to cultivate trust among participants, alleviate risks linked to fraudulent activities and manipulations, and drive the broad acceptance of a technology that stands ready to transform conventional norms related to trust and accountability.

This paper is organized as follows: Section II explains the Blockchain architecture. Section III discusses the literature survey provides details about blockchain security attacks, and section IV discusses the applications of blockchain. Section V presents the various attacks on Blockchain, and Section VI provides the conclusion of the paper.

II. BLOCKCHAIN ARCHITECTURE

Blockchain Architecture [3] refers to the structural design of a peer-to-peer (P2P) network of nodes that acts as underlying framework for applications and systems. This network operates cohesively as a singular entity, resembling a virtual machine, despite the absence of a central authority overseeing the interaction among its nodes.

A. Nodes

A complete copy of the whole blockchain is stored on each of the nodes, or individual computers, that make up the blockchain network. Together, they verify transactions and agree on the ledger's current status. There are two types of nodes:

- Full Nodes: They take part in the consensus mechanism, validate transactions, along with keep a whole copy of the blockchain.

- Lightweight Nodes: They rely on complete nodes for validation of transactions, and these nodes keep a portion of a blockchain

B. Blocks

Blockchains are created chronologically by grouping transactions into blocks. A collection of transactions and a distinct identifier, or hash, are contained in each block. Blockchain immutability is ensured by an interconnected chain that is created when the hash of a block is generated based on both its content and the hash of the preceding block.

C. Consensus Mechanism

A consensus method is used to keep the blockchain state consistent amongst nodes. This system makes sure that nodes verify and concur on the order and validity of transactions. Proof of Work, Proof of Stake, Proof of Authority and Delegated Proof of Stake etc are widely used mechanisms that determine which node has the ability to contribute a new block.

 e-ISSN No. 2584-1025

In order to validate transactions and generate new blocks under Proof of Work (PoW), miners must solve intricate cryptographic puzzles. Mining is the term for this procedure, which uses a lot of computational power and, thus, electricity. PoW energy usage is frequently criticized for its negative effects on the environment. Large PoW networks, like Bitcoin, use around the same amount of energy as tiny nations.

PoS, however, does not need deciphering cryptographic riddles. Instead, the quantity of bitcoin that validators are ready to "stake" as collateral determines which of them gets to construct new blocks. PoS is significantly more energy-efficient than PoW because it doesn't require a lot of processing power. Compared to PoW, the PoS transaction validation method uses less electricity.

While PoS offers a more energy-efficient option with security based on pledged collateral and economic incentives, PoW is recognized for its high energy consumption and strong security model based on computational difficulty. The particular requirements and priorities of a blockchain network will determine which consensus algorithm is used, as each mechanism has distinct advantages and disadvantages.

D. Transactions

In a blockchain, transactions are the basic exchanges that take place. Transactions are the cornerstones for any kind of digital asset transfer, data recording, or smart contract execution. The address of the sender, the address of the receiver, the exchange amount, the timestamp, also a digital signature for authentication are all included in every transaction.

E. Smart Contract

A Smart contract is a self-executing programs that store terms and conditions for agreements. Smart Contracts provide for trustless and decentralized agreement execution without the need for middlemen by automatically executing when predetermined circumstances are met. Smart contracts use programming languages unique to the blockchain technology. On blockchain systems such as Ethereum, EOS, or Binance Smart Chain, smart contracts provide automated and untrusted code execution. Smart contract code is created and deployed by developers, who also give each contract a unique address and define its terms and activities. By sending transactions to these addresses, users can communicate with smart contracts by causing code execution. The consensus mechanism of the blockchain network verifies and processes transactions, guaranteeing their legality. On the blockchain, smart contracts save their state, guaranteeing security and immutability. They facilitate complicated decentralized apps (DApps) by handling the automatic transfer of digital assets and emitting events for interactions. Figure 1 shows Blockchain's essential features.

Fig. 1. Blockchain Features

III. Related Work

With an emphasis on its history, consensus algorithms, cryptography, smart contracts, applications, security threats, actual attacks, flaws, security measures, problems, and research trends, the paper [1] offers discussion of consensus mechanisms, cryptography, applications, security issues, actual attacks, bugs, and security solutions are all covered in this paper's comprehensive examination and analysis of blockchain technology. Using a thorough examination of blockchain technology and security concerns, the technique digs into cryptography, consensus algorithms, smart contracts, and history. To compile thorough findings from different research projects, the authors review papers from prestigious security conferences and journals. The summary of discussion includes various research trends and challenges in blockchain technology such as scalability on transactions and chain data sharing, audit, monitor and anomaly detection, privacy preserving techniques, quantum computing impact on blockchain, adoption of IOTA technology, and regulation and standards for blockchain. The impact of blockchain technology on multiple sectors is discussed in this paper [2], with a particular emphasis on IoT privacy issues and the implementation of privacy protection in IoT systems based on blockchain. Significance of blockchain in transforming the IT industry and its capacity to unite disparate entities is emphasized, along with the practical difficulties associated with privacy leakages in IoT systems and the requirement for strong privacy protection measures in blockchain-based IoT systems. In the Internet of Things domain, blockchain technology is revolutionizing security and governance. Paper discusses issues with privacy leaks in Internet of Things systems and offers fixes. IoT information systems improve governance, transparency, and dependability. The process includes outlining blockchain technology, talking about security flaws and threats, examining privacy breaches in Internet of Things systems, and making recommendations for how to preserve privacy. The article covers a wide range of topics, including blockchain attacks, security concerns, adoption barriers, applications, and advantages. It also summarizes current security solutions and unresolved research questions.

The paper [3] offers a methodical analysis of the security risks associated with blockchain technology, examines actual assaults on well-known blockchain systems, evaluates security augmentation techniques, and makes recommendations for future research paths in this field. The study's methodology includes a survey of actual assaults on blockchain systems to identify the vulnerabilities these attacks exploit as well as a methodical analysis of security threats to blockchain systems.

For blockchain security to be prominent[4,5], the cryptographic primitives that are employed must be strong and resilient. The security of blockchain systems may be jeopardized by theoretical flaws or dubious parameters in the standardized elliptic curves used in blockchain security. - Popular cryptographic algorithms used in blockchain, such ECC and ECDSA, are under risk from the impending era of quantum computing. Resolving this threat is important to blockchain systems security in future.

Survey based on the blockchain's consensus protocol attack [6-8]via most recent publications by different publishers was conducted as part of the study's methodology. The writers integrated a number of blockchain-related techniques and sought to clarify previously published studies in order to comment on several important techniques in the context of a survey study. They used targeted keywords to find referred papers in a survey of recently released referenced articles from a variety of sources. Cross-chain technologies offer a wide range of applications, including decentralized exchanges and new financial products. They are essential for facilitating interoperability across various blockchain networks. Cross-chain systems need to be extremely secure since any security lapses could cost all parties engaged in cross-chain transactions a lot of money. The necessity and importance of cross-chain technologies for upcoming blockchains is what inspired this research. The approach entails outlining and contrasting the most popular cross-chain technologies currently in use, examining several cross-chain system threats and suggesting countermeasures, and talking about takeaways and unresolved issues.

IV. Blockchain Applications

Blockchain Technology has applications in the following areas: cryptocurrency; finance; Internet of Things; digital records ; reputation system ; and security and privacy , the military, mobile applications, supply chain, automotive [9], identity management, voting, education, law and enforcement, asset tracking [10], , intrusion detection [11], digital ownership management, property title registries, healthcare, insurance, copyright protection, energy, and society applications like blockchain music, blockchain government, advertising [12]. Some other applications of Blockchain include:

A. Cross-Border Payments

Blockchain's provision of end-to-end remittance services, eliminating intermediaries, has streamlined cross-border transfers.

B. Certificates of Birth and Death

A large number of people worldwide lack a valid birth certificate, particularly in the world's poorer nations. A third of children under five do not have a birth certificate, according to UNICEF. Additionally, the issue is comparable to death certificates. On the flip side, blockchain offers a solution by creating a secure and authenticated database[13] for birth and death certificates, accessible solely to authorized individuals.

C. Royalties and Copyright

Blockchain applications have also made an impact on the creative sector, including music, cinema, and more. Copyright and royalties pose significant concerns in these artistic domains, seemingly unrelated to blockchain. However, this technology plays a vital role in ensuring security and transparency in creative industries. Instances of unauthorized copying of music, movies, artwork, etc., with insufficient attribution to the original creators, are not uncommon. Blockchain, featuring an extensive ledger of artist rights, offers a solution to this problem. Moreover, blockchain provides a transparent platform for recording artist royalties and agreements with major production companies. Digital currencies like Bitcoin can facilitate royalty payments. Figure 2 illustrates the diverse blockchain applications in various fields.

D. SupplyChain

There are several advantages to supply chain management when blockchain technology is used, such as:

- Enhanced Transparency, Traceability, and Trust

The transparent and unchangeable record of every transaction made inside the supply chain is the primary feature of the blockchain. This lowers the possibility of fraud, increases accountability, and makes it easier to track things from their point of origin to their destination. Additionally, this increases supply chain transparency and enables businesses to track goods and keep an eye on performance in real time. Consequently, this has the potential to enhance confidence across supply chain partners.

- Greater Efficiency Produces Speed

Blockchain technology can lower costs and boost efficiency in the supply chain by automating several procedures. This can entail tracking inventory levels, automating payments, or optimizing logistical procedures.

There are many use cases of Blockchain in Supply Chain such as finance, logistics, payments, food safety etc.

As sustainability and ESG considerations gain prominence, blockchain technology is increasingly utilized to enhance environmental sustainability by tracking carbon emissions and other ecological impacts throughout the supply chain. This data can pinpoint areas for improvement, thereby reducing the overall environmental footprint. Moreover, blockchain helps ensure products are ethically sourced by tracing their journey from origin, allowing businesses to detect and address issues like child or slave labor, fair wages, and safe working conditions within the supply chain.

- Quality Assurance

Blockchain technology ensures products meet specified quality standards throughout the supply chain. By recording data at each production stage on the blockchain, companies can monitor and verify compliance with these standards.

- Counterfeit Prevention

Counterfeiting is a major issue in industries such as luxury goods and pharmaceuticals. Blockchain technology combats this by creating a tamper-proof record of product ownership and authenticity, thereby preventing brand and product piracy.

- Streamlining Payment Processing

Blockchain also streamlines payment processing in supply chains. Smart contracts enable automated payments based on predefined conditions, such as delivery confirmation or quality inspection, making the process more efficient.

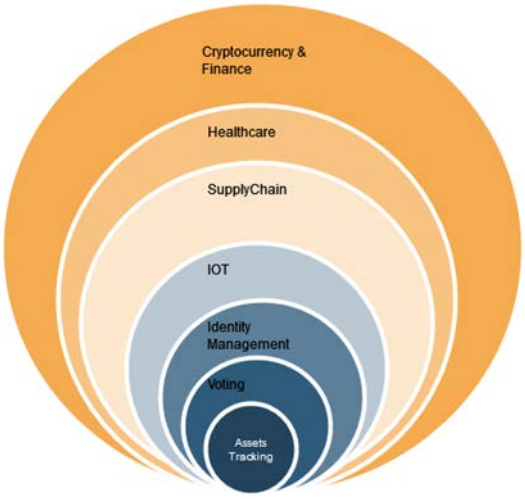

Fig. 2. Blockchain Applications

V. Attacks on Blockchain

Although Blockchain Technology is used to secure applications, there are security concerns on Blockchain that can lead to inconsistency in the blocks. Below are major attacks on Blockchain:

A. Double Spending Attacks

This issue arises when two successful transactions are made using the same funds. It could be a weakness in digital currency since it allows for the double spending of the same digital token. Despite the fact that every transaction is validated by the blockchain consensus mechanism, it is difficult to prevent double-spending [14]. According to the authors of a Bank of Canada study, "a miner theoretically loses their ability to control double spending incentives if they control more than half of all miners' computational capacity." This can be done by a dishonest or malevolent miner who raises the arrival rate over the total of all other honest or law-abiding miners [15]. Aspects of double spending that are attacked include Finney, 51%, Vector 76 attack and race.

1) Impact:

a) Loss of Trust: When double-spend attacks are successful, the impacted blockchain network's credibility is damaged, which discourages users and merchants from taking part.

b) Financial Losses: When transactions are accepted by double-spend attack victims and subsequently reversed, they may experience financial losses and possible disruptions to their business operations.

2) Countermeasures:

a) Using Consensus Mechanisms: Compared to conventional consensus mechanisms, advanced consensus mechanisms provide improved security against double-spending attacks.

b) Putting Zero-Confirmation Policies into Practice: Double-spending is more likely when transactions are accepted with zero confirmations from certain merchants and services. By putting in place regulations that need a certain amount of confirmations, this risk can be reduced.

B. Sybil Attack:

This attack exploits a vulnerability in computer security systems[16] by generating a fake identity within a peer-to-peer network, thereby compromising its reputation mechanism. In networks where nodes are required to authenticate themselves before gaining access, such as permissioned or private blockchains, the fabrication of identities becomes significantly more challenging. Soska and Christin (2015) introduced the "Beaver" system, which imposes fees to deter Sybil attacks while preserving users' privacy.

1) Impact:

The main consequence of the Sybil attack's consequences on blockchain networks is the prohibition of users from using those networks.. In a blockchain network, the phony nodes can overwhelm the real ones. Sybil nodes have the ability to drastically alter how the network functions once they take over. Above all, Sybil nodes have the ability to reject block additions or transmissions within a network. Consequently, the phony node can prevent other users from connecting to the network. The attacks may result in a brief decline in cryptocurrency values, which might harm blockchain protocols' standing.

2) Countermeasures:

a) Using Consensus Mechanisms: The creation of a reputation system is the most crucial aspect of Sybil blockchain attacks and defense strategies. Sybil attacks depend on the amount of fictitious identities increasing steadily. As a result, a reputation system might enable various network users to have distinct degrees of authority.

b) Graphs of Social Trust: Social trust graphs are a reliable addition to the arsenal of defenses against Sybil assaults. Social trust graphs function by thoroughly examining the connectivity information among the nodes. As a result, it can assist in locating and halting aberrant nodes before they cause harm.

C. Balance Attack

In order to carry out a transaction within one of these subsets[17], an attacker simply needs to introduce a delay between valid subsets possessing equal mining power. To ensure the dominance of the subtree belonging to the other subset over the transaction subset, the attacker proceeds to mine an ample number of blocks within those subsets. This allows the attacker to create a block containing a transaction with a strong likelihood of overtaking the subtree it's associated with, even if the transaction hasn't been confirmed.

D. 51% Vulnerability Attack:

To create mutual trust, blockchains use distributed consensus techniques[18]. Despite this, an attacker can take over the entire blockchain by taking advantage of a 51% weakness in the consensus system. In particular, a 51% attack may be launched in a PoW-based blockchain if a single small hash function accounts for more than 50% of the total hash function across the board. Because of this, if mining power is distributed among multiple mining pools, unforeseen circumstances may occur, as when one pool controls over 50% of the total processing power. For instance, in one actual instance, the mining pool "ghash.io" was responsible for over 42% of the mining power used to process bitcoins. 51% attacks are thought to pose a bigger risk to recently established blockchain networks since they are still relatively tiny and thus susceptible to takeover. Figure 3 shows the 51% attack scenario.

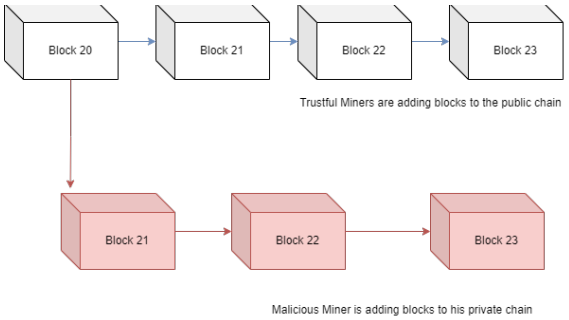

Fig. 3. 51% Attack Scenario

1) Impact:

After seizing control, the hacker temporarily disables other miners' addresses. This prevents the honourable miners from regaining control of the network. The attacker's fictitious series of transactions may thus end up being irreversible.

Reversing a transaction: An attacker may prevent payments from being made by any or all users. This interferes with the network's regular operation and may cause long delays in transaction confirmations, eroding users' faith in the dependability of the system.

2) Countermeasures:

a) Modifications to Consensus Algorithm: Changing to an alternative consensus algorithm is a workable strategy to lower the probability of 51% attacks. As Proof of Stake (PoS) consensus process necessitates that a hacker own the majority of the blockchain's entire stake—often an unaffordable endeavor—it is less vulnerable to these kinds of attacks.

b) Postponing Blockchain Verification: Delaying blockchain confirmations is another powerful disincentive. By using this technique, the network can gain time to recognize and possibly prevent a 51% attack. Attackers would have to maintain control over 51% of the network for a longer period of time in order to prolong the transaction confirmation time.

E. Liveness Attack:

Kiayias and Panagiotakos [19] presented two instances of such attacks on Bitcoin and Ethereum, suggesting that these attacks could potentially lead to delays in the acknowledgment times of targeted transactions. The liveness attack process, as outlined in three steps , involves blockchain latency, transaction denial, and preparation. This exploit aims to prolong the confirmation time of the transaction. During the preparation stage, the attacker seeks to gain an advantage over dishonest players to establish their private chain. Subsequently, in the transaction denial phase, the attack aims to delay the arrival of the block containing the transaction. If the delay appears insufficiently convincing, the attacker progresses to the blockchain render phase, where they endeavor to decelerate the rate at which the chain transaction grows.

1) Impact: Ability of the blockchain to advance and come to a consensus is the goal of liveness denial attacks, as opposed to conventional denial-of-service (DoS) attacks[20], which concentrate on blocking access to a service.

2) Countermeasures:

a) Dynamic Transaction Prioritization and charge rules: By guaranteeing that network resources are distributed effectively, the implementation of dynamic transaction prioritization methods and charge rules can assist reduce liveness denial attacks. The blockchain can prioritise valid transactions and disincentivize spam by dynamically altering transaction fees based on network factors such as congestion levels and transaction volume. Creating algorithms that rank transactions according to criteria like user reputation, transaction value, and urgency is the solution to this problem. Furthermore, rate limitation or adaptive charge structures that identify and penalize spam transactions can assist minimize network congestion and guarantee smoother transaction processing [21].

b) Improving Consensus Algorithms and Adaptive Network Protocols: Improving Consensus Algorithms and Network Protocols to Mitigate Liveness Denial Attacks and Adapt to Changing Conditions and mitigate Liveness attack.

VI. Conclusion & Future Scope

Blockchain is an emerging technology that has varied applications in various sectors including Finance, Supply chain, Healthcare, IoT and many more. Investigating the security of Blockchain is a critical aspect in the market adoptability of the technology for developing applications. The intelligent properties of smart contracts are demonstrated by their programmability and autonomous execution; enhancing the blockchain technology security will assist for enhancing the overall Smart Contracts security design.

Future research scope for enhancing the security of Blockchain involves investigating Machine learning and Deep Learning algorithms for detection of attacks & suggestion of mitigation strategies. Also investigating which algorithms are efficient and more accurate in detection is a matter of research.

References

[1] A survey on blockchain technology and its security Huaqun Guo a, Xingjie Yu b, Blockchain: Research and Applications Volume 3, Issue 2, Elsevier, June 2022.

[2] Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network SAURABH SINGH, A.S.M. SANWAR HOSEN , and BYUNGUN YOON , IEEE January 2021 IEEE Access PP(99):1-1 DOI:10.1109/ACCESS.2021.3051602

[3] Z. Zheng, S. Xie, H. N. Dai, X. C., and H. Wang. "Blockchain challenges and opportunities: a survey." International Journal of Web and Grid Services 14, no. 4 (2018): 352-375.

[4] S. Singh, I. H. Ra, W. Meng, M. Kaur and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," International Journal of Distributed Sensor Networks, Vol. 15, no. 4, pp.1-17, 2019.

[5] X. Jiang, M. Liu, C. Yang, Y. Liu and R. Wang: A Blockchain Based Authentication Protocol for WLAN Mesh Security Access, Computers, Materials & Continua, Vol. 58, No. 1, pp. 45-59, 2019.

[6] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen and H. Kim: BlockchainBased Trusted Electronic Records Preservation in Cloud Storage, Computers, Materials & Continua, Vol. 58, No. 1, pp. 135-151, 2019.

[7] R. Song, Y. Song, Z. Liu, M. Tang and K. Zhou: GaiaWorld: A Novel Blockchain System Based on Competitive PoS Consensus Mechanism, Computers, Materials & Continua, Vol. 60, No. 3, pp.973-987, 2019.

[8] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng, H. Zhao, D. Wang and L. Xu: Research on Public Opinion Propagation Model in Social Network Based on Blockchain, Computers, Materials & Continua, Vol. 60, No. 3, pp.1015-1027, 2019.

[9] NEM, NEM Technical Reference. https://nemplatform.com/wp-content/uploads/ 2020/05/NEM_techRef.pdf, 2018.

[10] K. Karantias, A. Kiayias, D. Zindros, Proof-of-Burn, in: J. Bonneau, N. Heninger (Eds.), Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science, vol. 12059, Springer, Cham, 2020, pp. 523–540.

[11] A. Hayes, Proof of Capacity (cryptocurrency), Invest, 2020. Available online: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp.

[12] L.S. Sankar, S. M, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in: 2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017); 6–7 Jan 2017; Coimbatore, India, IEEE, Piscataway, NJ, USA, 2017, pp. 1–5.

[13] Z. Zheng, S. Xie, H. Dai, et al., An overview of blockchain technology: architecture, consensus, and future trends, in: IEEE 6th International Congress on Big Data; 25–30 Jun 2017; Honolulu, HI, USA, IEEE, Piscataway, NJ, USA: IEEE, 2017, pp. 557–564.

[14] A.P. Joshi, M. Han, Y. Wang, A survey on security and privacy issues of blockchain technology, Mathematical Foundations of Computing 1 (2) (May 2018) 121–147.

[15] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generat. Comput. Syst. 107 (June 2020) 841–853.

[16] E.J. De Aguiar, B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchain based strategies for healthcare, ACM Comput. Surv. 53 (2) (2021) 1–27.

[17] H.T.M. Gamage, H.D. Weerasinghe, N.G.J. Dias, A survey on blockchain technology concepts, applications, and issues, SN Computer Science 1 (114) (2020).

[18] D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, A survey on blockchain for information systems management and security, Inf. Process. Manag. 58 (1) (January 2021).

[19] On Trees, Chains and Fast Transactions in the Blockchain, Aggelos Kiayias & Giorgos Panagiotakos, Part of the book series: Lecture Notes in Computer Science ((LNSC,volume 11368))

[20] H. Poston, Mapping the OWASP top ten to blockchain, Procedia Comput. Sci. 177 (2020) 613–617.

[21] Ji.H. Park, Jo.H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry 9 (8) (2017) 164