Blockchain Vulnerabilities and Recent Security Challenges: A Review Paper

1st Aysha AlFaw
College of Information Technology
University of Bahrain
Sakhir, Bahrain

2nd Wael Elmedany
College of Information Technology
University of Bahrain
Sakhir, Bahrain

3nd Mhd Saeed Sharif
School of Architecture
Computing and Engineering
University of East London
London, England
s.sharif@uel.ac.uk

***Abstract*—Blockchain is a relatively new technology, a distributed database used for sharing between nodes of computer networks. A blockchain stores all information in automated digital format as a database. Blockchain innovation ensures the accuracy and security of the data record and generates trust without the need for a trusted third party. The objectives of this paper are to determine the security risk of the blockchain systems, analyze the vulnerabilities exploited on the blockchain, and identify recent security challenges that the blockchain faces. This review paper presents some of the previous studies of the security threats that blockchain faces and reviews the security enhancement solutions for blockchain vulnerabilities. There are some studies on blockchain security issues, but there is no systematic examination of the problem, despite the blockchain system's security threats. An observational research methodology was used in this research. Through this methodology, many research related to blockchain threats and vulnerabilities obtained . The outcomes of this research are to Identify the most important security threats faced by the blockchain and consideration of security recently vulnerabilities. Processes and methods for dealing with security concerns are examined. Intelligent corporate security academic challenges and limitations are covered throughout this review. The goal of this review is to serve as a platform as well as a reference point for future work on blockchain-based security.**

***Index Terms*—security, blockchain, blockchain threat, blockchain vulnerabilities**

I. Introduction

In recent years, the blockchain system has become increasingly popular, as it is known as a system that records information. A blockchain is a distributed database that makes the process of recording transactions in a business network easy. One of the main reasons for interest in blockchain is its advantages, which provide security, data integrity, and anonymity without any third-party interference in controlling transactions. Besides that, the blockchain provides some important characteristics,such as:

- Distributed:each network entity has a copy of the ledger, ensuring complete transparency.
- Immutable:any validated record cannot be undone and cannot be changed.
- Time-stamp:every block contains a timestamp and this offers information about the data's freshness.
- Unanimous:all entities agree that all of records will be validated [1].

Blockchain technology is used in the latest technologies such as artificial intelligence, virtual reality, the IoT, supply chain management, and cyber security. Blockchain technology faces many challenges that continue to raise concerns, such as security, privacy, compliance, and governance [2]. Secure peer-to-peer communication is allowed by blockchain technology and the transactions are publicly available for reading , but no one can modify the transaction once it has been recorded [3]. Although most of these technologies are constantly being developed, it can be challenging to comprehend the security implications or threats they pose [4]. Many people consider blockchain to be a technological breakthrough in cybersecurity or cryptography. It is also the basis of digital cryptocurrencies such as Bitcoin and smart contracts. The blockchain has increased its absolute importance in the digital world by retaining its critical attributes of decentralization, immutability, anonymity, and suitability for the electronic money transaction process. On the other hand, the successful experience in Blockchain attracts several organizations to research how Blockchain technology can be used to build different decentralized applications [5].

This study reviews blockchain types, which are divided into three categories: permission blockchains, permissionless blockchains, and consortium blockchains. In addition, the paper explains the security risks and privacy concerns, then deals with the most important issue related to the blockchain system, namely the security vulnerabilities. The paper is based on recent studies that have presented the modern security vulnerabilities that the blockchain is exposed to. Then explores the importance of finding a solution to these problems, as the paper describes some of the blockchain attacks and recent challenges to its security.

II. Literature Review

Recently, many studies have been published on security and solutions that are related to the blockchain, especially with regard to security issues and vulnerabilities. Blockchain is really used in a variety of fields, including education, medicine and government. There are numerous issues with the blockchain's security, performance, and authority. As is well known, security is the foundation for ensuring blockchain

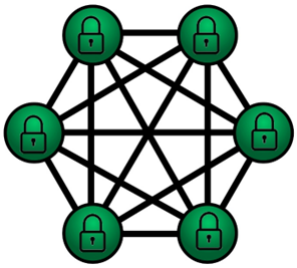

Fig. 1. Permissioned blockchain

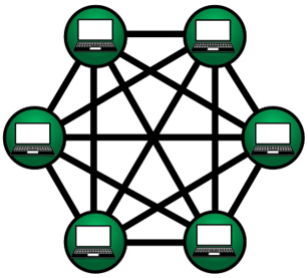

Fig. 2. Permissionless blockchain

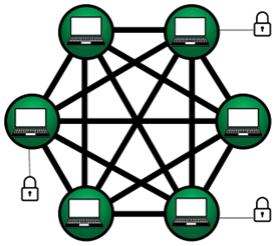

Fig. 3. Consortium blockchain

operations and is one of the essential criteria for blockchain adoption. However, getting to know the types of blockchain is one of the essentials to knowing the levels of security in each type [6].

A. Classification of Blockchains

One of the critical design decisions for blockchain-based systems is the access method. Access to the blockchain is classified into three types, as shown below:

1) Permissioned blockchain:: A permissions blockchain, commonly known as a private distributed ledger is not publicly accessed. To access the permissions blockchain, users need to identify themselves digitally, either by obtaining certificates or by using other means to access them. Businesses are discovering the benefits of permissioned blockchains and are increasingly using that.This type of blockchain is preferred by entities that need to define identities, roles, and security in the blockchain.

A blockchain's core structure, such as Ripple's, defines the participation roles that allow certain parties to access or publish information on the blockchain, then agree to give and accept new participants. Since different users in this type of blockchain have different permissions to control access, the authorized blockchain is considered partially decentralized. In addition to the security provided by conventional blockchain schemes like Bitcoin, permissioned blockchains also require a layer of access control. Figure 1 shows a private blockchain. [5].

2) Permissionless blockchain:: The permissionless blockchain stands for a public blockchain that is open source. best described as allowing "records to be shared by all network users, updated by miners, monitored by all, and not owned and controlled by anyone. Every transaction on public blockchains is entirely transparent, which means anyone can examine the details of the transaction. This type of blockchain has the advantage of decentralization and has been supported by the success of many applications, including cryptocurrencies such as Bitcoin [5] [7].Figure 2 shows the public blockchain.

3) Consortium blockchain:: The consortium blockchain is also known as the Federation blockchain. This type of blockchain provides a balance between the private and public, and it is considered partially decentralized, such as hyperledger and R3CEV, which are both consortium blockchains. This technology enables organizations to find solutions, saving time and money on development. The network security offered by this type of blockchain is different from public chains. Additionally, it enables significant levels of control, faster processing, and greater efficiency and security. Figure 3 shows the Consortium blockchain.

[8].

TABLE I
BLOCKCHAINS TECHNOLOGY CLASSIFICATION

Types of blockchain	Description	Scenarios
Permissionless blockchain	Anyone can participate, and it is accessible from anywhere on the world.	Decentralized global scenarios
Consortium Blockchain	Controlled by the consortium's pre-selected nodes	Selected organisations' businesses
Permissions blockchain	An organisation is in charge of writing rights.	In an organization, information sharing and management are essential.

These three types of blockchain all have essential characteristics, as shown in table 1. Transactions all rely on decentralized peer-to-peer networks, and they all require that each transaction be digitally signed and only added to the blockchain once [9].

B. Security and privacy

Since the blockchain eliminates the need for a central authority, a person can not simply change any properties of the network for their own benefit. In addition to decentralization, cryptography puts another layer of protection for users on blockcahin [10]. Cryptography is a way to ensure the availability and security of blockchain, especially in the use

of hash functions. To assess the blockchain security, it is a necessary to look at it from the of cryptography, which means looking at the attackers analysis of the cryptographic algorithm, The relationship between the security concepts of a cryptographic system and the difficult mathematical problems , and the potential disadvantages of a cryptographic system presented by the practical application environment [11]

Many studies related to blockchain security and privacy have focused on two threads:

- Disclosure of some attacks on blockchain-based systems.
- Making specific proposals to use some of the latest countermeasures against a subset of these attacks [9].

A recent study [12] used a survey to present a description of blockchain security and privacy features, dividing them into two categories: inherent attributes and additional attributes in online transactions.The security and privacy of the blockchain-based system and the application techniques to achieve privacy attributes include, for example, anonymous signatures and non-interactive zero-knowledge proof.
A research paper discussed the current regulatory concerns and integrated cost issues, as well as the blockchain fork issue, which causes security issues and challenges [8].

It has been found that blockchain has grown dominant in resolving security and privacy challenges across several governments and private sectors as a significant factor influencing development that impacts technology to attract a wide range of applications. [13].

There are some approaches for improving blockchain security and privacy are presented in the section below:

1) Digital signature: It is possible to protect a user's privacy by using anonymous digital signatures. Blockchain-based technology uses signatures like "ring signature" as well as "group signature" to enhance anonymity. In the group signature approach, each participant is given their shared public key as well as their private key. Any group member could use the private key to verify on behalf of its members, which could be verified by other participants using the shared public key [14]. Studies show that using an RSA electronic signature on the blockchain increases the ledger's integrity and promotes wireless network standards of care and security. The suggested solution uses the Blockchain with RSA digital signatures to verify that the flow of information in all forms of communication is secure and trusted [13].

2) Zero-knowledge proof (ZKP): The cryptographic approach ZKP used to verify the volume of a transaction inside the blockchain network without revealing confidential transaction information. Hung et al. [15].proposed a blockchain-based reliable data consistency checking system that employs efficient verifiable delay functions, smart contracts, and Evidence of Retrieval to guarantee that outsourced data from a data server is constantly retrievable using zero-knowledge data protection for the client.

3) Attribute Based Encryption Algorithm(ABE): ABE is the most commonly used technique among public key-based authentication techniques. ABE uses attributes to achieve flexible one-to-many encryption. The decryption of a ciphertext is only allowed if the user's key set of attributes matches the ciphertext attributes [16]. Despite its effectiveness, the ABE has still not been widely employed due to a lack of knowledge of its ideas and implementation details. Blockchain installation could be made possible by using it as a monitoring mechanism for the authority in respect of issuing tokens [17].
The novel anonymity blockchain infrastructure for IoT techniques that rely on (ABE) approaches was developed in a review article. Secure and quantitative evaluations were given for the proposed strategy to be tested in that approach. [18].

C. Security Threats and Common vulnerabilities

The blockchain system currently has numerous issues with authority and security, and this paper focuses on some of these issues. Wang et al. [6] discussed some security issues, such as underlying code security. This means that the code of a blockchain, particularly a public blockchain, should be open source, shareable, and auditable. Because it is open-source, more people will be able to participate, but the open-source will also make it easier to attack the blockchain.
A study focused on the dearth of comprehensive analyses of threats, blockchain threats are broken down into three categories: security threats to the blockchain data structure; vulnerabilities in peer-to-peer data transmission, and vulnerabilities in the blockchain apps. A total of 17 assaults are outlined by the authors in their paper. [19].
Blockchain-based systems are also examined in this paper [20]. The previous work focuses mostly on highlighting vulnerabilities in Bitcoin's privacy and security as well as its proof-of-work sense of satisfaction. A description of current remedies to these dangers is provided by the researchers in order to highlight one specific implementation of distributed ledger technology.Besides providing a detailed review of blockchain data protection, and construct a reference architectural model, that they examine inside the duration of the study, highlighting flaws and possible areas of threat in the process. There are four attacking surfaces provided by the scholars, as well as graphs are used to represent assaults including sets of intrusions in order to uncover causal links. There are a total of 29 intrusions that the reserchers have identified. Ethereum smart contracts, the particular implementation of a blockchain network ,are examined in this reserch paper [21]. There are no assaults on those other consensus methods because this research is exclusive to the Ethereum platform.
Zhou et al. [22]provides a further method for arranging assaults in 2020. Systematizing threats on Bitcoin, the researchers allocate assaults to three groups aimed at a specific area of information: confidentiality, availability of data, and data consistency intrusions.
In addition, a research paper [23] takes an in-depth look at the many ways in which blockchain technologies are vulnerable to cyberattacks. Threats to Bitcoin's proof-of-work consensus process are the only ones considered here.
Broad descriptions of attacks against blockchain networks

have appeared infrequently recently. While attempting to offer a complete review, are nonetheless restricted in scope. The document that lists the most attacks has 49 of them. The limitation of replication is also a result of the authors' lack of transparency in their methodological approach [24].

Maleh et al. [25] classified the blockchain vulnerabilities and threats into five categories, as shown in table 2. This research will focus on the first two points, the most critical vulnerabilities in blockchain technology.

TABLE II
BLOCKCHAIN THREATS AND VULNERABILITIES

Type	Classification
Client vulnerabilities	Digital signature vulnerabilities, Hash function vulnerabilities , Mining Malware , Software flows, User addresses vulnerabilities,
Consensus mechanism vulnerabilities	51% Attack, Alternative history attack, Finney attack, Race attack, Vector76 attack
Mining pool vulnerabilities	Block withholding attack, Birbery attack, The selfish mining attack, Pool hopping attack, Fork after withholding attack
Network vulnerabilities	Delay attack, sybil attack, DDos attack, Transaction malleability attack, Timejacking attack
Smart contract vulnerabilities	EVM bytecode vulnerabilities,Solidity vulnerabilities

1) Client vulnerabilities:

- Digital signature vulnerabilities:
  The Elliptic Curve technique is Bitcoin's standard kind of asymmetric encryption. Bitcoin addresses are generated through elliptic curve public keys, whereas ECDSA digital certificates are used to validate the transactions. Inadequate randomization is provided by elliptic curve cryptography, resulting in a danger to the participant's private key. There must be random data linked with the private key to every operation to establish a digital certificate [26].

  The process of verification and signature (ECDSA), which requires only one inversion operation, significantly affects the efficiency of digital signatures. Most research techniques have improved efficiency by reducing reverse operations, but they have ignored difficulties like forged signature attacks. Concurrently, the poor randomness of ECDSA on the blockchain will result in a forging random number attack. By the way, that is a potential issue with digital currency transactions [27].
- Hash function vulnerabilities: Cryptographic primitives ensure the validity and accuracy of operations in various blockchain networks, such as the BTC blockchain. These primitives have become breakable due to rapid advances in processing power and advanced cryptanalysis. The hash function is one of these primitives. For instance, the hash function employed in the Bitcoin blockchain, SHA256, is subject to various cybersecurity vulnerabilities, including preimage and collision attacks [28].
- Mining malware: Cryptocurrency mining in support of perpetrators is called "illegal crypto-mining" since clients' assets are being used. Browsers' crypto-jacking has been the topic of the latest studies [29].
  For example, an attacker might exploit a malware and mobile device's computing power in order to mine the block of cryptocurrency, which takes quite a bit of power and might even harm the user's system operation [25].
- Users Addresses Vulnerability : Identity fraud is possible since the Bitcoin blockchain credentials are not authenticated. The man-in-the-middle approach, for example, might be used by an intruder to change the intended BTC number to the opponent's address. The marketer might well commit vandalism on the specific website in an attempt to grab money from the victim. Due to the difficulty of returning a payment once it has been accepted and registered on the bitcoin, an attack like this might have deadly results [30].

2) Consensus mechanism vulnerabilities:

- 51% Attack: According to a study [31], 51% of attacks occur due to the consensus algorithm. The consensus algorithm is in charge of picking the metals accountable for solving mathematical problems. The blocks will be added to the chain and disseminated throughout the network after it is solved. An attacker can take control of the blockchain if he or she has more than 50% of the computer power. Attackers use their overwhelming computer power to seize control, generate the block, and then fork the chain.
- Finny attack A Finney attack is a blockchain attack in which an attacker impersonates a miner, mines a block, and conducts a transaction in stealth mode. Then he sells the currency to a merchant, who accepts the transaction despite the network's failure to validate it. After that, the miner publishes the block and confirms the previous transaction. The miner is double-spending as a result of this study. [32].
- Race attack Since the attacker may enjoy the benefits of the time lag between the transaction's issuance and validation inside a blockchain system using the Pow technique, such a threat is straightforward. There was a double-spending vulnerability because an offender had gotten the genesis operation results without mining the verification transaction [33].

D. Recent security challenges

1) Privacy: The lack of privacy and secrecy that occurs with blockchain transactions is exacerbated because each network has access to data on some other nodes. Thus, anybody following the blockchain may see every transaction. This topic has been addressed in several studies. However, the approaches offered only address a subset of concerns and cannot be used universally [34].

Due to the large volume of data being transmitted, attackers may employ assaults such as man-in-the- Transaction Malleability -middle (MitM) and DoS/DDoS to intercept conversations containing sensitive data. The Internet of Things raised many new privacy issues, such as the collection and use of personal data and the potential for vehicle and phone tracking. The recognizer is also being used to enable devices to communicate massive data stores for computation while monitoring talks [35].

2) The transaction Malleability: It is relatively unusual for a convention not to include all of the data in the hashed operation in contract transactions. On the other hand, the access point can modify the operation of the network to prevent validation of the hash.
Khan et al. [36] published the analysis to find situations that may lead to a successful transactional malleability assault in a blockchain network and emphasized the elements contributing to specific threats to help develop protection measures. The study successfully simulated a transaction reversibility threat inside the framework of blockchain-based online voting.

3) Redundancy: Costly replication in order to remove the arbitrator, which enables every system node to get a duplicate of every operation. It is financially and legally unreasonable for a bank to complete each transaction for every item accessible through illegal operations of an institution or via completion of other institutions' transactions. As a result of such redundancy, the overall cost is increased while no additional value is provided [37].

4) Regulatory Compliance: Blockchain technology addresses a variety of regulatory challenges that are similar to many different use cases, such as privacy, while others are specific to specific usess [38]. Regardless of the law, the blockchain is accurate. Government officials do not always modify how they execute their duties due to their presence. Non-Bitcoin currencies face regulatory obstacles when using blockchain technology in the financial and legal sectors, even though infrastructure regulation is very close to blockchain regulation [35].

5) Criminal Activity: Users can buy and sell a wide range of things using Bitcoin-enabled third-party trading sites. Because these systems are anonymous, tracking user behavior and imposing legitimate consequences is challenging. Bitcoin-related criminal behavior typically includes the underground markets at the moment, ransomware, in addition to money laundering. Due to illegal activities, the underground markets that operate online trade as or hidden services use Bitcoin as an exchange currency, and blockchain availability is uncertain. [37].

E. Smart Contract

It has been demonstrated that smart contracts can reduce the cost of administration by changing traditional business operations and broadening the use of blockchain technology to domains outside of bitcoin. Despite this, security vulnerabilities have become a significant worry due to the rapid growth and extensive deployment of digital currencies. As a result, they have gained much attention from various sources. As a reaction to this, a significant amount of work has been done in the past years to enhance and promote the safe design and deployment of intelligent transactions by providing novel and cutting-edge solutions for the identification of vulnerabilities and the protection of users' privacy. As a response to this, there is an urgent requirement for an in-depth analysis of the most recent advancements in security-enhancing technology for blockchain-based smart contracts. Based on the relevant literature released in the past several years, this study [39] offers an overview of the current academic status and achievements in the field of intelligent contract vulnerability. Abstract interpretation, symbolic execution, fuzz testing, deep learning, formal verification, and privacy improvement are the six subheadings that make up the areas of their review, which follow the technological trend of dividing it into categories.

III. Security solution

This section has taken a look at some of the current blockchain remedies that have been offered for use in various industries. In this study, the fundamental idea, major traits, features, and limits of previously conducted research on blockchain solutions are the primary discussion topics. The focus on how to solve the risks associated with blockchain security may be the main reason for making blockchain technology attractive to organizations. Many organizations have resorted to using hardware security components that are well-equipped with blockchain handling methods to counter any threats from hackers to avoid being hacked. The number of verification stages for transactions can be increased in a private blockchain environment to ensure that transactions are approved only by authorized and trustworthy business participant entities. Cryptography keys must also be distributed securely exclusively within the network of participating businesses. Any significant blockchain security risk can be mitigated with a domain-specific blockchain design [40].

A. Health Care

Linn et al. [41]found simple yet effective blockchain usage for keeping people's health information secure. Such technology allows every person's whole medical record to be maintained on a unique blockchain, which benefits both patients and healthcare providers. The majority of information is kept inside data lakes, which makes it possible to do basic and complex forms of analysis and deep learning. Data lakes are easy-to-use environments for storing a wide variety of information; the blockchain for every user provides an index catalog as well as a one-of-a-kind user identifier, the data encryption link, and a checksum, which indicate the most recent data variations.

Additionally, Alhadhrami et al. [42] explored how distributed ledgers may be utilized in the medical industry to manage, authenticate, and organize data, mainly information concerning consortium blockchains. They are acceptable blockchains, inside which the node administrator, as well as

the miners, retain control over who may view the blockchain. The concept of consensus would be at the heart of the jobs completed by consortium blockchains, which seek to determine the optimal number of information checks. Patel described the design of a cross-domain image-sharing digital ledger, which enables the interaction of people with radiological and medical pictures built on the consensus blockchain. This network might be used for a variety of applications. The system developed by the researcher seeks consensus among a relatively small number of trusted institutions in order to sustain a more careful consensus that would require less work to maintain the sophisticated privacy and security modules.

B. Transaction Sectors

Turner et al. [43]explored how bitcoin is used for unethical purposes, including illegal acts on the internet. The anonymity provided by Bitcoin transactions is perhaps its most appealing quality; the transactions themselves obscure any information that may be used to identify a user. Previous investigations into Bitcoin users relied primarily on meticulous study of transaction patterns ('for instance, where stolen public keys are being used'). The utilization of Bitcoin Fog or dark wallets, in which many transactions containing a single bank account are released to a destination node all at once, continues to be a problem in this context. Actions on the blockchain that include piggy banking are frequently anonymized since it is hard to determine the beneficiary of the transaction. In addition, if the Tor browsers are used in conjunction with piggy banking, then the exchange process is entirely secret, and it is not feasible to monitor it.

IV. Results and Discussion

This research discussed different issues related to blockchain security and vulnerabilities. The primary attacks that have recently affected the blockchain systems are growing. The negative influence of hackers and human factors may lead to more risks. When security is low, not all operations that strengthen the fundamentals are reliable. Blockchain technology is a method of connecting many parts and providing a road to future success. Organizations should employ blockchain technology to make profits by varying advanced resources and sustaining the overall market.

V. Conclusion

There is no doubt that blockchain technology has recently emerged as a hot issue. Although it is crucial to remain aware of specific problems, some have already been solved thanks to the development of new approaches that are becoming increasingly advanced and reliable. The concept of using blockchain technologies to overcome fundamental problems, such as trustworthiness and non-repudiation, has sparked the interest of scholars working in a wide range of disciplines.
The value of blockchain systems is overgrowing because of the decentralized and peer-to-peer characteristics it possesses. A wide variety of modern perspectives were utilized during this research study to investigate the plethora of issues, including obstacles related to the blockchain technique's privacy protection, as well as the weaknesses and dangers that prevent its more widespread application.

References

[1] M. Wazid and P. Gope, "Backm-eha: A novel blockchain-enabled security solution for iomt-based e-healthcare applications," *ACM Transactions on Internet Technology (TOIT)*, 2022.

[2] J. H. Mosakheil, "Security threats classification in blockchains," 2018.

[3] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," *Internet of Things*, vol. 8, p. 100107, 2019.

[4] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 341–390, 2020.

[5] M. Liu, K. Wu, and J. J. Xu, "How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain," *Current Issues in auditing*, vol. 13, no. 2, pp. A19–A29, 2019.

[6] Q. Wang, L. He, X. Zhu, Y. Huang, and Z. Li, "Privacy protection of blockchain security development status," in *2021 4th International Conference on Information Systems and Computer Aided Education*, 2021, pp. 2592–2596.

[7] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[8] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[9] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[10] O. Oksiiuk and I. Dmyrieva, "Security and privacy issues of blockchain technology," in *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. IEEE, 2020, pp. 1–5.

[11] M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain," in *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, 2018, pp. 47–55.

[12] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2018.

[13] V. Suma, "Security and privacy mechanism using blockchain," *Journal of Ubiquitous Computing and Communication Technologies (UCCT)*, vol. 1, no. 01, pp. 45–54, 2019.

[14] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2019.

[15] Y. Huang, Y. Yu, H. Li, Y. Li, and A. Tian, "Blockchain-based continuous data integrity checking protocol with zero-knowledge privacy protection," *Digital Communications and Networks*, 2022.

[16] H. Zheng, J. Shao, and G. Wei, "Attribute-based encryption with outsourced decryption in blockchain," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1643–1655, 2020.

[17] D. Daniel and C. Ifejika Speranza, "The role of blockchain in documenting land users' rights: The canonical case of farmers in the vernacular land market," *Frontiers in blockchain*, vol. 3, p. 19, 2020.

[18] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based iot ecosystem using attribute-based encryption," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2017, pp. 1–6.

[19] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[20] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, "An overview of blockchain security analysis," in *China Cyber Security Annual Conference*. Springer, Singapore, 2018, pp. 55–72.

[21] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.

[22] L.-H. Zhu, B.-K. Zheng, M. Shen, F. Gao, H.-Y. Li, and K.-X. Shi, "Data security and privacy in bitcoin system: a survey," *Journal of Computer Science and Technology*, vol. 35, no. 4, pp. 843–862, 2020.

[23] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67 189–67 205, 2018.

[24] M. K. Shrivas, T. Y. Dean, and S. S. Brunda, "The disruptive blockchain security threats and threat categorization," in *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*. IEEE, 2020, pp. 327–338.

[25] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani, *Blockchain for cybersecurity and privacy: architectures, challenges, and applications*. CRC Press, 2020.

[26] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE access*, vol. 8, pp. 21 091–21 116, 2020.

[27] S.-G. Liu, W.-Q. Chen, and J.-L. Liu, "An efficient double parameter elliptic curve digital signature algorithm for blockchain," *IEEE Access*, vol. 9, pp. 77 058–77 066, 2021.

[28] R. Singh, A. D. Dwivedi, G. Srivastava, A. Wiszniewska-Matyszkiel, and X. Cheng, "A game theoretic analysis of resource mining in blockchain," *Cluster Computing*, vol. 23, no. 3, pp. 2035–2046, 2020.

[29] S. Pastrana and G. Suarez-Tangil, "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 73–86.

[30] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, p. 101654, 2020.

[31] A. Haque and M. Rahman, "Blockchain technology: Methodology, application and security issues," *arXiv preprint arXiv:2012.13366*, 2020.

[32] A. Soundararajan, "Blockchain and new age security attacks you should know," *Accessed: Jul*, vol. 29, p. 2018, 10.

[33] N. Rathod and D. Motwani, "Security threats on blockchain and its countermeasures," *Int. Res. J. Eng. Technol*, vol. 5, no. 11, pp. 1636–1642, 2018.

[34] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, 2014.

[35] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting iot security and privacy through blockchain," *Cluster Computing*, vol. 24, no. 1, pp. 37–55, 2021.

[36] K. M. Khan, J. Arshad, and M. M. Khan, "Simulation of transaction malleability attack for blockchain-based e-voting," *Computers & Electrical Engineering*, vol. 83, p. 106583, 2020.

[37] J. McKendrick, "Reasons to be cautious with blockchain," 9.

[38] D. Gozman, J. Liebenau, and T. Aste, "A case study of using blockchain technology in regulatory technology," *MIS Quarterly Executive*, vol. 19, no. 1, pp. 19–37, 2020.

[39] Y. Wang, J. He, N. Zhu, Y. Yi, Q. Zhang, H. Song, and R. Xue, "Security enhancement technologies for smart contracts in the blockchain: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, p. e4341, 2021.

[40] P. Hacker and C. Thomale, "Crypto-securities regulation: Icos, token sales and cryptocurrencies under eu financial law," *European Company and Financial Law Review*, vol. 15, no. 4, pp. 645–696, 2018.

[41] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*. NIST Gaithersburg, MD, USA, 2016, pp. 1–10.

[42] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *2017 international conference on electrical and computing technologies and applications (ICECTA)*. IEEE, 2017, pp. 1–4.

[43] A. Turner and A. S. M. Irwin, "Bitcoin transactions: a digital discovery of illicit activity on the blockchain," *Journal of Financial Crime*, 2018.