A Review on Blockchain Security Issues and Challenges

Conference Paper · August 2021

DOI: 10.1109/ICSGRC53186.2021.9515276

6 authors, including:

Md Rafiqul Islam
International Islamic University Malaysia
1 PUBLICATION **8** CITATIONS
SEE PROFILE

Md Mahmud
Sunway University
12 PUBLICATIONS **142** CITATIONS
SEE PROFILE

Muslim Har Sani Mohamad
International Islamic University Malaysia
31 PUBLICATIONS **358** CITATIONS
SEE PROFILE

Abd Halim Embong
Auckland University of Technology
17 PUBLICATIONS **64** CITATIONS
SEE PROFILE

A Review on Blockchain Security Issues and Challenges

Md Rafiqul Islam
Mechatronics Engineering
International Islamic University Malaysia
Kuala Lumpur, Malaysia
engrrafiqul@gmail.com

Muhammad Mahbubur Rahman
Mechatronics Engineering
International Islamic University Malaysia
Kuala Lumpur, Malaysia
mahbub@iium.edu.my

Md Mahmud
Research Center of Nano-Materials and Energy Technology
Sunway University
Kuala Lumpur, Malaysia
mahmud.md@ieee.org

Mohammed Ataur Rahman
Mechanical Engineering
International Islamic University Malaysia
Kuala Lumpur, Malaysia
arat@iium.edu.my

Muslim Har Sani Mohamad
Accounting
International Islamic University Malaysia
Kuala Lumpur, Malaysia
muslimh@iium.edu.my

Abd Halim Embong
Mechatronics Engineering
International Islamic University Malaysia
Kuala Lumpur, Malaysia
ehalim@iium.edu.my

2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC) | 978-1-6654-4011-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICSGRC53186.2021.9515276

***Abstract*—Blockchain is one of the emerging technology in recent years in the field of information technology. Blockchain is a decentralized, traceable, temper proof, and trustworthy distributed database system operated by multiple nodes. Blockchain is used not only in cryptocurrency or electronic cash, but also in other applications such as financial transactions, healthcare, insurance, IoT, manufacturing, education, etc., with the promise of more skills and higher resilience. Over the past few years, a significant number of public announcements and news have been made about its goals, partnerships, development, and implementation. However, the most important aspects and discussions on issues related to blockchain security, challenges and policies have been raised around the world. Focus on blockchain security issues and this review paper reviewed 80 research papers. Notable works in this review article are on the concept of blockchain ecosystems, the division of blockchains, the implementation of blockchains and finally security issues and blockchain challenges. This review paper will be helpful for the new research work and safety related issues for blockchain.**

Keywords— blockchain, security, encryption, soft fork, cryptocurrency, bitcoin.

I. INTRODUCTION

Blockchain technology has it is potential scope to transform the way of business, communicate with their customers, other businesses, and regulators. A person or group of people in 2019, was using the pseudonym Satoshi Nakamoto published a paper and introduced a new cryptocurrency is called "bitcoin" and suggested a peer-to-peer network (P-to-P) solution for online fund transfer from one party to another without any third or trusted party [1]. It is an ecosystem that growing faster to changes the technological concept across the globe. Blockchain is a type of distributed ledger technology that is a distributed and immutable ledger to transfer ownership, keeping transactions records, tracing assets, ensure transparency, trust, and security for various types of transactions [2]. Though most people believe one of its benefits is the inherent resiliency of cybersecurity, still it is not a fully secured and cyber-attack-free technological platform.

Today entrepreneurs, investors, and policymakers become more focused on this latest new edge technology due to its future possibilities to use for other customers, other businesses, and regulators [3]. So, it will carry the security threats which include serious impact due to intentional or unintentional activities of participants of the blockchain network, where social engineering techniques will be used to gain confidential credentials [4]. Just a Compromise with security, all valuable assets on blockchain could have a severe impact that point-out the violation of laws and regulations of the country [5].

Blockchain technology is one the biggest innovation of the 21st century that has provided a wave from the financial industry to manufacturing, and education as well [6]. Blockchain is capable to bring substantial positive changes in the financial sectors, IoT, supply chain, voting, medical treatment, insurance, education, and other industries as well [7]. It has some distinct capabilities to minimize the cyber-security risks and the security features are (I) Blockchain increase the resiliency of the network from being a compromise of single-point failure (II) Blockchain uses the consensus mechanism which provides transparency and integrity of the ledger (III) Very difficult for the hackers or attackers to inject or deploy the malicious software or malware [8]. On the other hand, some of the majors blockchain security challenges like endpoint, scalability, regulatory, third party vendor, and insufficient testing cannot ignore [9]. A 51% attack is another type of attack on blockchain where attackers or groups of people can take the control of blockchain network [10]. In this article, we will highlight the security issues and challenges of blockchain technology.

II. CATEGORY OF BLOCKCHAIN

According to the nature of business and user requirements, the blockchain can be divided into the public blockchain, private blockchain, and consortium blockchain [11].

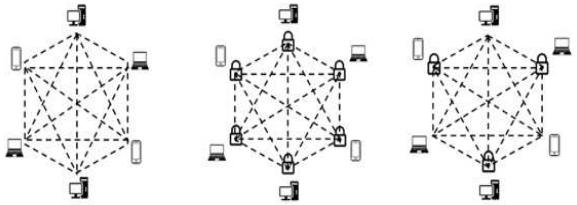

Fig 1. Public blockchain, Fig 2. Private blockchain, Fig 3. Consortium blockchain

A. Public Blockchain

Blockchain protocols based on Proof of Work (PoW) consensus algorithms are open source where anyone can participate without permission [12]. Anyone can download the code and install their local device through which they can validate the transaction in the network. Anyone can send the transactions through the network and monitor them in the blockchain as well as can read and write transactions on the public network [13]. For example, Bitcoin, Ethereum, XRP, Dash, Litecoin, Dogecoin, etc. figure 1 shows the public blockchain.

B. Private Blockchain

Permissioned private blockchain may be distributed in the restricted to an arbitrary extent but the write permissions are strictly controlled by one organization [12]. The advantage of the private blockchain is established by groups and participants who can verify the transactions internally. It has the risk of security breaches like a centralized system whereas public blockchain is secured by a game theory incentive mechanism. However, private blockchain will be more advantageous than others when it will come to the state data privacy act and other regulatory issues. Figure 2 shows private blockchain.

C. Consortium Blockchain

Private Consortium Blockchain is controlled by an organization or the leadership of a group and they do not allow all internet users to participate in the process of verifying the transactions [12]. The administrator of a consortium chain defines user access rights. A consortium blockchain is faster, highly scalable, and provides more transaction privacy other than public blockchain. For example, Ripple is one of the largest cryptocurrencies to support the permission-based blockchain network [14]. Figure 3 shows consortium blockchain.

III. Application of Blockchain

Blockchain applications are not only limited to cryptocurrency, but it has also many other applications in different sectors which may save the business time and cost as well [15]. Such applications software can be grouped in different sectors like the financial sector, healthcare, etc.

A. Cryptocurrency

Blockchain technology is widely used in the financial sector which is called cryptocurrency and these currencies are introduced by application software [16]. Bitcoin is the original decentralized cryptocurrency that was introduced by Satoshi Nakamoto in 2009 and the data structure and transaction system were built by blockchain technology, and it has no physical currency [17]. Cryptocurrency uses a highly secured technique called encrypted technology for making direct transactions between buyer and seller without third-party intervention [18]. The sender digitally signs the message or input with his/her private key before sending bitcoin and sends the same to the receiver's public key through broadcasting to the network where the verifications are completed by other users [19]. A few numbers of cryptocurrency systems are as follows table 1.

TABLE I. Cryptocurrency Systems

Cryptocurrency	Hash Algorithm	Year	Mining Method
Bitcoin [20]	SHA-256		Proof of Work
Litecoin [21]	Scrypt Proof-of-Work Algorithm	2011	Proof of Work
Monero (XMR) [22]	Ring signatures.	2014	Proof of Work
Ethereum [23]	Ethash	2015	Proof of Work
Ripple [24]	SHA 512	2012	Consensus
Primecoin [25]	Cunningham chain	2013	Proof of Work
Peercoin [26]	SHA-256	2012	Proof of Work
Blackcoin [27]	Scrypt	2014	Proof of Work

B. Smart Contract

Smart contracts execute is automatic executing contracts based on the agreement between buyer and seller which is written into the lines of code, and the codes and agreements exist into the decentralized blockchain network [28]. Most of the benefits of smart contracts are visualized in business collaborations where the agreements are build-in, and all the participants knew the outcomes without third-party involvements [29]. Smart contracts work like a person where the codes are executed automatically and can hold the assets temporarily [30]. Ethereum is an open source blockchain platform where smart contracts exist and offering a decentralized virtual machine to operate the contract through using a digital currency called ETH [7].

C. Hyperledger

Hyperledger is an open-source platform, a collaborative effort including leaders in finance, banking, supply chain, IoT, manufacturing, and technology, and hosted by Linux Foundation [31]. Hyperledger does not have any cryptocurrency, and the access into the network is applicable for the authorized members where the transaction mechanism is controlled by chaincode (smart contract) [32]. The transaction request is submitted into the Hyperledger Fabric by the user for ordering and validation, where the request initializes a chaincode in a specific channel. The components of the Hyperledger Fabric are ordering nodes, peer nodes, and client applications [33]. Through an isolation channel, the privacy of the transaction mechanism in the network is ensured between the participants.

D. Other Applications

Blockchain is not only applicable to cryptocurrency mining and smart contract, but also for other sectors like healthcare, education, voting, supply chain management, IoT, insurance, international payment, trade finance, etc. [34].

IV. Security Issues and Challenges of Blockchain

A. 51% Attacks

The 51% attack into blockchain network is a technique that intends to fork a blockchain for double spending [35]. The main security challenge of blockchain is 51% attacks, which is comparatively hypothetical, where the attackers can roll back the transactions in the alternative block in a side chain or branch and can hide the information that is happening in the main chain of the blockchain [36]. The probability of mining blocks by the miners depends on the proof of work. To mining more blocks, miners together and use more computer power to hold the network control. If

anyone or group can hold more than 51% computational power, the person or group can find out the nonce which will help miner/miners to decide which block belongs to permissible and which are not [7]. It will help the attacker to modify the transactions that may cause the double-spending attack, which also helps to hold the blocks from verifying the transactions [37]. However, it is not always required to gain 51% hashing power to compromise the blockchain network, the double-spending attack is also possible with less than half of the hashing power, but the probability of success for the same is very less [38].

B. *Forking issue*

Forking is another blockchain problem. Forking indirect divergence in the blockchain can be temporary or permanent, and it can happen when a blockchain splits into two parts [39]. Forking is different for each type of blockchain which depends on its architecture and use case [40]. There are two types of forking:

i. *Hard Fork*

The hard fork is the permanent changes of the protocols into a blockchain network, splits a single cryptocurrency into two which validates blocks and transactions that were previously invalid or vice-versa [41]. Network nodes are using the older version, which is not accepted by the new version, the transaction into the new chain is invalid into the older chain. Miners need to upgrade their old version with the latest version for doing transactions into the fork chain. For the adoption and incorporation of version changes, the miner nodes are required to vote in the blockchain network [42]. Bitcoin cash is one of the examples of a hard fork in August 2017, and the Bitcoin cash wallets rejected the transactions for Bitcoin and blocks [43]. Figure 4 shows the hard fork issue.

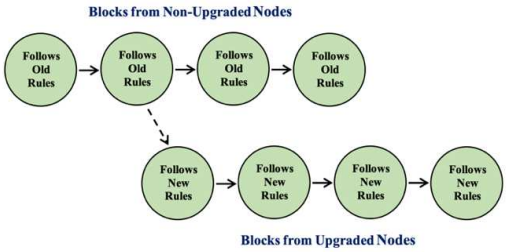

Fig. 4. Hard Fork

ii. *Soft Fork*

Soft fork in blockchain means the change of software protocol where the previously valid transaction blocks are invalid, and the older nodes recognize the new transaction blocks as valid which means soft fork is backward compatible [44]. In a soft fork, most of the miners need to upgrade the software version for enforcing the new rules [45]. The computing power required for the new nodes is much higher than old nodes, the blocks that mines by the old nodes will not be validated by the new nodes, but both the new and old nodes will work into the same network [7].

C. *Eclipse Attacks*

In the eclipse attack, the attacker attacks on a decentralized network to isolate a specific user or users, rather than an attack on the whole network [66]. This type of attack is possible because a decentralized blockchain network does not allow all the computers to be simultaneously connected to all other computers of the network. A Bitcoin node can only hold 8 outgoing and 117 incoming connections [46]. Due to the limited outgoing connections, the attackers may establish the connections through injecting malicious codes. For Ethereum, there are two types of eclipse attacks that can be occurred. First, the attackers can establish Maxpeers incoming PCP connections to its malicious nodes before clients establish outgoing TCP connections, and the second eclipse is to be owing to the table [45]. Through rebooting, there is a high probability of the victim to occupies all outgoing nodes to its adversarial nodes [46].

D. *Application Bugs*

Any software-based solution is developed by a human being. The act of a human being is not error-proof. So, human coding errors create the conduits for threats of blockchain applications. Most of the blockchain applications belong to an open platform and anyone can join these networks. For example, one of the biggest MtGox attacks occurred in 2014 with a declared loss was $600 million, the other one Bitfinex occurred in 2016 with the cost of $65 million [47]. In 2016 hackers exploited the coding errors in the program of a virtual company named Distributed Autonomous Organization (DAO) and theft Ether digital currency fund worth $55 million [48].

E. *Short Address*

A short address attack is the weakness of the Ethereum Virtual Machine (EVM), and it is an input validation bug that occurs from the sender's end due to weak transaction generation code [49]. Short Address Attack occurs when the contract receives less data than expected, and the EVM includes zeros at the end of the address to ensure the 256-bit data types [50. The attacking strategy of a short address is like SQL injection bug [51].

F. *Timestamp Dependence*

Timestamp Dependence vulnerability can be exploited by the bad miners, and due to personal benefit, miners can re-arrange the timestamp within few seconds [52]. In a blockchain system, the miner has the choice to set the timestamp into the block by few seconds [53]. It is capable to detach the Ethereum network from the global clock. Smart contract generates random numbers to determine the lottery result which helps the miners to put a timestamp within 30 seconds of block validation, and it provides the opportunity for miners for exploration.

G. *Scalability Issue*

Blockchain is a distributed ledger system. The popularity of this new edge technology has increased tremendously along with other IT-enabled services in different sectors like IoT, education, agriculture, healthcare, insurance, banking, and finance, etc. The processing power or speed of blockchain is completely dependent on computing powers. For comparison purposes, Bitcoin processes 4.6 transactions per second whereas VISA processes 1,700 transactions per second on average [54]. The blockchain-based transaction is very slow which is the major concern for enterprises, and it depends on the high performance inherit transaction

processing system [55]. The lack of standard and i] nteroperability in a different blockchain platform is another challenge for adaptability [56]. As per Deloitte, five things need to overcome for the widespread adoption of blockchain systems which are ((i) transaction speed, (ii) standard and interoperability, (iii) enhance technical feasibility (iv) supportive regulation, and (v) expansion of consortia [57].

Although, a significant number of scaling methods have been proposed for adoption the of blockchain technology, each of them comes with its limitations. One of the most notable issues is the sharing of the database. For blockchain development, database sharing is processed to enhance the computational and storage workload into the storage system across the Peer-to-Peer (P2P) network, so that every node can process transactions only its corresponding sharing database [58]. The major challenges of sharing the database in the blockchain are related to security and communication among the nodes of the network, which includes the extra complexity for blockchain developers that require an extra level of communication protocol.

However, there are being various solutions have been proposed to solve these issues. Proof of Stake (PoS) is more efficient than Proof of Work (PoW), two nodes in Practical Byzantine Fault Tolerance (PBFT) research a consensus for the event of malicious node being exist, Delegated Proof of Stake (DPoS) consensus that represents the democratic consensus; and Tendermint is another consensus algorithm based on a Byzantine algorithm which very scalable to perform approximately 10,000 transactions per second [59].

H. Regulatory Issue

"Regulation of Cryptocurrency Around the World" was published in 2018 to address this issue [60]. The implementation of blockchain applications across the world must go for a lot of complex regulation in terms of economic and political, and no central bank policy available for the same. For example, some countries banned Bitcoin and not accepted them for payment. Bitcoin is a decentralized blockchain and controlled by a specific person or group, and no central banks have control over it. Until a proper regulatory framework is established, it is not possible to use digital currency to make the payment through banking channel as well. Further research is required before applied cryptocurrency globally.

A total number of 82 countries across the globe have declared the cryptocurrency is legal, but this legalization does not mean that the government of those countries supports the virtual currency any way [61]. And it raises the question about the usability of the blockchain application. Further research is required before applied cryptocurrency globally.

I. Integration Issue

Changing the existing system with a new blockchain application is another big challenge for the organization in terms of cost, infrastructure setup, human mindset, management expectation, etc. There is a major corporate challenge how to integrate the new application with the existing legacy system, where organizations are required to completely restructure their old system in such a way for successful integration of two technologies [62]. Due to a lack of skilled blockchain developers, it is very hard to pool technical experts for the same. On the other hand, the incident of data loss and breach that may discourage the organizations from transitioning to blockchain-based application. A breach of data loss may encourage fraudulent activities which may issue the blockchain security concern and could cause a barrier for new application integration problems [63].

J. Inegration Issue

Changing the existing system with a new blockchain application is another big challenge for the organization in terms of cost, infrastructure setup, human mindset, management expectation, etc. There is a major corporate challenge how to integrate the new application with the existing legacy system, where organizations are required to completely restructure their old system in such a way for successful integration of two technologies [57]. Due to a lack of skilled blockchain developers, it is very hard to pool technical experts for the same. On the other hand, the incident of data loss and breach that may discourage the organizations from transitioning to blockchain-based application. A breach of data loss may encourage fraudulent activities which may issue the blockchain security concern and could cause a barrier for new application integration problems [58].

TABLE II. SUMMARY OF SECURITY ISSUES AND CHALLENGES.

SI	Security issues and challenges	Description
01	51% Attacks	The 51% attack into a blockchain network is a technique that intends to fork a blockchain for double-spending where the attackers can roll back the transactions in the alternative block.
02	Forking issue	Forking is indirect divergence in the blockchain can be temporary or permanent, and it can happen when a blockchain splits into two parts.
03	Eclipse Attacks	In the eclipse attack, the attacker attacks a decentralized network to isolate a specific user or users, rather than an attack on the whole network.
04	Application Bugs	The act of a human being is not error-proof. Human coding errors may create the conduits for threats of blockchain applications.
05	Short Address	A short Address Attack occurs when the contract receives less data than expected, and the EVM includes zeros at the end of the address to ensure the 256-bit data types.
06	Timestamp Dependence	Timestamp Dependence vulnerability can be exploited by the bad miners where miners can re-arrange the timestamp within few seconds.
07	Scalability Issue	The blockchain-based transaction is very slow which is the major concern for enterprises.
08	Regulatory Issue	The implementation of blockchain applications in different sectors is highly challenging due to complex regulation in terms of economic and political, and no central bank policy is available so far.
09	Integration Issue	Changing the existing system with a new blockchain application is another big challenge for the organization in terms of cost, infrastructure setup, human mindset, management expectation, etc.

K. Success and failures of blockchain security

The security of the blockchain heavily depends on cryptography to achieve data security where the block hash is

generated on the present block and the previous block. The success factor of blockchain security depends on the consortium including business cases, robust governance policy, operational issues, data privacy, and other regulatory environments [59]. On the other hand, the default blockchain security is not enough to protect the security threats including payment processors, smart contracts, and the third-party vendors that comparatively maintaining the weak security measures on their apps and websites. As a result, hackers are stealing money from blockchain platforms by exploring the design, implementation, and execution of these networks [60]. The figure 5 below is presenting the statistics of total transactional amount vs hacking amount from 2015 to 2020 [61]-[80].

Fig 5. Cryptocurrency transaction vs hacking statistics (2015 – 2020)

V. Conclusion

There is no doubt that the blockchain is an emerging technology in recent years, especially in the field of information technology due to its decentralized platform and peer-to-peer network. There is a remarkable and momentous scope for blockchain for various organizations which will encourage the development of such a reliable, secure, and immutable system in the feature. Though it has problems need to be addressed, some of the issues have already been improved along with new technological concept on blockchain application getting more stable. Despite being a significant number of advantages, it contains some security concerns which have been highlighted in this article. The regulator needs to address the corresponding regulatory issues for this new edge technology, and at the same organizations should be ready for adoption of the blockchain technology that may reduce the impact on the current system.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, 2019.

[2] A. Collomb and K. Sok, "Blockchain/distributed ledger technology (DLT): What impact on the financial sector?," *Digiworld Economic Journal*, (103), 2016.

[3] E. English, et all., "Advancing blockchain cybersecurity: technical and policy considerations for the financial services industry," *Cybersecurity policy and resilience*, *81, 2018*.

[4] S. S. Smith, "Emerging Technologies and Implications for Financial Cybersecurity," *International Journal of Economics and Financial Issues*, *10*(1), 27, 2020.

[5] Z. Zahoor, et all., "Challenges in privacy and security in banking sector and related countermeasures,'' *International Journal of Computer Applications*, vol. *144*(3), pp. 24-35, 2016.

[6] C. Vijai, et all., "The Blockchain Technology and Modern Ledgers Through Blockchain Accounting," *Adalya Journal*, vol. *8*(12), 2019.

[7] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges,'' *IJ Network Security*, vol. *19*(5), pp. 653-659, 2017.

[8] W. Park, et all., "*International chamber of commerce arbitration," 2020.*

[9] J. Sengupta, et all., "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IioT," *Journal of Network and Computer Applications*, *149*, pp. 102481, 2020.

[10] C. W. Cai, "Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain," *Accounting & Finance*, vol. *58*(4), pp. 965-992, 2018.

[11] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper*, *3*(37), 2014.

[12] S. McLean and S. Deane-Johns, "Demystifying Blockchain and distributed ledger technology–hype or hero," *Computer Law Review International*, vol. *17*(4), pp.97-102, 2016.

[13] R. Yang, et all., "Public and private blockchain in construction business process and information integration," *Automation in Construction*, *118*, pp.103276, 2020.

[14] A. Mirchandani, "The GDPR-blockchain paradox: exempting permissioned Blockchains from the GDPR. *Fordham Intel," Prop. Media & Ent. LJ*, *29*, pp.1201, 2018.

[15] S. Daley, "Blockchain Applications & RealWorld Use Cases Disrupting the Status Quo," 25.

[16] B. A. Tama, et all., "A critical review of blockchain and its current applications," In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, pp. 109-113, 2017.

[17] G. C. Dumitrescu, "Bitcoin–a brief analysis of the advantages and disadvantages," *Global Economic Observer*, vol. *5*(2), pp.63-71, 2017.

[18] A. Khan, "Bitcoin–payment method or fraud prevention tool?" *Computer Fraud & Security*, *2015*(5), pp.16-19, 2015.

[19] A. H. Dyhrberg, et all., "How investible is Bitcoin? Analyzing the liquidity and transaction costs of Bitcoin markets," *Economics Letters*, *171*, pp.140-143, 2018.

[20] R. Caetano, "*Learning Bitcoin*," Packt Publishing Ltd.

[21] M. Haferkorn and J. M. Q Diaz, "Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin," In *International Workshop on Enterprise Applications and Services in the Finance Industry*, Springer, Cham, pp. 106-120, 2014.

[22] P. Bajpai, "The 6 most important cryptocurrencies other than bitcoin," Investopedia, 2017. http://www. investopedia. com/tech/6-most-important-cryptocurrenciesother-bitcoin/,(27.08. 2017).

[23] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum *project yellow paper*, *151*(2014), pp. 1-32, 2014.

[24] P. Haiss and J Schmid-Schmidsfelden, "Bitcoin Compared on Price, Liquidity and Volatility: Crypto "Currencies" or an Asset Class of Their Own?" *European Financial Systems 2018*, 128, 2018.

[25] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," vol. *1*(6), 2013.

[26] M. Campbell-Verduyn, "Bitcoin, crypto-coins, and global anti-money laundering governance," *Crime, Law and Social Change*, vol. *69*(2), pp. 283-305, 2018.

[27] P. Vasin, "Blackcoin's proof-of-stake protocol v2," 2014. URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf, 71.

[28] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," *The Review of Financial Studies*, vol. *32*(5), pp. 1754-1797, 2019.

[29] F. Idelberger, G. et all, "Evaluation of logic-based smart contracts for blockchain systems," In *International symposium on rules and rule markup languages for the semantic web*, Springer, Cham, pp. 167-183, 2016.

[30] A. Kosba, et all., "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839-858, doi: 10.1109/SP.2016.55

[31] V. J. Morkunas, et all., "How blockchain technologies impact your business model," *Business Horizons*, vol. *62*(3), pp. 295-306, 2019.

[32] Q. Nasir, et all., "Performance analysis of hyperledger fabric platforms," *Security and Communication Networks*, *2018*.

[33] C, Cachin, "Architecture of the hyperledger blockchain fabric," In *Workshop on distributed cryptocurrencies and consensus ledgers*, Vol. 310(4), 2016.

[34] A, Meola, "The growing list of applications and use cases of blockchain technology in business & life," *Business Insider, 2017*.

[35] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, vol. *9*(9), pp. 1788, 2019.

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

[37] K. Jonathan and A. K. Sari, "Security Issues and Vulnerabilities On A Blockchain System: A Review," In *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)* , pp. 228-232, 2019.

[38] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009,* 2014.

[39] H. Hasanova, et all., "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. *29*(2), e2060, 2019.

[40] J. V. Andersen, and C. I. Bogusz, "Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking," *Journal of the Association for Information Systems*, vol. *20*(9), 11, 2019.

[41] N. Webb, "A fork in the blockchain: Income tax and the Bitcoin/Bitcoin Cash hard fork," *North Carolina Journal of Law & Technology*, vol. *19*(4), 283, 2018.

[42] N. C. Yiu, "An Overview of Forks and Coordination in Blockchain Development," *arXiv preprint arXiv:2102.10006*, 2021.

[43] J. Herrera-Joancomartí and C. Pérez-Solà, "Privacy in bitcoin transactions: new challenges from blockchain scalability solutions," In *International Conference on Modeling Decisions for Artificial Intelligence*, Springer, Cham, pp. 26-44, 2016.

[44] K. Nayak, et all., "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 305-320, 2016.

[45] E. Heilman, et all., "Eclipse attacks on bitcoin's peer-to-peer network," In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 129-144, 2015.

[46] G. Xu, et all., "Am I eclipsed? A smart detector of eclipse attacks for Ethereum," *Computers & Security*, *88*, 101604, 2020.

[47] A. Kiayias and G. Panagiotakos, "On trees, chains and fast transactions in the blockchain," In *International Conference on Cryptology and Information Security in Latin America*, Springer, Cham, pp. 327-351, 2017.

[48] S. Porru, et all, "Blockchain-oriented software engineering: challenges and new directions," In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, pp. 169-171, 2017.

[49] D. Siegel, "Understanding the DAO Attack," Coindesk, 2016. https://www. coindesk. com/understanding-dao-hack-journalists/, updated on, 3(28), 2018.

[50] S. Sayeed, et all., "Smart contract: Attacks and protections," *IEEE Access*, vol. *8*, pp. 24416-24427, 2020.

[51] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pp. 2-8, 2018.

[52] H. Chen, et all., "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys (CSUR)*, vol. *53*(3), pp. 1-43, 2020.

[53] S. Eskandari, et all., "Sok: Transparent dishonesty: front-running attacks on blockchain," In *International Conference on Financial Cryptography and Data Security*, Springer, Cham, pp. 170-189, 2019.

[54] B. Jiang, et all., "Contractfuzzer: Fuzzing smart contracts for vulnerability detection," In *2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pp. 259-269, 2018.

[55] K. Li, "The blockchain scalability problem & the race for visa-like transaction speed," Retrieved *November 29*, 2019.

[56] R. A. N. D. Europe, "The Potential Role of Standards in Supporting the Growth of Distributed Ledger Technologies/Blockchain," 2019.

[57] D. Schatsky, et all, "Blockchain and the five vectors of progress," *Recuperado de*, 2018. https://www2. deloitte. com/us/en/insights/focus/signals-for-strategists/value-of-blockchain-applications-interoperability. html.

[58] L. P. Cox and B. D. Noble, "Samsara: Honor among thieves in peer-to-peer storage," *ACM SIGOPS Operating Systems Review*, vol. *37*(5), pp. 120-132, 2003.

[59] A. A. Monrat, et all., "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE *Access*, vol. *7*, pp. 117134-117151, 2019.

[60] L. C. Schaupp and M. Festa, "Cryptocurrency adoption and the road to regulation," *In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pp. 1-9, 2018.

[61] U. W. Chohan, "Assessing the differences in bitcoin & other cryptocurrency legality across national jurisdictions," *Available at SSRN 3042248*, 2017.

[62] C. R. Meijer, "Remaining challenges of blockchain adoption and possible solutions," 2020.

[63] H. F. Atlam, et all., "Blockchain with internet of things: Benefits, challenges, and future directions," International *Journal of Intelligent Systems and Applications*, vol. *10*(6), pp. 40-48, 2018.

[64] Ajay Kumar, Kumar Abhishek, Pranav Nerurkar, Muhammad Rukunuddin Ghalib, Achyut Shankar. Empirical Analysis of Bitcoin network (2016-2020). 2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)

[65] blockchain.com. (n.d). Retrieved from https://www.blockchain.com/charts/estimated-transaction-volumeusd.

[66] Reader, R. (2015). Bitstamp resumes Bitcoin trading after $5 M in losses led to shutdown. Venture Beat, 9(1).

[67] Higgins, S. (2015). BTER claims $1.75 million in bitcoin stolen in cold wallet hack. Coindesk, February.

[68] Zamani, E. et all. (2020). On the security risks of the blockchain. Journal of Computer Information Systems, 60(6), 495-506

[69] Dotson, K. (2015). Bitfinex Bitcoin exchange hot wallet hacked, estimated 1474 BTC stolen. Available: https://www.hackread.com/bitcoin-exchange-bitfinex-hot- wallet-hacked/.

[70] Suberg, W. (2016). Steemit Hacked for '$85,000' as Users Complain of Weak Security. Bitcoin.com.

[71] Higgins, S. (2016). Gatecoin claims $2 million in Bitcoins and ethers lost in security breach

[72] Falkon, S. (2017). The story of the DAO—its history and consequences. Medium

[73] Gikay, A. A. (2018). Regulating decentralized cryptocurrencies under payment services law: Lessons from European Union Law. Case W. Res. JL Tech. & Internet, 9, 1.

[74] Lazarenko, A., & Avdoshin, S. (2018). Financial risks of the blockchain industry: A survey of cyberattacks. In Proceedings of the Future Technologies Conference, pp. 368-384. Springer, Cham.

[75] Suberg, W. (2017). Zerocoin Hacker "Creates" and Spends 370,000 Tokens Worth 410 BTC. Coin Telegraph

[76] De, N. (2018). Bee token ico stung by $1 million phishing scam. Coin Desk, 1(2).

[77] Abdel-Qader, A. (2018). Indian Bitcoin Exchange Coinsecure Claims $3.5 Million Lost in Insider Hack. Finance magnates.

[78] Haentjens, M. et all. (2020). The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them. Leiden Law School Research Paper, Hazelhoff Research Paper Series, (9).

[79] Wilmoth, J. (2018). Breaking: South Korean Crypto Exchange Bithumb Hacked, Thieves Steal $30 Million.

[80] Selfkey. (2020). A Comprehensive List of Cryptocurrency Exchange Hacks. https://selfkey.org/list-of-cryptocurrency-exchange-hacks/.