International Journal of Advanced Science and Technology
Vol. 29, No. 8, (2020), pp. 5371 - 5376

`

# Security Issues By Allied Attacks In Blockchain Technology

[1] Mohamed Jamaldeen Ahamed Sabani, [2] Shafana Muhammed Shareef, [3] Razik Kariapper Ahmadh Rifai Kariapper

[1, 2, 3] *Department of Information and Communication Technology, South Eastern University of Sri Lanka* [1] mjasabani@seu.ac.lk , [2] zainashareef@seu.ac.lk , [3] rk@seu.ac.lk

***Abstract***

*Blockchain technology is for distributing reports of all transaction or digital events, and it is the most trending topic nowadays. Blockchain technology is integrated with some other technologies like cryptography, mathematics, peer to peer networks uses distributed consensus algorithm and economic model etc. Blocks are coupled together to assemble as a linked list. Generally, the blocks of blockchain incorporate main data, a hash of previous and current blocks, timestamp, Nonce and Merkle tree root. It offers great advantages to the application of Information Technology. Blockchain provides more reliable and desirable services. It involves public and social services in more different ways such as financial, healthcare, automobile, risk management, Internet of Things (IoT). However, before using this technology, better to get knowledge and be aware of security and privacy level of the related applications with blockchain. This study focuses on great features of blockchain, common types of security attacks, and existing solutions to overcome the shortcomings of the security problems on the blockchain. According to the study, there are six critical elements assembled to create blockchain technology such as decentralized, transparent, open-source, autonomy, immutable and anonymity. Blockchain technology guarantees some properties such as integrity, availability, privacy, authentication and non-repudiation. But there is a possibility for security and privacy attacks such Double-spending attack, Majority attack, denial of service attack, Eclipse attack, Selfish mining attack, Reentrancy Attack, and Liveness attack and some unidentified attacks. In this technology, it offers and complies important security aspects needed for the secure transaction and handling. There is room to invent appropriate more security features to overcome these risk and attacks even though blockchain integrated with existing security technologies.*

***Keywords:*** *- Blockchain, Security, Privacy, Attacks on the Blockchain*

## 1. Introduction

Blockchain is a database that distributes reports of all transactions or digital events. The majority of computer participants verifies each transaction. It contains every record of each transaction. Blocks are coupled together to assemble as a linked list [1]. Blockchain technology first emerged in 2008 when a person or group called "Satoshi Nakamoto" published a white paper entitled "Bitcoin: A Peer to Peer Electronic Cash System". Blockchain transaction records are incorruptible because of which distributed over the network.

Bitcoin and digital currency are the first applications of blockchain technologies. As we are using money in the real world, bitcoin is used for trade things over the internet. The primary objective of Bitcoin is to function as a decentralized digital currency which is independent of trusted third parties. As the bitcoin technique proves the success, many fields are emerged with blockchain technologies nowadays, such as the Internet of Things, medical treatment and storage, financial marketing, supply chain and voting [2].

The blockchain technology is an emerging research field along with some other security problems of the distributed system, such as secure timestamping, distributed namespaces, and so on. Blockchain technology is integrated with some other technologies like cryptography, mathematics, peer to peer networks uses distributed consensus algorithm and economic model etc.

Generally, the blocks of blockchain incorporate main data, a hash of previous and current blocks, timestamp, Nonce and Merkle tree root. Next block of the blockchain is proposed by solving a cryptographic puzzle by the miners. This procedure is called Proof of work (PoW). Thus, it has a



ISSN: 2005-4238 IJAST

`

cryptographic property; blockchain is said to be immutable. It means that changing the data is extremely hard and changes easily detectable. A Merkle binary tree with hash pointers is a structure for efficient and secure verification of content in a lengthy body of data. And the first block is called as the genesis block.

There are six (06) key properties assembled to create blockchain technology such as decentralized, transparent, open-source, autonomy, immutable and anonymity [2]. Blockchain does not rely on any centralized control. Data can be updated and distributed. It can be trusted due to the data records, and updates are open to each node. These technologies are available publicly for people. They can use them to create the application they want. Data transfers and updates are safety on every node of blockchain-based on consensus. No interventions are there. Records retain forever, and can't be altered unless someone at the same time controls more than 51% nodes. Data transfers or transactions are being anonymous.

Nowadays, many areas are using blockchain technology such as financial application, supply chain traceability, identity certification, insurance, International payments, the Internet of Things and the protection of privacy etc. [3 - 8]

According to the literature, blockchain technologies guarantee for integrity, availability, privacy, authentication and non-repudiation. The cryptographic mechanism is used to avoid unauthorized changes on blockchain data. Therefore, it verifies integrity by guaranteeing the primary features of immutability. The service blockchain is ever available for the requests of legitimate users. It maintains blocks as decentralized with various copies on the nodes of blockchain. That is how it ensures the availability of data. Blockchain hides user identities by using a pseudo-anonymization mechanism. This way, it allows the authorized person to access the information. Blockchain technologies allow authorized users to process the transaction by providing a function with private keys. The communicators in blockchain cannot deny receiving or sending a message. Therefore, there is no chance for repudiation on sending and receiving messages [9].

Blockchain is being used in many fields effectively. However, before starting to use the applications which are merged with this technology, we need to be aware of challenges deeply related to security and privacy on the blockchain. Most security attacks aim to control the generation of blocks on the chain by dishonest nodes. There are few types of significant attacks in blockchain as a double-spending attack, 51% majority attack, Eclipse, Selfish mining, Distributed Denial of Service attack, and Balance attack [10 – 18].

## 2. Methodology

Sources for this review were identified using multiple databases. Initially, to establish a list of peer-reviewed articles, searches were done in Google scholar by using broad terms. In the beginning, we used a basic search of "issues in blockchain". From the research article's titles derived by the initial seek, we were able to use an extended list of refined terms when accessing other databases. Through the repositories and digital libraries of Universities, we applied a narrow search to find the conference papers related to our topic. The search terms were hand-picked for this literature survey comprised of "security issues, blockchain loopholes, disadvantages of blockchain, dissatisfaction in blockchain, attacks on blockchain, privacy issues etc. These terms were cumulated in diverse ways with "AND" command to retrieve the narrowly filtered relevant articles.

Most of these searched terms were produced from the results of the initial search and combined with results found from the various academic repositories. Each of the terms utilized because of their appropriateness and relevance with the motive of this study. Selected sources were analyzed based on the number of criteria. First, the chosen source had to be in lined with the objectives of this study. We searched deeply about the consequences of all the security issues in blockchain and identified the allied attacks with each.

## 3. Discussion

Even though, blockchain providing some security features, also there are vulnerabilities and creates risks [19 – 21]. The blockchain establishes mutual trust by a distributed consensus mechanism. In Proof of Work (PoW) based blockchains, If any miner gets a hash power more significant than 50% of the



ISSN: 2005-4238 IJAST

`

total hash power of blockchain, then that miner can arbitrarily manipulate the data from the blockchain [20]. In Proof of Stake (PoS) based blockchains also, there is a possibility for this attack if a single miner owned the number of coins more than 50% of the entire blockchain. It can be considered as Majority attack and leads to some other issues such as reverse the transaction, double spending, modifying the transaction order, hampering the mining operation, impede the transaction confirmation, and denial of service attack [21]. This is a common risk causes in blockchain 1.0 and 2.0

The majority attack can be defended by applying Two-phase Proof of Work (Eyal & Sirer, 2014), Random mining group selection technique [23], and Proof of activity protocol [24]. Likewise, with the purpose of mining blocks before the authorized miners, attackers trying to delay the message passing between the miners by identifying a group of miners who have similar mining power [25]. It is known as Balance Attack in PoW based blockchain. In this attack, the attacker with low-mining-power disrupts the communications between subgroups which have similar mining power. In this case, attacker introduces a delay in between those correct subgroups with equivalent mining power. And the transactions may be issued in one subgroup called "transaction subgroup", and the attacker may mine blocks in another subgroup called ‘‘block subgroup’’, and the attacker can overwrite or delete the blocks containing the transaction even though the transactions are already committed. The balance attack also allows double-spending.

Another challenging attack in the blockchain is a double-spending attack which refers that using the same cryptocurrency multiple times for transactions. The seller of the transaction verifies the validity given by the customer with the peer. If the peer is malicious, a conflict transaction will be created by generating a double-spend using the same cryptocurrency. And it validated by another client before the transaction is spread. Therefore, both these transactions are proposed for mining. In this case, if the seller processes the transaction before the validation by a miner, there will be a result of double-spending, and it will allow for rob [20] [26]. It may produce a smart contract risk of dependency on contracts order. The order of execution of two successive transactions may affect the final state because the implementation of the smart contract is associated with a single state [20]. In addition to that, triggering smart contracts is dependent on timestamp. It is the content of each block in the blockchain. It can be defined according to the miner's local system. Therefore, smart contracts are vulnerable if they can be changed by attackers [20]. This type of attacks can be defeated by some techniques such PoW scheme and a distributed timestamping service [27], waiting for more confirmations exponentially [26], Listening period, inserting Observers and forwarding Double-spending Attempts [28], and Fair deposits [29] mechanism.

Eclipse attack [10] is performed to isolate the victim’s communications with other peers in the blockchain network by monopolizing other victim’s connections. This may cost for an unnecessary computing power for the victim. Furthermore, the attacker can use the computing power of the victim to conduct malicious acts. There are two types of eclipse attacks, namely botnet attack and infrastructure attack on a peer-to-peer network of Bitcoin. Bots of divers IP address range launches the botnet attacks and the infrastructure attack models the threat from an ISP. Eclipse attack may lead to some other attacks such engineering block races which wasting mining mower on orphan blocks, splitting mining power which may trigger 51% vulnerability, selfish mining attack which leads the attacker to be rewarded more than the regular mining, and double-spending attacks. This attack can be solved by Deterministic random eviction, Random selection, Test before evict, Feeler connections, Anchor connections, more buckets, more outgoing connections, Ban unsolicited ADDR messages, Diversify incoming connections and Anomaly detection [10].

Moreover these, there also chances of attacks and vulnerabilities such as the denial of service attack [30], selfish mining attack [11] [31], Reentrancy Attack [32] and liveness attack [33].

Selfish mining attack is an attack cause to obtain an undue reward or wasting the computing power of honest miners [31]. The selfish miners discover and hold blocks privately and then fork a private chain. Afterwards, attackers would mine on the private chain they found, and try to discover more new blocks to keep a more extended private branch than the public branch. In the meanwhile, honest miners proceed with the open chain. The private chain would be published by attackers when the public chain reaches the length of the private chain. Such that the honest miners proceeded with the public chain end up without no reward and just wasted computing power, this attack threatens the property of decentralization of blockchain [11]. Selfish mining attack can be defeated by Freshness Preferred



ISSN: 2005-4238 IJAST

`

mechanism [34], Decentralized backwards-compatible defence mechanism [35], and ZeroBlock scheme [31].

Ethereum [36] is another open sourced and decentralized cryptocurrency platform which uses 'Ether' as the cryptocurrency for blockchain transaction. An attack in Ethereum blockchain is DAO attack; the attacker uses the reentrancy vulnerability for this. Initially, the attacker releases a malicious smart contract which with a 'withdraw ()' function call to DAO. The 'withdraw ()' function sends Ether in the form of a call to invoke the callback of malicious smart contract function again. In this way, the attacker tries to rob all the Ether from DAO. The smart contract vulnerability is leading to some other vulnerabilities and being as a gateway for some other attacks such Out-of-gas send Exception disorder leads to King-of-the-ether-throne attack, Field disclosure leads to Multi-player games attack, immutable bug leads to Rubixi attack, Unpredictable state leads to Dynamic libraries attack, and the GovernMental attack exploits the Immutable flaw, Stack overflow, Unpredictable state, Timestamp dependence vulnerabilities.
Attackers exploit the recursive sending through Reentrancy attacks [32]. In addition to that, through the Liveness Attack, attackers use the dilation of the confirmation duration [33]. This attack comprised of three phases, such a preparation phase, transaction denial phase, and the blockchain retarder phase. Preparation phase behaves as same as the selfish mining attack in which attacker build the private chain longer than public chain and take advantage over honest miner who is proceeding with the public blockchain. Dishonest miners privately keep the transaction blocks to prevent the transaction from being recorded into the public chain. At the last phase, the attacker would release their privately held blocks into a public chain in a proper time.

## 4. Conclusion

From this study, it can be identified that the blockchain is a trending technology deal with transaction aimed to be with high-end security. In this technology, it offers and complies important security aspects needed for the secure operation and handling. However, some vulnerabilities also exist and may lead to some identified attacks. It is necessary to invent appropriate technology to overcome these risk and attacks even though blockchain integrated with existing security technologies. As Summary, Blockchain 1.0, 2.0 may face some critical risks such Majority attack caused by consensus mechanism, private key security caused by public-key encryption scheme, criminal activity caused by cryptocurrency application, Double spending caused by Transaction verification mechanism, Transaction privacy leakage caused by a Transaction design flaw, and Criminal smart contracts caused by Smart contract application. And especially, Blockchain 2.0 faces some other risks such vulnerabilities in the smart contract created by a Program design flaw, Under-optimized smart contract caused by Program writing flaw, and Under-priced operations caused by EVM design flaw. Most of these attacks leaves a room for some other attacks, so that simply we can say that most of the attacks are allied with at least one attack.

## References

[1] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies Introduction to the book*. 2016.
[2] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, 2017.
[3] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016.
[4] S.N. Samsudeen and M.H. Thowfeek, Blockchain Technology Adoption by Chain Professionals, *International Journal of Psychosocial Rehabilitation*, 24 (1), pp. 121-137, 2020.
[5] D. Wörner and T. Von Bomhard, "When your sensor earns money: Exchanging data for cash with Bitcoin," *UbiComp 2014 - Adjun. Proc. 2014 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput.*, pp. 295–298, 2014.
[6] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.
[7] M. Ali *et al.*, "Blockstack : A Global Naming and Storage System Secured by Blockchains,"



ISSN: 2005-4238 IJAST

`

*USENIX Annu. Tech. Conf.*, pp. 181–194, 2016.

[8] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 2015, pp. 180–184.

[9] S. Sayadi, S. Ben Rejeb, and Z. Choukair, "Blockchain Challenges and Security Schemes: A Survey," in *Comnet 2018 - 7th International Conference on Communications and Networking*, 2019.

[10] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," *USENIX Secur. Symp.*, 2015.

[11] I. Eyal and E. G. un Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," in *Financial Cryptography and Data Security: 18th International Conference*, 2014, pp. 436–454.

[12] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proceedings - IEEE Symposium on Security and Privacy*, 2015.

[13] N. T. Courtois and L. Bahack, "On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency," 2014.

[14] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," 2015.

[15] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," *IEEE Secur. Priv.*, 2014.

[16] K. Wüst, H. Ritzdorf, G. O. Karame, V. Glykantzis, S. Capkun, and A. Gervais, "On the Security and Performance of Proof of Work Blockchains," 2016.

[17] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Čapkun, "Tampering with the delivery of blocks and transactions in Bitcoin," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2015.

[18] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, 2017.

[19] N. Hajdarbegovic, "Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack," *Coindesk*, 2014. .

[20] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[21] Dean, "51% attack," 2015. [Online]. Available: http://cryptorials.io/glossary/51-attack.

[22] I. Eyal and E. G. un Sirer, "How to Disincentivize Large Bitcoin Mining Pools," 2014. [Online]. Available: http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/.

[23] J. Bae and H. Lim, "Random Mining Group Selection to Prevent 51% Attacks on Bitcoin," in *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018*, 2018, pp. 81–82.

[24] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake," *Cryptol. ePrint Arch.*, 2014.

[25] C. Natoli and V. Gramoli, "The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example," 2016.

[26] M. Rosenfeld, "Analysis of Hashrate-Based Double Spending," pp. 1–13, 2014.

[27] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute," 2008.

[28] G. O. Karame, E. Androulaki, and S. Čapkun, "Double-spending fast payments in Bitcoin," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2012.

[29] X. Yu, M. T. Shiwen, Y. Li, and R. Deng Huijie, "Fair deposits against double-spending for Bitcoin transactions," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017.

[30] B. Rivlin, "Vitalik buterin on empty accounts and the ethereum state," 2016. [Online]. Available: https://www.ethnews.com/vitalik-buterin-on-empty-accountsand- the-ethereum-state.

[31] S. Solat *et al.*, "ZeroBlock : Preventing Selfish Mining in Bitcoin To cite this version : HAL Id : hal-01310088 ZeroBlock : Preventing Selfish Mining in Bitcoin," 2017.

[32] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK),"



ISSN: 2005-4238 IJAST

`

in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, pp. 164–186.

[33] A. Kiayias and G. Panagiotakos, "On Trees, Chains and Fast Transactions in the Blockchain," 2019.

[34] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (Poster Abstract)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[35] R. Zhang and B. Preneel, "Publish or perish: A backward-compatible defense against selfish mining in Bitcoin," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[36] "What is Ethereum?" [Online]. Available: https://ethereum.org/en/. [Accessed: 04-Sep-2020].



ISSN: 2005-4238 IJAST