

Overview of Issues, Challenges and Various Attacks Executed on Blockchain Technology

Raju B Amle¹ and Ajay U. Surwade ²

¹⁻²School of Computer Sciences Kavayitri Bahinabai Chaudhari North Maharashtra University,
Jalgaon, INDIA

Email: amle.raju@gmail.com, ajaysurwade@gmail.com

Abstract—Blockchains is one of the emerging technologies now a days. It has been popular because of its decentralized, peer-to-peer transaction and immutable properties. In this current scenario blockchain technology is suffering from various attacks such as Liveness Attack, Selfish Mining Attack, DAO Attack, BGP Hijacking Attack, Sybil Attack along with some scams which includes Ponzi scam, honeypot, and smart contracts vulnerability.

In this paper, we have presented systematic overview of the issues and challenges blockchain technology is facing along with various types of attacks executed on blockchain technology.

Index Terms— Blockchain, Issues and challenges, Scams or Attacks.

I. INTRODUCTION

Blockchain technology is becoming popular because of its decentralized, peer-to-peer transaction and immutable properties. In blockchain once the data is added to the block then no one can modification of this data. In the blockchain network all the blocks are cryptographically connected to each other with hash [1-4]. Satoshi Nakamoto first introduces the Blockchain concept, for solving double spending problems in electronic transactions [3,4]. Blockchain is also called a distributed digital ledger which is immutable and secured with cryptographic techniques. The peer nodes are imitated by consensus in a peer-to-peer network for transaction log that is controlled in a decentralized fashion [4,7]. Now-a-days number of criminal activities are occurred in the blockchain network such as honeypot, Sybil attack, Liveness attack, Selfish mining attack, DAO attack. One of the scams that affect the cryptocurrencies and blockchain network is Ponzi scam. Ponzi scam is a financial fraud, in which company promises the investor to return high value for the investment. Currently many cryptocurrencies fraud and scam that are executed on the blockchain network [5].

The paper is organized as Blockchain Issues, followed by challenges and which is then followed by various attacks executed on Blockchain. It is then followed by conclusion.

II. BLOCKCHAIN ISSUES, CHALLENGES AND ATTACKS

The Blockchain network has various issues, challenges and Attacks which are described below.

A. 51% Vulnerability

First, Satoshi Nakamoto has modeled the threat of 51% Vulnerability or attacks on blockchain theoretically. In which he proposed that the strength of blockchain network can be braked if an attacker can read 51% basics of

that blockchain [6]. For validating transactions in the blockchain network, it needs minimum approval of 51% node means, it is greater than 50%. Even though it looks difficult to get 51% approval, but the situation may arise where a single node can hold majority of resources (i.e., 51% resources) where the attacker may utilize these nodes to validate the invalid transactions [4, 7]. The same situation had happened in 2014, the mining resources of Bitcoin reached up to 42 percent in the case of ghash.io. The other users had withdrawn their participation from the system by assuming that it would reach 51% [4, 6, 7].

B. Slow and Cumbersome Execution

For individual transactions, transaction speed time along with storage capacity are important issues. Table-1 shows the transaction speed per second for different blockchain networks.

TABLE I. BLOCKCHAIN NETWORK TRANSACTION SPEED IN SECONDS [8-12]

Blockchain Network Name/Type	Transaction Speed Per Second
Bitcoin	7 [8]
Ethereum	15 [9]
Ripple	1500 [10]
Visa	56,000 [11, 12]

In the blockchain, it requires the selection of blockchain protocol and framework that provide guidelines, the structure of the blockchain, and the development of software applications [1, 13-16].

C. Security of the Private Key

For the sake of providing security, secrete key is assigned for the node in blockchain technology which is unique. If randomization of this secrete key is poor, an attacker hacks the private key and grabs the content of it [17]. Thus, the security of private keys is an issue in the blockchain network.

D. Double Spending

The same cryptocurrency is used for executing more than one transaction in Blockchain. In this double-spending process, the gap between starting time of the first transaction and the confirmation time of other transactions is exploited. In this process, before majority of nodes declare that the transaction is invalid, attackers collect the result of the first transaction which creates a problem [18, 7].

E. Standardization

In Blockchain network standard protocol for users or customers who are interconnected with it is missing. In the current scenario, the number of users are increasing day by day. Lack of standardization or lack of protocol allows expert users or programmers to do everything as per their wish and level of expertise which creates problems for the IT departments [6, 19]. It needs to develop some standard or mechanism using which the users are restricted from doing some nuisance. The standards to interconnect or mechanism would certainly help organizations and users of blockchains networks to easily interact with application development, consensus algorithm to validate and easy to use or integrating to the existing systems [6, 7, 20].

F. Environmental Cost

To use blockchain in any company or industries it requires Blockchain-based software, hardware, cost of operating blockchain may affect the environment [6]. Blockchain technology is affecting the environment in terms of power consumed which emits CO₂ in the environment.

G. Criminal Activities

Over the Internet, very large number of malicious users along with attackers are trying to hack the various networks, they execute various types of attacks which includes Smart Contracts with vulnerability, Liveness attack, Selfish mining attack, DAO attack, Ponzi scheme, Border Gateway Protocol (BGP) Hijacking, Honeypot and Sybil Attack on the blockchain network.

Since Bitcoin are assigned to users without verifying their address proofs and identity it is difficult to trace out payment made in the form of Bitcoin.

Criminal activities can be executed on the blockchain, one example of it is the widespread Ransomware all over the world. The Ransomware is meant to attack the Windows OS which encrypts the Users data and all import files on the user's machine and then demand is initiated from the attackers for the payment in the Bitcoin currency [6, 21]. The following are some attacks that are executed on Blockchain networks:

Ponzi scheme

Ponzi scheme is popular fraud executed by making a fake promise to the user to return high value on the money they have invested in several schemes. In this process, the old investor's fund or money is paid to the new investors. In this way, money is circulated among the users, if enough fund is not available then the money lost by other users are used for this purpose.

Systematic research has been carried in [18, 22]. Massimo Bartoletti et al. [22] have identified 138 Ponzi schemes on Ethereum, that deployed public dataset on Ethereum platform, Total 184 contracts are used from goo.gl/CvdxBp website [22].

Weili Chen et al. [23] have proposed a model to estimate that more than 400 Ponzi schemes that running on Ethereum platform, to Used machine learning methods and data mining techniques to detect the Ponzi scheme in the Ethereum blockchain [23].

Massimo Bartoletti et al. [24] have used the clustering algorithms and classifiers to detect Ponzi schemes on Bitcoin [24]. The features extraction and method to detect Ponzi scheme have been discussed in [23] and [24]. The development and implementation of Blockchain now the Ponzi scheme is a veil of smart contract the detection of Ponzi scheme is one of the important problems [23].

Amle and Surwade [25] have suggested an architecture to classify the Ponzi and Non-Ponzi Schemes on Blockchain by extracting features using Machine Learning Classifier.

Honeypot

The Smart contract Honeypot has hidden traps that contain attacks inside. The definition quoted in [26], "A honeypot is a smart contract that pretends to leak its funds to an arbitrary user (victim), provided that the user sends additional funds to it. However, the funds provided by the user will be trapped and at most, the honeypot creator (attacker) will be able to retrieve them".

The honeypot is a trap that attracts the users which operates in the following manner:

- 1 Initially, the attacker deploys the contract which is vulnerable and places a trap for the user in the notion of money or funds.
- 2 The user then responds to this contract and sends or provides the required amount of money and gets in the trap.
- 3 The attacker after step 2, withdraws the money or funds together with the amount paid by the victim [18, 26].

The honeypot can easily be set up for trapping the users. In [26] the detailed taxonomy of honeypot has been described.

Smart Contracts with Vulnerabilities

The invoked smart contract has a series, which can occur throughout its lifetime [27]. The exploits which is the consequence of smart contract invocations are called trace exploits. These exploits are classified as suicidal, prodigal, and greedy [28] described below.

Suicidal Contracts

The Smart contracts which are killed by any arbitrary address are called suicidal contracts. These contracts are built with a provision that can kill themselves against attacks. In The ParitySig attack [29] the same situation was occurred, in which the arbitrary user got the ownership of the library contract and killed it. It had locked the funds associated with it [29].

Prodigal Contracts

The Smart contracts which can leak the fund or money to any addresses, which is neither the owner of the contract nor has deposited Ether to the contract are called prodigal contracts. These contracts have internal calls to send funds to some other contracts or addresses [28].

Greedy Contracts

The Smart contracts which are unable to release Ether are classified as greedy contracts. In ParitySig attack described in [27-29], very large number of contracts that were dependent on library contracts would not release funds or ether which has resulted in the estimated loss of 30 million USD. The greedy contracts are further divided into two types one is the contracts that can accept Ether but do not possess instruction to send funds, so could not release funds and the other type is the contracts that accept Ether do have instructions to send funds, but still not able to transfer the funds [27-29].

The Liveness Attack

The liveness attack is proposed by Aggelos. et.al [30], in which he suggested that it is possible to delay the confirmation time of the target transaction for considerably more time during which an attack can be executed. In [30, 31] two instances of similar attacks on Bitcoin and Ethereum has been discussed. This attack consists of the following three stages which include preparation phase, transaction denial phase, and blockchain delay phase [32]. The attackers during the preparation phase, want to get the potential advantage by targeting the honest players for building their private chain. The attacker tries to delay a block that is genuine, which consists of transaction, and proceeds to the blockchain render phase when attackers decide that this delay is unconvincing, and they try to reduce the rate at chain transaction grows [5].

Selfish Mining Attack

The new miner executes this attack for wasting the computing power and time vested by the legitimate miners, prevents them to earn the profit and earning the rewards. These attackers divide the private chain by making the discovered block private [33]. Self-employed miners try for maintaining a long private branch of blocks than the public branch which can be dug out and can personally hold the large number of blocks which are found. During this period the public chain is being dug by the honest miners. When the length of the public branch reaches the length of the private branch newly mined block is revealed by attackers [34]. Thus, it keeps these honest miners away from the profit that they should earn using these blocks [5, 34].

DAO Attack

Due to lack of the centralized authority, the Decentralized Autonomous Organizations (DAOs) are used as funds invested for crypto, and distributed spaces have minimized costs and provide more access and control to the investors. The German start-up Slock has developed the coding framework, which is open source in nature for developing smart locks. The DAO is not owned by anyone it is just software running on the Ethereum platform [36, 37]. The attackers started exploited the bugs of DAO and these are called DAO attacks. Prior to this attack, it has collected funds of 120 million and the attacker stole around US\$60 million, thus, it became one of the major attacks executed on the Ethereum consensus model. The attacker is exposed to malicious smart contracts, which are having a call-back function along with a call to 'withdrawal' function. It transfers Ether to the called party. Thus, an attacker can steal all the Ethers. [5, 37].

BGP Hijacking Attack

The Border Gateway Protocol (BGP) was developed for sharing the information of routings on the internet, which disseminates the information of IP packets forwarded towards destination from the source. The attackers after intercepting this information in the blockchain network can route the traffic according to their wish by manipulating the BGP [38]. According to a report published by Dell Secure Works, the connections of the mining pool of servers of Bitcoin has been intercepted by this attack in the year 2014 [5, 39].

Sybil Attack

In Sybil attacks many nodes in the distributed system are controlled by few real entities which forces the reputed system to misbehave by changing its identity in peer-to-peer networks [5]. Thus, the Sybil attacks defame the reputed systems in the security system. The Beaver system is proposed in [40] to resist Sybil attacks and to protect the privacy of users by collecting nominal money as processing fees.

III. CONCLUSIONS

This paper presents an overview of the emerging technique called Blockchain. Blockchain technology is becoming popular because of its decentralized, peer-to-peer transaction and immutable properties.

It also discusses Blockchain issues along with challenges and attacks which includes Ponzi scheme and Greedy threat to Ethereum smart contract. The Blockchain has been suffering from the challenges such as transaction speed of blockchain network and several attacks such as 51% Vulnerability, Technical execution problems of Blockchain which is Slow and Cumbersome execution, Security of Private key and Double Spending.

Blockchain technology is not having a standard protocol using which users can connect to Blockchain networks. It has increased problems while validating the consensus algorithm. So, setting up a standard protocol is necessary. Blockchain technology is affecting the environment in terms of power consumed which emits CO₂ in the environment.

This paper has discussed overview of Blockchain along with issues and challenges. As a new technology, blockchain is susceptible to malicious attacks such as the Ponzi scheme and Honeypot. Also, selfish mining

attacks, DAO attacks, Liveness attacks, Border Gateway Protocol (BGP) Hijacking, and Sybil attacks are emerging threats to this popular blockchain network.

REFERENCES

- [1] Mohsen Attaran. Blockchain technology in healthcare: Challenges and opportunities, *International Journal of Healthcare Management*, pp:1-14, DOI: 10.1080/20479700.2020.1843887. 2020.
- [2] Andreas M. Antonopoulos. *Mastering Bitcoin Programming the Open Blockchain*. Second Edition. O'Reilly Media. 2017.
- [3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008, (www.bitcoin.org/bitcoin.pdf) 2008
- [4] H. T. M. Gamage, H. D. Weerasinghe, N. G. J. Dias¹, A Survey on Blockchain Technology Concepts, Applications, and Issues. *SN COMPUT. SCI.* 1, 114 Springer Nature Singapore, DOI: 10.1007/s42979-020-00123-0, 2020.
- [5] Saurabh Singh, A. S. M. Sanwar Hosen, And Byungun Yoon, "Blockchain Security Attacks, Challenges, And Solutions For The Future Distributed Iot Network" *Special Section On Internet-Of-Things Attacks And Defenses: Recent Advances And Challenges Volume 9*, 2021, DOI 10.1109/ACCESS.2021.3051602.(2021).
- [6] Suyel Namasudra, Ganesh Chandra Deka, Prashant Johri, Mohammad Hosseinpour, Amir H. Gandomi., *The Revolution of Blockchain: State-of-the-Art and Research Challenges*, *Archives of Computational Methods in Engineering* DOI: 10.1007/s11831-020-09426-0. 2020.
- [7] Saleh F. Blockchain without waste: proof-of-stake. *SSRN Electron J.* DOI:10.2139/ssrn.3183935. 2019.
- [8] Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gün E. On scaling decentralized blockchains. *Lecture Notes in Computer Science*. PP106–25. DOI: 10.1007/978-3-662-53357-4_8. 2016.
- [9] Ethereum Wiki. Sharding FAQ. (<https://github.com/ethereum/wiki/wiki/Sharding-FAQ>.)
- [10] Ripple.com. XRP | Ripple. (<https://ripple.com/xrp/>.)
- [11] Herrera-Joancomartí J, Pérez-Solà C. Privacy in bitcoin transactions: new challenges from blockchain scalability solutions. *Lecture Notes in Computer Science*. pp 26–44. DOI: 10.1007/978-3-319-45656-0_3. 2016.
- [12] Visa Inc. Visa: 56,582 transaction messages per second! (<http://visatechmatters.tumblr.com/post/108952718025/56582-transaction-messages-per-second>.)
- [13] Pirtle C, Ehrenfeld JM. 2018. Blockchain for Healthcare: The Next Generation of Medical Records? *Journal of Medical Systems* 42:172. DOI: 10.1007/s10916-018-1025-3. (2018)
- [14] Bhabendu Kumar Mahanta, Debasish Jena, Soumya Shree S. Panda, Srichandan Sobhanayak., *Blockchain technology: A survey on applications and security privacy Challenges*. *Internet of Things* 8 100107. 2019.
- [15] Juon-Chang Lin^{1,2} and Tzu-Chun Liao, Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, Vol.19, No.5, PP.653-659, DOI: 10.6633/IJNS.201709.19(5).01. 2017.
- [16] S. Dey. Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory: A Proof of Work, *10th Computer Science and Electronic Engineering (CEECE)*, pp. 7-10, DOI: 10.1109/CEECE.2018.8674185. (2018).
- [17] ECDSA Security in Bitcoin and Ethereum: a Research Survey. <https://blog.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-and-Ethereum-a-Research-Survey.pdf>
- [18] Z. Zheng, S. Xie, H.-N. Dai et al., An overview on smart contracts: Challenges, advances and platforms., *Future Generation Computer Systems* DOI: 10.1016/j.future.2019.12.019.
- [19] Schatsky D, Arora A, Dongre A., *Blockchain and the five vectors of progress*. (<https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/value-of-blockchain-applications interoperability.html>)
- [20] Blockchain.com. Blockchain Size. (<https://www.blockchain.com/charts/blocks-size>.)
- [21] Juels A, Kosba A, Shi E. The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, New York, NY, USA, pp 283–295. 2016.
- [22] M. Bartoletti, S. Carta, T. Cimoli, R. Saia. Dissecting ponzi schemes on ethereum: identification, analysis, and impact, *Future Generation Computer Systems*, arXiv preprint arXiv:1703.03779. 2019.
- [23] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, Y. Zhou, Detecting ponzi schemes on ethereum: Towards healthier blockchain technology, *Proceedings of the 2018 World Wide Web Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, 2018, pp. 1409–1418. (2018).
- [24] M. Bartoletti, B. Pes, S. Serusi., Data mining for detecting bitcoin ponzi schemes, *Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT)*, IEEE, 2018, pp. 75–84 . (2018)..
- [25] R. B. Amle and A. U. Surwade, "Ponzi Scam Attack on Blockchain", In the *Proceeding of the 6th International Joint Conference on Advances in Computational Intelligence (IJCAI-2022)* organised by SAU Center for Research and Innovative Learning (SCRIL), South Asian University, India and Jahangirnagar University, Bangladesh held on 15-16 October 2022.
- [26] C. F. Torres, M. Steichen., The art of the scam: Demystifying honeypots in Ethereum Smart Contracts, arXiv preprint arXiv:1902.06976v2. 2019.
- [27] Wesley Joon-Wie Tann, Xing Jie Han, Sourav Sen Gupta, and Yew-Soon Ong. Towards Safer Smart Contracts: A Sequence Learning Approach to Detecting Security Threats. *Proceedings of ACM (Conference '19)*. ACM, New York, NY, USA, 12 pages. (2019).

- [28] Ivica Nikolić, Aashish Kolluri, Ilya Sergey, Prateek Saxena, and Aquinas Hobor. Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC '18). ACM, New York, NY, USA, 653–663. DOI: 10.1145/3274694.3274743. (2018).
- [29] Parity Technologies. Security Alert. (<https://paritytech.io/security-alert-2/>.)
- [30] A. Kiayias, G. Panagiotakos, On trees, chains and fast transactions in the blockchain, 2016. URL <https://eprint.iacr.org/2016/545.pdf>. 2016
- [31] A. Kiayias and G. Panagiotakos. On trees, chains and fast transactions in the blockchain, Lecture Notes in Computer Science (LNCS); Vol. 11368, Springer International Publishing, <https://doi.org/10.1007/978-3-030-25283-0>. 2019.
- [32] S. W. Kim. Safety and Liveness—Blockchain in the Point of View of FLP Impossibility. (<https://medium.com/codechain/safety-and-liveness-blockchain-in-the-point-of-view-of-flp-impossibility-182e33927ce6>)
- [33] Q. Zou, Y. Tang, , J. Chen, K. Li, C. A. Kamhoua, K. Kwiat, and L. Njilla. ChainFS: Blockchain-Secured Cloud Storage. Proceedings IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 987–990. (2018)
- [34] S. Solat and M. Potop-Butucaru,. ZeroBlock: Preventing selfish mining in bitcoin. Sorbonne Universities, UPMC Universities, Paris, France, Tech. Rep. hal-01310088v1, 2016, pp. 1–17. (<https://hal.archives-ouvertes.fr/hal-01310088v1>). 2016.
- [35] What is Selfish Mining. Tokens. (<https://www.tokens24.com/cryptopedia/mining/what-is-selfish-mining>.)
- [36] Understanding the DAO Attack. CoinDesk. (<https://www.coindesk.com/understanding-dao-hack-journalists>)
- [37] Phil Daian. Analysis of the DAO Exploit. (<http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>)
- [38] M. Apostolaki, A. Zohar, and L. Vanbever,(Hijacking bitcoin: Routing attacks on cryptocurrencies. . Proceedings IEEE Symp. Secur. Privacy (SP), May 2017, pp. 375–392. 2017).
- [39] J. Stewart. BGP Hijacking for Cryptocurrency Profit. (<https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit>.)
- [40] K. Soska, A. Kwon, N. Christin, and S. Devadas, 2016. Beaver: A Decentralized Anonymous Marketplace with Secure Reputation. IACR Cryptol. ePrint Arch., vol. 2016, pp. 464–479, 2016.