IEEE - 45670

Blockchain Security Attack: A Brief Survey

ANITA.N
Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai, India
anita.anjalinatarajan@gmail.com

VIJAYALAKSHMI.M
Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai, India
mviji@tce.edu

***Abstract*—Blockchain technology has attracted various areas like corporations, education, government, and healthcare because of its unhackable security features. In spite of common arguments about the occurrence of Blockchain technology in terms of security and privacy, in reality, several attacks can be launched against them. This paper presents a comprehensive survey of the most vulnerable Blockchain attacks and the different approaches proposed against these attacks. This paper also provides taxonomy of attacks, which are most challengeable to Blockchain security key features. Additionally, a review of the countermeasures, which have offered solutions to avoid these attacks, has been presented.**

Keywords—Blockchain, Attacks, Distributed transactions, Distributed Denial of Service, 51% attack, Challenges .

I. INTRODUCTION

Traditional data management software has been used globally across every industry. A traditional database has client-server network architecture. Control of the database remains with administrators, by allowing access permissions to be maintained by the central authority. This will lead to a single point of failure and inefficiency. Although, the current business scenario has overcome this deficiency by means of distributed transactions, they have their own disadvantages. It includes third-party validation, limited transaction sizes, increasing transaction cost and transparency.

Most of the Indian economy relies on the interpersonal trust for their daily transaction. This trust is just temporary and is never authenticated anywhere by the peers. This leads to a large number of security vulnerabilities in the present transaction system. Hence, to improve the security and authenticity in the transactions, there is a necessity for a new paradigm and as a result Blockchain is introduced to enhance the security.

The Blockchain is an open, decentralized ledger that records transaction between two parties in a permanent way without a third-party authentication. The need for security has led the researchers to the path of Blockchain which has promising features such as immutability, transparency, distributed ledger, decentralized systems, better security, consensus, non-third-party authentication, faster settlement, cost-effective and anonymity .Of the various advantages and the features of the technology, the key features and its description are given below in Table 1.

TABLE 1: BLOCKCHAIN KEY FEATURES AND ITS DESCRIPTION

Key features	Description
Immutability	Nobody can modify the distributed ledger of Blockchain.
Transparency	Transactions of each public address are open to all Blockchain users in trustworthy and secured manner.
Distributed ledger	A digital system or database for storing the transactions and recorded in multiple places .
Consensus	A fault tolerant mechanism and way of reaching agreement between all members of Blockchain.
Anonymity	Transactions on Blockchain are untraceable; it gives higher level of privacy.
Smart contract	Computer program allow the transaction without third parties.

Satoshi Nakamoto, the pioneer researcher in Blockchain, has proposed a system for electronic transaction [1] without a trusted party and provided a solution to double spending problem using peer to peer network. The Blockchain was initially rumored to be used only for Bitcoin application. But, Blockchain has emerged to be in use for various applications such as the Internet of Things (IoT), supply chain management, artificial intelligence, cryptocurrency, health care, governments [2-7].

Although Blockchain, is considered as a promising technology, it still has security loopholes through which the adversaries game in.

Blockchain threat report published by McAfee[8] has mentioned that Blockchain transactions carries security risks.Their list includes well adopted Blockchain implementations such as Bitcoin and Ethereum.

A plug-in in chrome browser [9] was found to be mining cryptocurrency without consent. Blockchain consumers are easier targets. Due to the focus on startup, the security often becomes a least priority, cryptocurrency companies falls in prey. IOTA cryptocurrency users lost 4 million by phishing attack[10].

Another notable incident is the theft of over $2 billion cryptocurrencies in 2017 on the Ethereum coinbase audit has been pointed out by a team of security analysts from coinbase. Fig1: Illustrates the comparison of the traditional and Blockchain network.

Therefore considering the seriousness of this security breaches, this paper focuses on the study of major Blockchain attacks and methodologies proposed against attacks. This paper presents taxonomy of various attack over Blockchain system. It also summarized the various methodologies to resolve these attacks in the Blockchain.

.

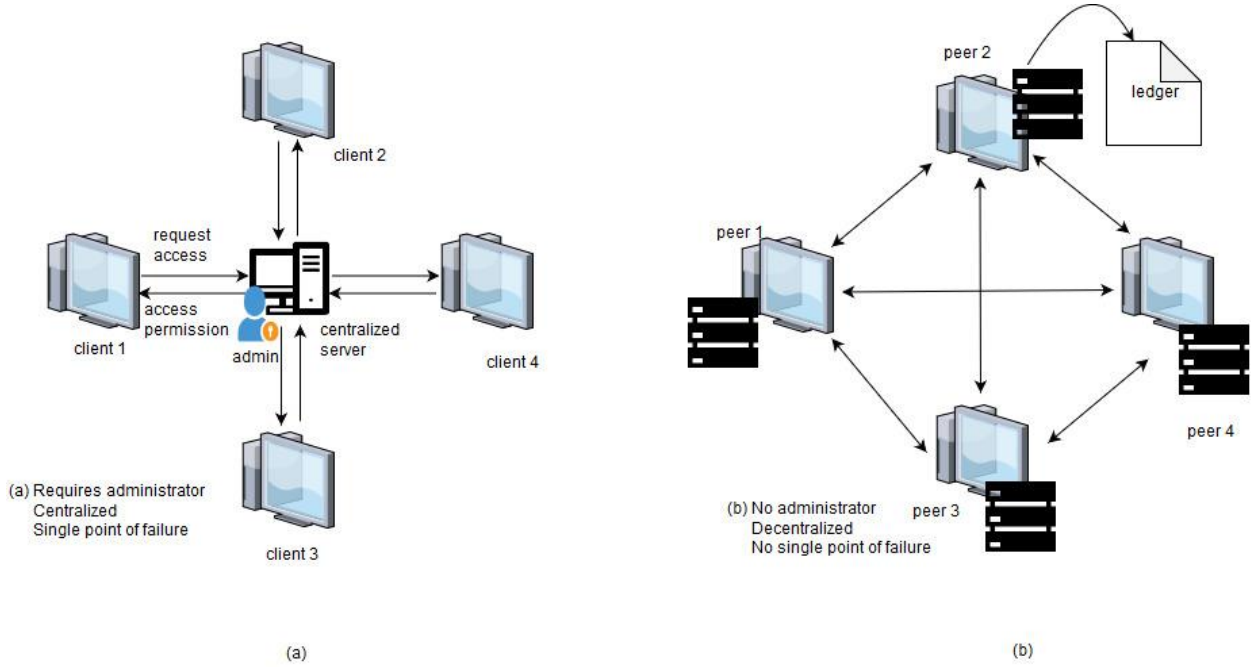

Fig 1 : (a) Traditional network and (b) Blockchain network

II. RELATED WORKS

As the need for security rises and the number of transactions escalated to a greater extent, researches in the field of Blockchain to mitigate the security issues also increased drastically. The most recent study and the methodologies in Blockchain are discussed as follows. Jiang et al. [11] have analyzed systematic study of the security threats to Blockchain and elaborated the corresponding real attacks which include selfish mining attack, DAO attack and BGP hijacking attack and eclipse attack. Banerjee et al. [12] have surveyed the articles focusing IoT security solutions and apprised attacks such as cyber attack, botnet malware, DoS and DDoS. The research of Taylor et al. [13] has systematically reviewed the recent and the most vulnerable attacked in the field of cyber security and the role of Blockchain in its mitigation. The various security issues is evaluated in IoT [14] and classified these issues pertaining to the various layers in the IoT stack. Recently, Ferraget al. [15] have categorized the thread models in the Blockchain protocols pertaining to the IoT networks. In [16] have deliberated the long-range attack wherein an attacker goes back to the genesis block and forks the Blockchain causing a serious threat to the proof of stack.

The related works listed above have focused on the security threats with respect to a particular application or a domain. This paper surveys the most predominant and vulnerable attacks in Blockchain system with respect to various applications. Unlike the existing papers, the proposed work deals with the classification of attack models which directly affects the security modules of Blockcahin directly such as decentralization, immutability, faster settlement and minting. In this paper research challenges have been analyzed.

III.TAXONOMY OF ATTACK INBLOCKCHAIN

Blockchain security services [17] have been divided into six categories: Data Privacy, Authentication, Data integrity, Non-reputation, Data Provenance, and Data confidentiality. Some of these services such as integrity, authentication, privacy, confidentiality are swaged by the most powerful attacks for example, Distributed Denial of Service(DDoS) [4], collision attack[18], sybil[19], eclipse[20], injection attack [21] [22], replay attack[6] and ransomware attack[23].

In this section, some of the major vulnerabilities of the Blockchain systems have been surveyed various security threats posed over Blockchain and the solutions which were proposed. Taxonomy of the attack on Blockchain is derived and presented in Fig 2.

A. Hash-based attack

This attack involves taking over hash values and trying to find the same hash value for various other messages transmitted. In this method, the attacker takes over more than 51 % of the hash value or the mining power of the network.

a) *51% percentage attack:* 51 % attack occurs in Blockchain, when a group of miners or a miner controls more than 50 percent of the mining hash or computer of the network. Attackers use 51% attack to reverse the transactions in a Blockchain and interfere with the process of the storing new block. These transactions are put into the pool of unconfirmed transactions and thereby neglecting the transaction from execution. 51% attack is possible even when mining power is less than 40% such as Ghash.io, Krypton and shift, Bitcoin Gold[24] but with a lesser probability.

The following attacks can be exploited by an attacker, due to this vulnerability that includes canceling all transaction, random forks, selfish mining and double spending.

Researchers have tried to mitigate [25] the 51% attack with the help of PirGuard Protocol implemented in Ethereum. Delayed proof of work [26] offered by Komodo gives a solution for avoiding the attackers to change or erase transaction records. The introduction of the distributed trust model for IoT [18] helps to avoid the launch of this attack.

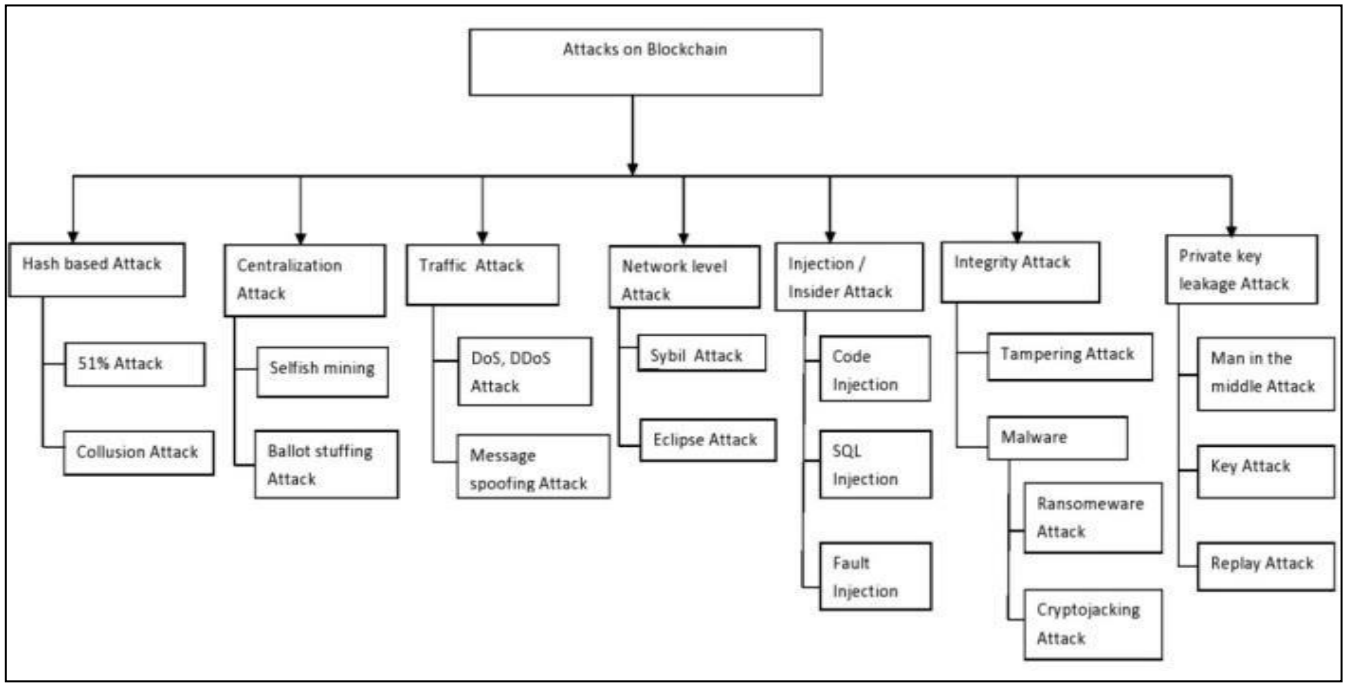

Fig 2: Taxonomy of attack on the Blockchain

Fig 3. indicates the work flow of 51 percent attack where an illegitimate miner creates a long chain because they have high computation power and can add a new block faster than a legitimate miner. New block created by the attacker will be added in the long chain of the network.

2) Collusion attack: A Collusion attacker finds a similar hash value for the data being transmitted in the network and thereby uses this value to gain reward by means of intrusion. In [18] have used Goldwasser-Micalli and Pilliar encryption schemes to restrict the collision attack and have used these encryption block in artificial intelligent applications. Both of these encryption schemes are highly cost-effective and induce less processing time, as they do not create any hashvalue.

B. Centralization attack

The Blockchain is a decentralized network that means the network operates on a peer to peer basis. The attacker here tries to break the decentralization and creates an illusion of centralization.

1) Selfish Mining: Malicious miner by keeping a valid block with themselves, they successfully send their secret block into the network. Zero Block scheme [27] guards this attack by using the novel timestamp-free technique. In this scheme, each block must be generated and received by the network within a max interval time. The selfish block will be rejected by an honest miner, when the selfish miner keeps that block as private more than the max interval. Nash equilibrium [28] model and some extended selfish mining strategies have been proposed to find an optimal policy for selfish miners

2) Ballot stuffing attack: The attack of e-voting Ballot stuffing or ballot box stuffing is an attack on the integrity wherein a person casts more than one allowable vote. Since the e-voting system is completely anonymous [29], universal verifiability of the identity of the person is difficult.

Universal verifiability, in some situations where anyone is able to check that the ballots in the boxes are counted correctly and hence, ballot box integrity problem occurs in both paper and electronic ballots. This attack may be avoided, when the voting date is organized as a national holiday. Zcash protocol [7] used in the voting system which offers anonymity of voter transactions. Decentralized trust management system [4] is formed in a vehicular network against ballot stuffing attack. Consequently, the proposed system stores the trust values in an effective and flexible manner. Obligation chain [2] with a built-in reputation mechanism reduces the delay of committing transactions.

C. Traffic attack

The traffic attack is one where the adversary node tries to jam the network by inducing congestion into the network and it results in the denial of service to the legitimate users.

*1) DDoS attack :*A distributed denial of service attack takes place, when the multiple systems flood the resources and the bandwidth of the targeted system. The target node gets denied off the transaction, due to overloading of the system. The security model [2] with multiple Blockchain technologies helps to filter out the illegitimate traffic using security switches. Security switches decide whether the node is normal or abnormal. Normal nodes are added into the legal node list and abnormal to the illegal node list and it is not connected to the Blockchain. This security model can detect an attack against spam transaction and avoids spam transaction.

A novel architecture [30] has been proposed for efficient and flexible DDoS mitigation solutions across the multiple domains. Recent research by [31] has introduced the component of the Patient-Centric Agent (PCA) which does not allow any of the fake traffic through the network. This mitigation is useful against DDOS attack in SDP devices and it is highly used in the healthcare sector.

DistBlockNet model for IoT [32] architecture is capable of detecting DDoS/DoS attack and security threads. As a result, it assures low-performance overhead and will satisfy the design principals in future IoT. Blockchain with the combination of cloud and network monitoring [c] provides

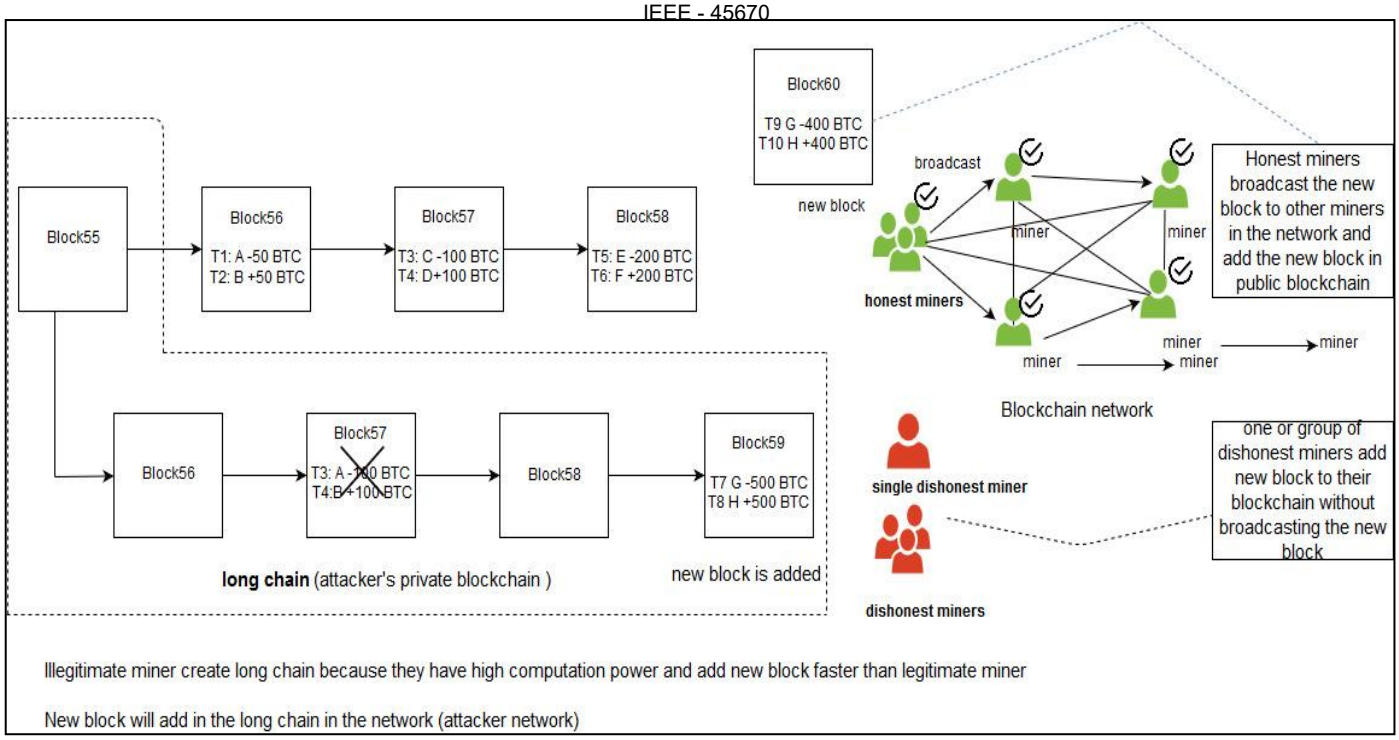

Fig 3: 51 percentage attack

the mitigation against DDoS attack. Fig 4: shows the DDoS attack on Blockchain.

The mitigation strategies for DDoS attack on Blockchain are as follows

- Operating Domain Name Server (DNS) on Blockchain.
- Using Ethereum and Blockchain.
- Network monitoring and DDoS mitigation tools.
- Using Software Defined Networking and Network Virtualization on Blockchain.

*2) Message spoofing attack :*Bayesian Inference-based rating generation scheme [18] has been used to prevent this attack by the message receiver. Message receiver analyzes the broadcast message from various vehicles and decides the trustworthiness of the messages. Trust values are combined in the Road Side Unit (RSU) based on rating generated by the message receiver. Blockchain with RSU works jointly to maintain a reliable and consistent database. An attacker may change the identity of the data owner by causing a spoofing attack. In tier based end-end architecture [31] an attacker cannot inject the wrong source or destination address.

D. Network level attack

Illegitimate user illegally uses the user accounts and privileges or stealing hardware, software to compromise the network security.

1) Sybil attack : Adversaries take control of multiple nodes in the network by setting nodes with multiple identities to create confusion in the network. As a result, the network topology causes abnormally high bandwidth consumption in VANET [19]. In [34] have proposed eco announcement protocol with threshold authentication method to achieve Sybil resistance by using signatures generated by a fixed number of different private keys. Proactive and retroactive [33] solutions have also been proposed against Sybil attack. Subsequently, it provides scalable implementation and it is consistent with network infrastructure.

2) Eclipse attack: An eclipse attack isolates communication with the normal node by blocking information. In [20] have proposed a total eclipse attack method to realize eclipse attack which monopolizes all the peer's connections. Bitcoin client divides two groups of methods namely new bucket and tried blocks based on IP address. New bucket contains the list of all peers and the unestablished outgoing connection in Bitcoin client. The tried block comprises the list of IP address which has been already established with connection by a client. As a result, the attacker fails to launch eclipse attack.

E. Injection or Insider attack

An unauthorized person accesses the computer system or network and delivers untrusted input to a program which is processed by an interpreter. Someone with an intimate knowledge of the system and administrative privileges tampers with the data and made a unique challenge. This is known as insider attack where an attacker with administrative privileges can alter login and records to eliminate the trace of attack and makes hard to detect the insider attack too hard.

1) Code Injection attack : An attacker exploits the vulnerabilities in the web application and injects code to change the course of execution. Blockchain anomaly detection [21] is resilient against the malicious user appending one's own transaction within a Blockchain causing injection of malicious code in the system.

*2) SQL Injection attack :*An attacker tricks the server to execute the malicious SQL queries, thus deleting or changing the database or stealing the sensitive data to introduce more attacks. A novel Blockchain based mutual authentication protocol proposed in RIFD(Radio Frequency Identification) guards against the SQL injection attack [22]. Consequently, security correctness proof and security attributes have made the RFID systems with high security and low real-time requirement and they can prevent from multiple attacks.

*3) Fault Injection attack :*The aim of this attack is to modify the software execution by sending the erroneous data to the device. A distributed protection framework [35] proposed in modern power systems utilizes Blockchain security characteristics. In this framework, meter nodes have

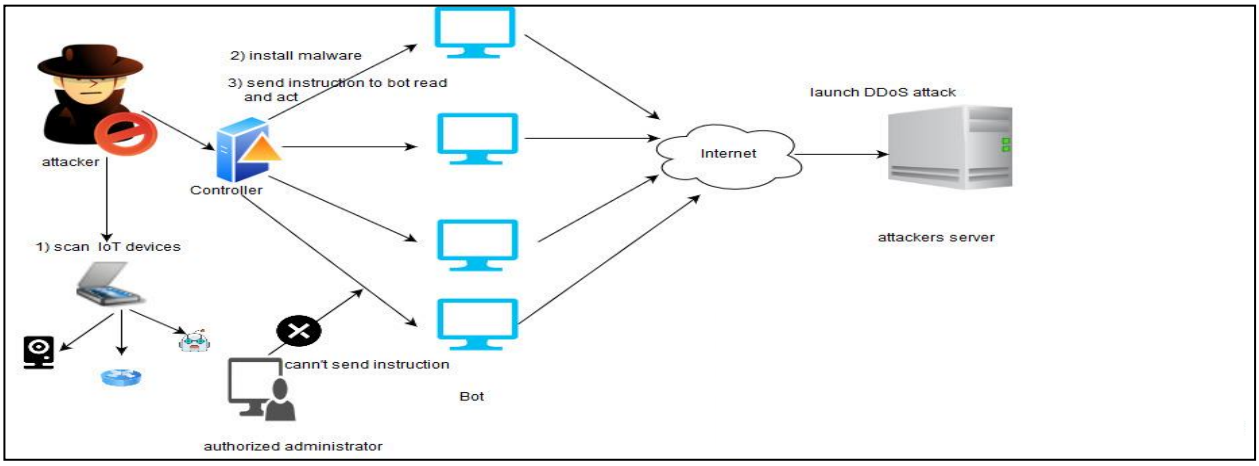

Fig 4: DDoS attack on Blockchain

considered a private Blockchain network. Each node verifies the integrity of the received data by using a consensus mechanism. IoT applications tend to provide wrong services or low reliability in the network, due to this attack. Authentication algorithm has been proposed by [36] in IoT applications to safeguard the network from false data injection attack.

E. Integrity attack

Merkle tree ensures the integrity of data in the Blockchain. Adversary tries to modify the data in the block and once the integrity is compromised, there is no way to restore the original data. The threat span from malicious alteration of data to data is updated without all the involved members.

*1) Tampering attack :*Credit coin [34] announcements and the transactions cannot be modified without authorization. The hash property saves the transactions from being tampered by hash re-computation in every block in case of modification. An attacker cannot do the tampering, due to the properties of hash in the Blockchain. It means, if an attacker modifies the content of block, the hash value is recalculated for every block. As a result, longer Blockchain protects against this attack.

*2) Malware attack :*Malware is a software designed to seize a computer's processing power secretly and to use it to mine the cryptocurrency. Unauthorized cryptocurrency miners in the network not only affect individual user device but also the overall network. These attacks are less visible, more silent threats and induce false sense of security.

- *Ransomware attack :*An attacker restricts the authorized user to access the data in one's own network by the injection of ransomware. Due to this attack, the victim is denied of the files, as the network is infected and encrypted by malicious software. Anti-malware deduction system [23] has been proposed to mitigate the ransomware attack. Malware Detection as a Service (MDaaS) provides the running services for Malware behavioral analysis, Malware code analysis, and Malware report. As a result, malware can be easily detected and mitigated.
- *Cryptojacking attack : Saad et al.* [5] have analyze malicious crypto jacking static and dynamically. In static based analysis, a content cryptocurrency based analysis finds crypto jacking attack between currencies and mining process . In JavaScript code, crypto jacking script is identified by using unique code complexity. The dynamic based analysis highlights the impact of crypto jacking on system resources and it is analyzed in terms of battery power and CPU.

F) Private key leakage attack

An attacker may extract the keys from memory or else they can use duplicate values [37] to leak nonces and secret keys when the same key and nonce used more than once.

*1) Man in the middle attack :*A tier based end-end architecture [31] has been structured where devices at a different segment have the same key for every session to preserve against man in the middle attack. In SSL and 802.11p based VANET [34] the traditional man in the middle attack is impossible. If the attacker modifies the value of coin or address, the transactions will be rejected by the receiver, during the consensus phase.

2) Key attack: Device wise dynamic key generation mechanism is used to generate the symmetric key for authentication [31]. Even when the attacker compromises with one device, other devices are safeguarded from key attack.

*3)*Replay attack: The lightweight authentication protocol [31] with system time($Time_s$) and nonce(N_s) is designed to guard against a replay attack. The message of the event[34] is generated with a description of time. Receivers check the current time and the event time when the Announcement- Aggregated Packet (AGP) is received. To the end, the adversary will fail to reply attack in case of discrepancies.

IV. RESEARCH CHALLENGES

Though several researchers have proposed mitigations to the Blockchain attack, security loopholes occur in Blockchain through which the attackers attack the system. The challenge, yet to replace with others to be addressed, is scalability which is a major issue with network security applications, where thousands of users need to be served and the network scales up fast. Both Bitcoin and Ethereum have slow transaction speed and higher fee is charged per transaction. Security framework is faced by current research in the field of security systems which needs a dynamic and adaptable security framework for Blockchain IoT architectures (BIoT). There is no correct solution to rectify the 51 percent attack.

Energy consumption is one of the challenge most of the

Blockchain use proof of work, in the next two years, Bitcoin requires more electricity than what the entire world presently uses. Public Key Infrastructure (PKI) relays on third-party Certificate Authorities (CA) to issue, revoke and store key pairs and an attackers can target easily. Resilience is another challenge and an innovative resilient design is needed against combined application free attacks in case of low resource-constrained IoT devices.

III. CONCLUSION

This paper presents taxonomy of security threats on Blockchain systems. The attack on Blockchain and the methodologies to mitigate them is presented in detail. It provides a comprehensive survey of attack and solutions to Blockchain system. The challenges and research directions are the presented at the end. This paper concludes with the further research challenges in Blockchain technologies. As a future scope, research methodologies and algorithms pertaining to the research areas are to be devised and the performance of the algorithm are to be improved.

REFERENCES

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic CashSystem. Accessed:. [Online]. Available: ps://Bitcoin.org/Bitcoin.pdf,Apr. 10, 2018.

[2] R. Di Pietro,X. Salleras,M. Signorini, and E. Waisbard, .A Blockchain-based Trust System for the Internet of Things, In Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies. ACM, pp. 77-83, 2018,June.

[3] M. Sidorov, M.T., Sridharan, R.V., Nakamura, J, R.Ohmura, and J.H. Khor, Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. IEEE Access,vol.7, pp.7273-7285,2019.

[4] Z. Yang,K. Yang,L. Lei,K. Zheng, and V.C. Leung, Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of ThingsJournal, vol.6,pp.1495-1505, 2018.

[5] M. Saad, A. Khormali, and A. Mohaisen, End-to-end analysis of in-browser Cryptojacking. arXiv preprintarXiv:1809.02152, 2018.

[6] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, A Blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In IFIP International Conference on Autonomous Infrastructure, Management and Security, Springer,Cham, pp. 16-29,2017, July.

[7] R. L. Rivest, Perspective on Electronic voting, in Financial Cryptography, 5th International Conference,, LNCS, Springer, FC 2001, Vol. 2339, pp.243-268, 2001.

[8] Catalin Cimpanu, IOTA Cryptocurrency Users Lose $4 Million in Clever Phishing Attack, https://www.bleepingcomputer.com/news/security /iota-cryptocurrency-users-lose-4-million-in-clever-phishing-attack/, 2019.

[9] Robert Hacket,,Popular Google Chrome Extension Caught Mining Cryptocurrency on Thousands of Computers, https://finance.yahoo.com/news/popular-google-chrome-extension-caught- 191006900.html, 2018.

[10] Charles McFarland ,Tim Hux ,Eric Wuehler , Sean Campbell, BlockchainThreat report, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-Blockchain-,2018.

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

[12] M. Banerjee, J. Lee, and K.K.R. Choo, A Blockchain future for the internet of things security: a position paper. Digital Communications and Networks, vol.4, no. 3,pp.149-160, 2018.

[13] P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi,and K.K.R. Choo, A systematic literature review of Blockchain cyber security. Digital Communications andNetworks, 2019.

[14] Khan, M.A. and Salah, K., IoTsecurity: Review, Blockchain solutions, and open challenges. Future Generation Computer Systems, Vol.82,pp.395-411, 2018.

[15] M.A.Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras,and H. Janicke, Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet of Things Journal, vol.6, pp.2188-2204, 2019.

[16] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, A Survey on Long-Range Attacks for Proof of Stake Protocols. IEEE Access, vol.7, pp.28712-28725, 2019.

[17] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, Security services using Blockchains: A state of the art survey. IEEE Communications Surveys &Tutorials, vol.21,no.1,pp.858-880, 2018.

[18] S. Yaji, K. Bangera, and B. Neelima, Privacy Preserving in Blockchain Based on Partial Homomorphic Encryption System for Ai Applications. In 2018 IEEE 25th International Conference on High-Performance Computing Workshops (CW) IEEE, pp. 81- 85, 2018, December.

[19] Y. Toor, P. Muhlethaler, and A. Laouiti, “Vehicle ad hoc networks: applications and related technical issues,” IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp.74-88, 2008.

[20] A.E. Yves-Christian, B. Hammi, A. Serhrouchni, and H. Labiod, Total Eclipse: How To Completely Isolate a Bitcoin Peer. In 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC) , IEEE, pp. 1-7, 2018, October.

[21] Matteo Signorini, and Matteo Pontecorvo, Wael Kanoun, Roberto Di PietroBAD: a Blockchain Anomaly Detection solution,arXiv:1807.03833v2[cs.CR], Jul2018.

[22] Siye Wang, Shaoyi Zhu, Yanfang Zhang , Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems, IEEE Symposium on Computers and Communications(ISCC), pp.00074-00077,2018.

[23] A. Bhardwaj, V. Avasthi, H. Sastry,and G.V.B. Subrahmanyam, G.V.B., Ransomware digital extortion: a rising new age threat. Indian Journal of Science and Technology, vol.9, no.14,pp.1-52016, 2016.

[24] https://www.investopedia.com/terms/1/51-attack.asp.

[25] Fawkes,“PirlGuard—Innovative Solution against 51% Attacks”, available [online], https://medium.com/pirl/pirlguard-innovative-solution-against-51-attacks-7dd45aa1109, 2018.

[26] David.Mories, ”51% attack Are growing a threat to smaller Blockchain; Komodo my be the solution”, Available online, https://breakermag.com/komodo-says-it-has-answers-to-some-of-Blockchains-biggest-problems-and-its-pushing-to-grow/, 2019.

[27] S. Solat,. and M. Potop-Butucaru, Zero blocks: Timestamp-free prevention of block-withholding attack in Bitcoin. arXiv preprintarXiv:1605.02435, 2016.

[28] Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar. “Optimal selfish mining strategies in Bitcoin.” arXiv preprint arXiv:1507.06183, pp.515-432, 2016.

[29] J. Williamson, Bits or paper: Which should get to carry your vote?. Journal of information security and applications, vol.38, pp.124-131, 2018.

[30] Kyung Kim , “Analysis of Spam Transaction on the Blockchain”,International Journal of Engineering and Technology, vol,7, no,3.34, pp. 551-553, 2018.

[31] M.A. Uddin, A. Stranieri,I. Gondal, and V. Balasubramanian, Continuous patient monitoring with a patient-centric agent: A block architecture. IEEE Access, vol.6, pp.32700-32726, 2018.

[32] P.K. Sharma, S. Singh, Y.S. Jeong, and J.H. Park, Distblocknet: A distributed Blockchains-based secure Sdn architecture for IoT networks. IEEE Communications Magazine, vol.55, no.9,pp.78-85, 2017.

[33] K. Alachkar,and D. Gaastra, Blockchain-based Sybil Attack Mitigation: A Case Study of the I2PNetwork, 2018.

[34] LunLi, Jiqiang Liu, Lichen Cheng, ShuoQiu, Wei Wang, Xiangliang Zhang, and Zhonghua Zhang,CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles IEEE Transactions on IntelligentTransportation Systems, vol. 19, no. 7, 2018, July.

[35] G.Liang, S.R.Weller, F.Luo, J.Zhao, and Z.Y. Dong, “Distributed Blockchain-Based data Protection Framework for Modern Power Systems against cyber attacks”, IEEE Trans. Smart Gird, vol.10, no.3, pp.3162-3173, , 2018.

[36] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, X. Du, Achieving efficient detection against false data injection attacks in smart grid, IEEE Access, vol.5 , pp.13787–13798, 2017.

[37] M. Brengel, and C. Rossow, Identifying key leakage of Bitcoin users. In International Symposium on Research in Attacks, Intrusions, and Defenses Springer,Cham, pp. 623-643, 2018, September.