International Journal of Research in Advent Technology, Vol. 7, No. 1, January 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Review on Blockchain Security Attacks

Dr. P. S. Gawande
Associate Professor, Rajarshi Shahu College of Engineering, Buldana, India

Abstract— Blockchain technology is being used in many different industries to increase security and privacy because it is a distributed ledger that cannot be altered. It details the Bitcoin cryptocurrency and its transactions, which have attracted a lot of interest from a variety of sectors. While blockchain technology does have many great features, it is also susceptible to attacks such as Denial of Service, Double Spending, and others. This study provides a comprehensive literature analysis on several blockchain attacks, including their execution, proposed detection, mitigation, and avoidance strategies, and their respective strengths and limitations. Even though no security measure has yet been suggested that might actually protect blockchain against cyberattacks, there is currently no way to identify attacks like the 51% attack until it is completely deployed.

Index Terms— blockchain technology, security attacks, denial of service, blockchain security, taxonomy of attack

I. Introduction

Blockchain technology offers numerous chances for diverse infrastructure and has enormous promise for a wide range of applications. Resource management is encouraged by technology, which also facilitates efficient and safe communication. When parties use Blockchain for financial transactions, there is less opportunity for fraud and an automatic record of transactions is created, which increases trust. establishing an automated background investigation for each user in the system. Blockchain's decentralized characteristics provide dependability and lower the risk involved with doing business with unknown parties. Nowadays, everyone uses the internet to communicate with one another through sophisticated technology. Over the internet, texts, images, voice calls, and video calls are sent straight from sender to recipient. Between the sender and the recipient, there needs to be a reliable third party for this transaction. In the old system, individuals must rely on a third party to conduct financial transactions. However, in the case of blockchain, it will provide absolute transaction security. Every transaction should be recorded in a block; it will function as a record book. A block is added to the blockchain as a permanent database after a transaction is finished. A new block is generated or added with this when a block is finished. A hash of the previous block is carried by each block [1].

Blockchain technology consists of six key elements.
Decentralization: is one of the best aspects of blockchain technology; it eliminates the power of central nodes by allowing nodes to work together and use various consensus methods to participate in decision-making.
Transparency: Every time a new block is added and confirmed, the distributed ledger known as blockchain is updated. This gives the blockchain transparency because everyone on the network can view the ledger whenever they'd like.
Anonymity: With blockchain, a user's generated wallet address is used to complete transactions, and their identity is hidden. Complete anonymity is ensured by using several addresses.
Immutable: Every node in the network stores a copy of the ledger, making it unchangeable barring a situation in which someone takes over 51% of the network at once.
Open source: Since blockchain is open source, anyone can develop any kind of application. The ledger is accessible to the whole public and can be viewed by any network user.
Autonomy: Since the transactions are consensus-based, data may be transferred and updated reliably across all devices.

II. Types of Blockchain Security

A comprehensive risk management solution for blockchain networks, blockchain security includes cybersecurity frameworks, assurance services, and best practices to lower the likelihood of fraud and cyberattacks. Let's examine the many forms of blockchain security:

A. *Public blockchains*

All operations, or transactions, that take place on public blockchains, often referred to as permissionless blockchains, are entirely transparent, and contributors' identities remain anonymous. Since the software code is publicly available, anyone can take part in the central operations of the blockchain network. Since public block chains are entirely decentralized, there are no limitations on who can access or audit the data they contain. Furthermore, the public network is unchangeable, which increases its security and imperviousness to fraud. Public blockchains contain popular cryptocurrency names like Ethereum and Bitcoin.

B. *Private blockchains*

The centralized nature of private networks, commonly referred to as permissioned blockchains, differs from that of

doi: 10.32622/ijrat.752019127

public blockchains. Only individuals who have been granted permission to join the private blockchain network are able to observe and interact with this network. The network is incredibly secret since the administrator establishes rules governing who is allowed to participate and who is not. Modifications to the network, such as transactions, full node operations, and change validation, are restricted to those with access. Among the companies using private blockchain services are R3, IBM, and Corda.

C. *Hybrid blockchain*

A hybrid blockchain combines elements of both public and private blockchains; although some parts of the system are accessible to everyone, others require authorization and permission to use. For businesses that like to keep some information private—such as private customer information in banks or the healthcare industry—while keeping other information accessible to the general public, this is highly practical. This kind of blockchain keeps security and transparency while offering a great degree of customization.

D. *Consortium blockchain*

Several organizations, as opposed to simply one, are in charge of managing the network in the Consortium blockchain. This kind of blockchain likewise combines permissioned and permissionless blockchain; however, consortium blockchain differs from hybrid blockchain in that it allows several organizations to operate together on a decentralized network, increasing its security.

III. CLASSIFICATION OF ATTACK IN BLOCKCHAIN

There are six distinct types of blockchain security services [2]: non-reputation, authentication, data confidentiality, data provenance, data integrity, and data privacy. Distributed denial of service (DDoS) attacks, collision attacks, sybil attacks, eclipse attacks, injection attacks, replay attacks, and ransomware attacks are all powerful enough to compromise these systems.

This section surveys some of the primary weaknesses in Blockchain systems, as well as the security risks associated with them and the suggested remedies. The Blockchain attack classification is derived and shown in Fig 1.

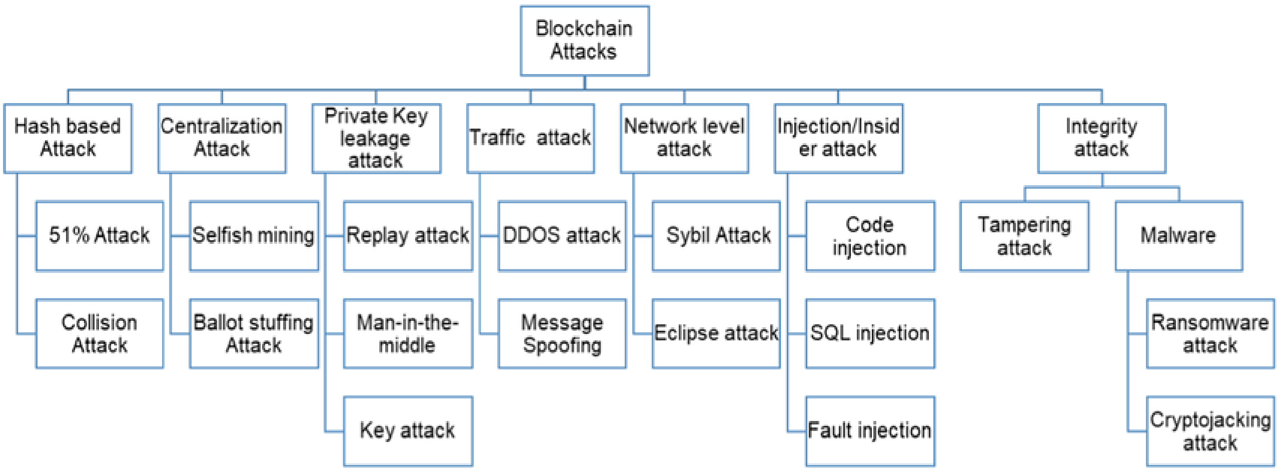

Figure 1: Classification of Blockchain Attacks

A. *Hash-based attack*

In order to carry out this attack, one must take control of hash values and attempt to determine which hash value corresponds to each sent message. Using this technique, the attacker gains control over more than 51% of the network's mining power or hash value.

a) 51% percentage attack: A 51% attack on a blockchain happens when one miner or a group of miners controls more than 50% of the network's mining computers or hash. Attackers can revers transactions on a blockchain and obstruct the process of storing new blocks by using a 51% assault. These transactions are ignored during execution because they are added to the pool of unconfirmed transactions. Even in cases where mining power is less than 40%, such as in Ghash.io, Krypton and shift, and Bitcoin Gold, a 51% attack is still feasible [11], albeit less likely. This vulnerability allows an attacker to take advantage of the following attacks: double spending, selfish mining, random forks, and cancellation of all transactions.

Researchers have attempted to use the Ethereum-based PirGuard Protocol to lessen [12] the 51% attack. Komodo's delayed proof of work [13] provides a way to stop attackers from altering or erasing transaction records. This attack can be thwarted with the adoption of the distributed trust paradigm for IoT. Because they can add a new block more quickly than a genuine miner and have greater processing capacity, attack miners in the 51 percent work flow build extended chains. The attacker's newly produced block will be added to the network's lengthy chain.

2) Collusion attack: A collusion attacker use a hash value that is identical to the data being carried over the network to obtain an advantage through infiltration. Goldwasser-Micalli and Pilliar encryption techniques were employed in [4] to limit collision attacks and to create encryption blocks for artificial intelligence applications. Both encryption

doi: 10.32622/ijrat.752019127

techniques are very economical and need less processing time because they don't produce a hash value.

B. Centralization attack

Since the Blockchain is a decentralized network, peer-to-peer communication takes place there. Here, the attacker attempts to undermine decentralization while fabricating the appearance of centralization.

1) Selfish Mining: By keeping a legitimate block for themselves, the evil miner can broadcast their hidden block into the network. To counter this, the Zero Block method [14] uses a novel timestamp-free strategy. There is a hard cap on how quickly the network can generate and receive blocks under this approach. If one miner keeps a block private for too long, the other honest miners will reject it. A few extended selfish mining approaches and the Nash equilibrium [15] model have been proposed to determine the optimal action for selfish miners.

2) Ballot stuffing attack: The electronic vote attack The act of casting more votes than is permitted, often known as "ballot stuffing" or "ballot box stuffing," is an assault on electoral integrity. Because the electronic voting mechanism is entirely anonymous [16], it is challenging to verify a person's identity across the board.

Ballot box integrity issues arise with both paper and electronic ballots in instances where universal verifiability allows anybody to verify that the votes inside the boxes are counted accurately. If the voting day is set as a national holiday, this attack may be prevented. The voting system uses the Zcash protocol [17], which provides voter transaction anonymity. In order to prevent ballot stuffing attacks, a decentralized trust management mechanism is built in a vehicle network. As a result, the suggested approach effectively and adaptably stores the trust values. Transaction commit time is shortened by an obligation chain [18] with an integrated reputation system.

C. Traffic attack

An enemy node attempting to cause congestion on the network in an attempt to jam it and deny service to authorized users is called a traffic attack.

1) DDoS attack: When several systems overwhelm the targeted system's resources and bandwidth, a distributed denial of service assault occurs. Because of the system overload, the target node is not allowed to complete the transaction. Using security switches, the security model [18] that incorporates several Blockchain technologies aids in separating out unauthorized traffic. Security switches determine the normalcy or abnormality of the node. The Blockchain is not involved in the addition of normal nodes to the list of legal nodes and abnormal nodes to the list of illegal nodes. This security model prevents spam transactions by detecting attacks against them.

In order to provide effective and adaptable DDoS mitigation solutions across many domains, a unique architecture [19] has been developed. The Patient-Centric Agent (PCA) component was introduced by recent research by [20] and prevents any fraudulent traffic from entering the network. This mitigation is often utilized in the healthcare industry and is helpful in preventing DDOS attacks on SDP devices. DDoS/DoS attack and security thread detection are capabilities of the DistBlockNet model for IoT [21] design. It guarantees low-performance overhead and will therefore meet the design principles of the Internet of things in the future. Blockchain provides DDoS attack mitigation in conjunction with network and cloud monitoring [c].

The following are the DDoS attack mitigation solutions for blockchain:

- Domain Name System (DNS) Operations on Blockchain.
- Using the blockchain and Ethereum.
- Tools for monitoring networks and preventing distributed denial of service attacks.
- The application of SDN and NV on blockchain technology.

2) Message spoofing attack: To stop the message recipient from launching this attack, a rating generating mechanism based on Bayesian inference [4] has been implemented. The message recipient evaluates the broadcast messages from different cars and determines which ones are reliable. Based on the rating that the message recipient generates, trust values are aggregated in the Road Side Unit (RSU). RSU and blockchain collaborate to keep a dependable and consistent database. Through a spoofing attack, an attacker can alter the identity of the data owner. It is impossible for an attacker to insert the incorrect source or destination address in tier-based end-end architecture [20].

D. Network level attack

An unauthorized user breaches network security by using user accounts and privileges illegally or by stealing hardware and software.

1) Sybil attack: In order to take over several nodes in the network, adversaries create confusion by putting up nodes with false identities. Consequently, the network design causes VANET to have extremely high bandwidth use [5]. A protocol for eco-announcements with a threshold authentication method was introduced in [22] to ensure Sybil resistance using signatures generated by a specified number of unique private keys. Furthermore, countermeasures to the Sybil assault have been proposed, both proactively and reactively [23]. Consequently, it provides consistent network infrastructure and scalable implementation.

2) Eclipse attack: An eclipse attack uses information blocking to cut off contact with the regular node. A method for implementing a total eclipse attack, which monopolizes all of the peer's connections, has been proposed in [20]. Based on IP address, the Bitcoin client separates two categories of methods: tested blocks and fresh buckets. The list of all peers and the unestablished outbound connection in the Bitcoin client are both contained in the new bucket. The list of IP addresses that have previously been connected to by

doi: 10.32622/ijrat.752019127

a client makes up the tried block. The attacker is unable to execute the eclipse attack as a result.

E. Injection or Insider attack

An unauthorized user gains access to the network or computer system and feeds dubious data to a program that an interpreter processes. A person with extensive system expertise and administrative access manipulates the data and creates a special challenge. This is referred to as an insider attack, in which a perpetrator with administrative access can change login credentials and data to remove any evidence of the attack and make it more difficult to identify the insider attack.

1) Code Injection attack: The web application's vulnerabilities are exploited by an attacker, who injects code to alter the execution path. Blockchain anomaly detection [8] can withstand the addition of a malicious user's transaction to a Blockchain, which could introduce harmful code into the system.

2) SQL Injection attack: In order to launch more attacks, an attacker deceives the server into executing fraudulent SQL queries, which delete, alter, or steal sensitive data from the database. SQL injection attacks are prevented via a unique Blockchain-based mutual authentication system that was presented in RIFD (Radio Frequency Identification) [8]. As a result, security features and security correctness proof have produced RFID systems with high security, less real-time requirements, and the ability to withstand several attacks.

3) Fault Injection attack: By delivering false data to the device, this attack seeks to alter the way software is executed. Modern power systems have proposed a distributed protection framework [24] that makes use of Blockchain security features. Meter nodes have been regarded as a private Blockchain network under this paradigm. Each node uses a consensus process to confirm the accuracy of the data it has received. Because of this threat, IoT apps frequently offer incorrect services or have poor network stability. In Internet of Things applications, an authentication technique has been proposed by [25] to protect the network from bogus data injection attacks.

F. Integrity attack

The Merkle tree ensures that every Blockchain data is authentic. Once an attacker tries to change the data within the block, it becomes impossible to restore the original data because of the integrity violation. Potential dangers include deliberate data manipulation and data updates that do not involve all stakeholders.

1) Tampering attack: Bitcoin (Credit) [22] notifies, and transactions cannot be altered without authorization. By recalculating the hash, the hash property ensures that transactions cannot be tampered with when a block is updated. An attacker can't tamper with the Blockchain because of its hash properties. So, if an attacker alters the block's content, the hash value must be computed for every block. Blockchains that are longer in duration prevent this kind of attack.

2) Malware attack: Malicious software is designed to stealthily mine bitcoin by utilizing a computer's computing power. The entire network and consumer devices are affected by unauthorized bitcoin miners. These threats are less noticeable and more subtle, but they might trick you into thinking you're safe.

• *Ransomware attack:* By injecting ransomware, an attacker limits the authorized user's ability to access data within their own network. since of this attack, the victim cannot access the files since malicious software has infected and encrypted the network.
An anti-malware deduction mechanism [10] has been suggested as a way to lessen the impact of ransomware. The services for malware behavioral analysis, malware code analysis, and malware reports are provided by Malware Detection as a Service (MDaaS). Malware can therefore be quickly identified and eliminated.

• *Cryptojacking attack:* Malicious cryptojacking has been analyzed both statically and dynamically by Saad et al. [5]. A content cryptocurrency-based analysis detects cryptojacking attacks between currencies and mining processes in static based analysis. Cryptojacking script in JavaScript code can be distinguished by its distinct code complexity. The dynamic based analysis examines how crypto jacking affects system resources, including CPU and battery life.

G. Private key leakage attack

When the same key and nonce are used more than once, an attacker may be able to extract the keys from memory or exploit duplicate values [26] to reveal secret keys and nonces.

1) Man in the middle attack: By ensuring that devices in separate segments use the same key for every session, tier-based end-end architecture [20] protects against man-in-the-middle attacks. According to [34], 802.11p and SSL-based VANETs make the classic man-in-the-middle attack impossible. In the event that an attacker alters the address or coin value during the consensus phase, the recipient will refuse the transaction.

2) Key attack: Devices in separate segments share a single session key in tier-based end-end architecture [20], which prevents man-in-the-middle attacks. With 802.11p and SSL-based VANETs, the conventional man-in-the-middle attack is not possible [34]. Transactions will be rejected by the receiver during the consensus phase if the address or coin value is changed by an attacker.

3)Replay attack: Using a nonce (Ns) and system time (Times), the lightweight authentication protocol [20] prevents a replay attack. The event's message is accompanied by a time description [22]. The receivers of the Announcement-Aggregated Packet (AGP) check the event time in addition to the current time. The adversary will be helpless to counter the attack if there are discrepancies.

doi: 10.32622/ijrat.752019127

IV. Challenges

Scalability: The blockchain network's scalability issue has come to light following the enormous success of Bitcoin. Prefixing the block size and block formation time for a set number of transaction processing makes it effective against the various threats listed above. However, processing of transactions may become slower when there are a lot of them. Scaling problems plague many blockchain applications. For example, Bitcoin's block size is limited to 1MB, and its average block confirmation time is 10 minutes. In contrast, Ethereum's block confirmation time is only 15 seconds. The block confirmation time must be short for a large transaction processing volume, but it must be high on average to provide security against attacker attacks. Basically, the idea of scalability encompasses the core problem that blockchain is experiencing. triage situation The statement that it is impossible to equally maximize the three desirable attributes—decentralization, scalability, and security—was first used by Ethereum founder Vitalik Buterin. According to the trilemma, the third can be sacrificed in order to maximize any two. Furthermore, because blockchains based on PoW consensus, like bitcoin, require a lot of processing power, they use more electricity. The authors of [14] have brought up the current remedy for the scalability problem.

Storage Management: The blockchain ledger is dispersed among all network nodes in order to enhance security. From the genesis block to the most recent block to be mined, the ledger includes every block in the chain. Because of this redundancy, a large amount of space is required. The size of the Bitcoin blockchain is currently about 16.5 GB and is growing at a rate of about 1 MB every hour. Over a million nodes running Bitcoin have taken up around 1.5736 Petabytes of space.

Lack of governance and regulation: Since blockchain networks are decentralized, no outside party is involved in approving transactions in permissionless blockchain networks. Millions of dollars have been lost by numerous people due to various problems. Standardizing the blockchain network is necessary for its viability, governance, and other aspects.

V. Discussion

The security of blockchain technology is discussed in this study. We can infer from this review article that there are security concerns with blockchain technology. The transactions ought to be impacted by these security flaws as well. This technology has the potential to be attacked in a variety of ways, and it provides some answers to these problems. Three primary categories of blockchain networks exist. public, private, and cooperative. This review article solely focuses on blockchain technology, both public and private. provides a brief analysis of these using a table of comparisons. Blockchain technology is becoming more and more popular. This technology is used in the development of numerous applications. This review paper provides possible solutions for current blockchain problems.

VI. Conclusion

The taxonomy of security risks to Blockchain systems is presented in this study. A detailed presentation is made of the Blockchain assault and the methods used to counter it. It offers a thorough analysis of blockchain system attacks and defenses. The final section presents the research directions and problems. The final section of this presentation addresses the problems for future blockchain research. Future work should focus on developing research methods, algorithms, and study fields, as well as enhancing algorithm performance.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Iuon-Chang Lin and Tzu-Chun Liao,” A Survey of Blockchain Security Issues and Challenges,” International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] A. Bhardwaj, V. Avasthi, H. Sastry,and G.V.B. Subrahmanyam, G.V.B., Ransomware digital extortion:

doi: 10.32622/ijrat.752019127

a rising new age threat. Indian Journal of Science and Technology, vol.9, no.14, pp.1-52016, 2016.

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

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

[13] 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.

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

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

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

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

[18] 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

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

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

[26] 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.

doi: 10.32622/ijrat.752019127