An Overview of the Security of Blockchain

Sree Preetha .K.R[1], Jaswanth .R[2], Dhanush Kumar .K[3], Keshore .S.M[4]

[1]Professor, Dept. of Computer Science Engineering, KPRIET, Tamil Nadu, India
[2,3,4]Student, Dept. of Computer Science Engineering, KPRIET, Tamil Nadu, India

Abstract - *The Blockchain is one of the most developing internet technologies in recent years through its introduction by Bitcoin and, it is also the most sought-after technology cause of the integrity, anonymity and security, it provides to the things that have value. Blockchain technology redefines how data are stored and distributed securely with cryptography and consensus mechanism in a distributed manner. Thus eliminating the need for having trust in a central authority. The data is made tamper-proof, secured by using an asymmetric encryption algorithm, hashing, and consensus algorithm. Because of this property, it is implemented in various domains such as medical, financial, supply chain management, etc. As the Block chain evolves the security of the Block chain must be evaluated comprehensively. This paper, discusses an overview of the Blockchain, its security drawbacks and, how these drawbacks are exploited.*

Key Words: **Blockchain Security, Privacy, Data Privacy, Blockchain, IPFS.**

I. Introduction

The Blockchain is still an emerging technology and people are still trying to grasp the full potential of it in various fields. Blockchain was first developed as an underlying framework for bitcoin when Satoshi Nakamoto released bitcoin white paper in 2008[5]. Since then bitcoin attracted many private financial institutions and organizations due to the anonymity and security it offers. The level of security and anonymity the bitcoin offers is possible only by its underlying framework Blockchain [4]. At its core, Blockchain is a digital decentralized ledger of financial transactions which is incorruptible. Blockchain was further developed with the introduction of Smart contracts in Ethereum Blockchain by VitalikButerin. Ethereum Blockchain can be programmed to store not only financial transactions but anything data of value [10]. As Blockchain continues to evolve in various domains, it is must to evaluate the security comprehensively.

II. Blockchain technology overview

The blockchain is not a single system but a combination of various technologies such as distributed technology, peer to peer communication, and cryptography working together. This section covers important components of Blockchain.

(i) Node and the Network

A node is a device on a blockchain network, that is, in essence, the foundation of the technology [5]. Nodes are distributed across a wide network and carry out a variety of tasks. A node can be an active electronic device, including a computer, phone as long as it is connected to the Blockchain. Nodes are the individual parts of the larger data structure that is a blockchain. The Blockchain network is a decentralized peer to peer network which consists of nodes. There are two types of node presented in the network [10] namely, Full node and Light node.

Full Node fully enforces the rules of Blockchain and has a copy of all the historical data of the Blockchain in it.

Light Node references trusted full node's copy of the Blockchain.

(ii) Ledger

Ledger is a database structure where data are stored securely. The ledger database is spread across several nodes (devices) on a peer-to-peer network, where each replicates and saves an identical copy of the ledger and updates itself independently [5], [10]. The primary advantage is there is no need for central authority. Once the information is stored, it becomes an immutable database, which the rules of the network govern. While centralized ledgers are prone to cyber-attack, distributed ledgers are inherently harder to attack because all the distributed copies need to be attacked simultaneously for an attack to be successful. Further, these records are resistant to malicious changes by a single party.

(iii) Consensus Protocol

These protocols create an irrefutable system of agreement between various devices across a distributed network, whilst preventing exploitation of the system. Blockchain consensus protocols keep all the nodes on a network synchronized with each other [6]. Consensus rules are a specific set of rules that nodes on the network will ensure a block follows when validating that block and the transactions within it. The key requirement to achieve a consensus is a unanimous acceptance between nodes on the network for a single data value, even in the event of some of the nodes failing or being unreliable. Consensus protocols also provide participants on the network who are maintaining a blockchain with rewards and incentives to continue doing so. These rewards come in the form of crypto currencies or tokens, which can be extremely lucrative, so much so that competition to confirm the next block in a chain is extremely fierce. Some of the most used consensus protocols are, proof of work and proof of stake.

1. Proof of work

Proof of work consensus protocol was devised by Satoshi Nakamoto in the Bitcoin white paper and is now widely used in many other cryptocurrencies. This process is known as mining and as such the nodes on the network are known as "miners". The "proof of work" comes in the form of an answer to a mathematical problem, one that requires considerable work to arrive at, but is easily verified to be correct once the answer has been reached [6]. The answer is in the form of a target hash that miners must produce with the current block for it to be confirmed into the blockchain and, the miners must perform a trial and error basis to get to the target hash. Technically, the target hash can be found at first attempt but it is highly unlikely.

This process involves rewarding cryptocurrencies for the miners who get the target hash and, this reward acts as an incentive for the miners to produce the target hash as the process involves wasting lots of computing power and electricity.

2. Proof of Stake

In proof of stake system, the creator of the next block is determined by a randomized system that is, in part, dictated by how much of that cryptocurrency a user is holding or, in some cases, how long they have been holding that particular currency [11]. Instead of computational power, as is the case in proof of work, the probability of creating a block and receiving the associated rewards is proportional to a user's holding of the underlining token or cryptocurrency on the network [3]. The randomization in proof of stake system prevents centralization, otherwise the richest individual in the system would always be creating the next block and consistently increasing their wealth and as a result their control of the system.

The main advantage of this system than proof of work is it doesn't waste much energy in confirming the block so it is cost effective. It is superior to proof of work system as it uses less electricity to run.

Delegated proof of stake (DPOS). Similar to POS[3], miners get their priority to generate the blocks according to their stake.

III. Security Risks in Blockchain

In the wake of Bitcoin's rise, blockchain is being adopted in many other industries, to securely deliver data in a series of encrypted transmissions that are extremely difficult to trace. But, Blockchain technology is not completely secured as there are some exploits and risks present in the Blockchain are explained in the below section.

(i) 51% Vulnerability

The consensus mechanism Proof Of Work has a big vulnerability in it that can be exploited, if a single miner or group of miner gets hold of more than 50% of computing power in the Blockchain then the miner has control over the Blockchain [8]. When a miner forms a valid block of transactions, the individual will normally broadcast the block to the rest of the miners on the network, so that other miners can verify its validity, which allows for consensus as to the shared state of the blockchain to be reached. However, a bad actor with more than 50% of a network's computing power could begin mining privately. The transactions included in these privately mined blocks are not broadcasted to the rest of the network. This results in a scenario in which the public version of the blockchain is being followed by the rest of the network, but the bad actor is working on his own version of the blockchain and not broadcasting it to the rest of the network.

When a malicious miner gets hold of more than 50% computing power of the Blockchain than the miner can do the following attacks,

i. Initiate double spending attacks [8].
ii. Change or modify the order of transactions.
iii. Restrict normal mining operations of other miners.
iv. Obstruct the confirmation of other transactions and blocks

The 51% attack would be in vain for the attackers as it would require significant expenditure and little financial returns. The attacker should spend more computing resource than half of the entire blockchain network and the result the miner will get from performing the attack will be unprofitable when compared to the resource the miner spent. The 51% vulnerability is not present in the Proof of Stake consensus protocol so it is much secured than Proof of Work protocol and some major blockchain system are currently in the transition of their consensus protocol from Proof of Work to Proof of Stake.

(ii) Private Key Security

Blockchain uses public/private key cryptography to generate the signature for a transaction and verification [1]. The private key is also used to managing assets in the wallet by the node participating in the network. Managing public/private key in the blockchain in a very important security measure but by default blockchain doesn't provide any security protocol to manage the keys so it is user's responsibility to secure it.

Once the user's private key is lost, it will not be able to be recovered. If the private key is stolen by criminals, the user's blockchain account will face the risk of being tampered by others. Since the blockchain is not dependent on any centralized third-party trusted institutions, if the user's private key is stolen, it is difficult to track the criminal's behaviors and recover the modified blockchain information.

Key generation method selection is also important. Depending on the blockchain, the hash and cryptographic key generation may vary. If unsafe or easy to crack methods are used to create a key in particular Blockchain implementation, the private keys of nodes could be possibly stolen.

Due to decentralized, distributed, and definite nature of the Blockchain, the rule of the Blockchain says that the transaction that has occurred and has been already approved cannot be deleted from the Blockchain forever (whatever happened, happened). Additionally, there is no Certification Authority (CA) or any other "golden source of information" present in the Blockchain system (note, this is applicable mostly for the public Blockchains). As a result, the end user has no reliable means to properly verify the credibility of other user's public key.

(iii) Untested Code

The blockchain is fresh and extremely fast developing the technology. Most of its code is actually open source and anyone in the world can contribute into the development of a number of major projects such as Bitcoin, Litecoin, etc[2]. As the blockchain technology is growing rapidly there may be still vulnerabilities left in the code even though many engineers must have tested it.

(iv) Scalability issues

As the blockchain continues to grow, it requires all the data to be stored in every node to secure it. It possesses a huge threat to the scalability of the technology. The growth of the blockchain ledger will become unmanageable for most of the users to participate in the network [2]. Also while Visa and MasterCard can verify thousands of transactions in a second, blockchain can only do a few. So these issues present a huge threat to the blockchain.

(v) Front end issues

The blockchain is just a backend technology and a front end user interface must be provided for the user to interact with it [2]. If the front-end used to interact with the Blockchain is faulty and its design lacks basic security countermeasures, the whole system could be compromised. In fact, so far nearly all documented incidents and successful attacks on the Blockchain technology where related solely to the faulty implementations of the frontend solutions.

IV. Security attacks on Blockchain

Blockchain brings major security enhancements with it when compared to traditional centralized systems. But Blockchains are maintained over a peer to peer to network and there are different attacks possible in it, likeDdoS, Sybil attack, routing an eclipse attack.

(i) Denial of service attack

The DDoS attack is a common attack to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic[6]. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.

Though Blockchain network is comparatively safer against the DDoS attack than a centralized network, it is still susceptible to it. In Blockchain the DDoS attack boils down into overloading the nodes in the Blockchain with packets consisting of valid transactions or junk packets. The nodes will get stuck processing these transactions and the network will be impacted. There are ways to limit the probability of success of DoS attacks but we cannot completely eliminate it.

(ii) Sybil Attack

One of the biggest issues when connecting to a peer-to-peer network is Sybil attacks [6]. A Sybil attack is one where the attacker pretends to be so many people at the same time. In Sybil attack, there is a malicious node that has been able to create so many identities in the network. Within the network, this malicious node looks like it is a large group of nodes representing a large percentage of the network. The other honest nodes that wish to connect to the network may not be able to detect such behavior and may accept shared information from this malicious node thinking the data is arriving from so many different sources.

Countermeasures such as Proof-of-Work (PoW) have been utilized by many cryptocurrencies to protect against Sybil attacks during mining. PoW requires each node that wishes to participate in the mining process to compete in an expensive crypto-puzzle. Now, creating multiple identities is still possible, but, providing the computational power to solve this puzzle then becomes the issue. So it doesn't completely eliminate the Sybil attack.

(iii) Eclipse Attack

Eclipse attacks are a type of network attack that aims at eclipsing certain nodes from the entire peer-to-peer network [6]. This simply means, monopolizing a node's connections so that it doesn't receive information from any nodes other than the attacking nodes. In contrast to Sybil attacks, Eclipse attacks are mainly focused on attacking single nodes rather the entire network at once.

An attacking node could easily perform a double spending attack in such a setting. This can easily be done by sending the victim node a transaction showing proof of payment, eclipsing it from the network, then finally sending another transaction to the entire network spending the same tokens again [12]. Given the fact that the victim node is isolated and only receives data from the malicious nodes, it will continue to believe the incorrect state of the blockchain.

The blockchain is resistant to Sybil attacks because of its proof of work concept[6] though in a worst-case scenario is when an honest node is being massively Sybil attacked but still has a single connection with an honest node that is connected to the true Bitcoin network. As long as a single honest node is passing the true data to the full node which is being attacked, it will ignore all the attempts from the Sybil attacker's nodes.

(iv) Routing Attacks

Routing attacks rely on intercepting messages propagating through the network and tampering with them before pushing them to their peers [6]. The only way for nodes to detect such tampering is when they receive a different copy of it from another node.Routing attacks are divided into two separate smaller attacks.

(i)Partitioning attack [12] where the attacker tries to split the network into two or more disjoint groups. This can be done by hijacking certain points within the network that act as the linking point between two groups.

(ii)Delay attack [12]: The attacker picks up the propagating messages, tampers with them and finally pushes them to the side of the network that has not seen it before.

There are valid methods to limit these attacks from occurring [13]. For example, by continuously diversifying the network connections, it will make an attacker's life much harder to find points to hijack and split the network into two or more disjoint groups. Another method is to monitor the network parameters such as Round-Trip Time (RTT) and recognize irregular patterns. Once detected, the nodes can simply disconnect themselves and try to connect to other random nodes.

V. Conclusion

The peer to peer system in which the blockchain works will never be secure but it definitely provides enhanced security over centralized systems. Without a doubt, there is a number of security threats applicable to the Blockchain. These threats must be noticed and remembered. Yet, most of them are already being resolved by the protocol design and software development side. For sure a standardized approach for the Blockchain security is needed and baseline framework and standards should be created by recognized organizations

References

[1] Fangfang Dai, Yue Shi, Nan Meng, Liang Wei, Zhiguo Ye, "From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues ", The 2017 4th International Conference on Systems and Informatics (ICSAI 2017), pp:975-978.

[2] Marek R. Ogiela, MichaMajcher, "Security of Distributed Ledger Solutions Based on Blockchain Technologies", 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications, pp:1089-1095.

[3] BitFury Group, "Proof of Stake versus Proof of Work white paper", [Online]. Available: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

[4] Liang Liu, BudongXu, "Research on Information Security Technology Based on Blockchain", 2018 the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis, pp:380-384.

[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Consulted, 2008.

[6] Mosakheil, Jamal Hayat, "Security Threats Classification in Blockchains" (2018). Culminating Projects in Information Assurance. Retrieved from URL:https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1093&context=msia_etds

[7] Deepak K. Tosh, Sachin Shetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, Laurent Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack", 2017 17th IEEE/ACM International

Symposium on Cluster, Cloud and Grid Computing, pp:458-462.

[8] Xiaoqi Li, Peng Jiang, Ting Chen, XiapuLuo, Qiaoyan Wen, “A Survey on the Security of Blockchain Systems”.

URL:https://www.researchgate.net/publication/319249505_A_Survey_on_the_Security_of_Blockchain_Systems/fulltext/5a8ce684458515a4068af02e/319249505_A_Survey_on_the_Security_of_Blockchain_Systems.pdf

[9] Zyskind, Guy, O. Nathan, “Decentralizing privacy: Using blockchain toprotect personal data,” Security and Privacy Workshops (SPW), IEEE,2015, pp: 180-184.

[10] Ethereum.org, “Ethereum White Paper,” 2014. [Online]. Available:

https://github.com/ethereum/wiki/wiki/White-Paper

[11] ZibinZheng, ShaoanXie, Hongning Dai, Xiangping Chen, and Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, 2017 IEEE 6th International Congress on Big Data, pp:557-563

[12] EhabZaghloul (2018), Blockchain Security Attacks Part 1—Network, Retrieved from https://medium.com/zkcapital/beginners-guide-on-blockchain-security-attacks-part-1-network-ca4e74435723

[13] Wang, F. (2015, October 4). Eclipse attacks on Bitcoin’s peer-to-peer network. Retrieved March 27, 2018, from https://medium.com/mit-security-seminar/eclipse-attacks-on-bitcoin-s
peer-to-peer-network-e0da797302c2.