International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 245-249
Published Online April 2020 in IJEAST (http://www.ijeast.com)

BLOCKCHAIN TECHNOLOGY: A REVIEW ON ARCHITECTURE, SECURITY ISSUES AND CHALLENGES

Priya Maidamwar
Department of CSE
G. H. Raisoni College of Engineering, Nagpur, India

Nekita Chavhan
Department of CSE
G. H. Raisoni College of Engineering, Nagpur, India

Abstract— **Data is one of the most significant resources. In this digital era, cyber security has become the worldwide issue. Since cyber criminals are getting progressively skilful in their attempts to destroy the valuable data, securing this data has become mandatory. Different procedures have been developed in the past to secure the data, but there are no bounds to security threats, resulting in theft of information from the devices. Currently Blockchain technology is the best tool to secure the data. Blockchain, originally known as Bitcoin, has become very popular technology to digitally create and manage transactions. It is a form of distributed public ledger which analyses and verifies transactions in decentralized manner and data is not under the control of any third party organization. This rapidly evolving technology can possibly change the opinion about digital transactions in various areas such as energy supply, peer-to-peer global payments, financial transactions, agriculture and industry. Regardless, this rising innovation is still in its beginning period of progression. Inspite of several opportunities offered by blockchain, it has limitations such as transaction cost, scalability, consistency security and administration issues which has not yet been addressed and investigated. In spite of the fact that there are a couple of studies on the security and privacy issues of the blockchain, they do not have an efficient assessment of the securing blockchain architectures. This paper presents a detailed architecture of blockchain technology along with systematic study of the security attacks rising in blockchain technology.**

Keywords— **Blockchain, Distributed, Decentralized, Scalability, Security Attacks**

I. INTRODUCTION

Block chains serves as digitally immutable database systems deployed in a distributed manner which is shared among every participating nodes within the network. In other words blockchain can avoid the single point of failure situation. This technology was first proposed in 2008 wherein electronic currencies were introduced. Here money is transferred electronically on a computer network in a distributed fashion. Other digital currencies like as Litecoin, Ripple, Bitcoin and Ethereum are examples of this technology. This technology is useful for wide range of applications.

Block chains are type of distributed digital ledgers where in all the transactions are cryptographically signed and grouped into blocks. After validation and undergoing a consensus decision, every block in the network is linked to the previous block. Whenever new block is added to the older one, it is not possible to modify older blocks. As new blocks are kept on adding, chain grows on continuously. Further across respective copies of the public database inside the network new blocks are replicated, and any conflicts among them are settled using established rules automatically [2].

Till now, lot of survey on blockchain has been done. It is available on different sources, for example website, Wikipedia, conference proceedings and journal papers. However, very little research has been presented on its network security. Subsequently, this paper describes layered architecture of blockchain technology in detail, explores several documents related to security requirements of blockchain, and analyzes the security issues of blockchain technology.

In this paper section 2 explains layered architecture of Blockchain. Section 3 introduces security threats in every layer of blockchains and summarizes major attacks. Section 4 presents challenges of blockchain technology. Finally, we briefly summarize the work of the full paper.

II. BLOCKCHAIN LAYERED ARCHITECTURE

This section covers the layered architecture of block chain. From top to bottom the block chain structure is divided into Application layer, Consensus layer, Network layer, Data layer and Hardware Layer.

A. Hardware/Infrastructure Layer

Blockchain is a distributed system of computers connected in a peer-to-peer manner that computes transactions, approves them, and stores them in shared database in an ordered structure. Every device within a blockchain network is called a node. The duty of nodes is to validate the transactions, organize them into blocks, and further broadcast them to the blockchain network. After verifying through consensus protocol, nodes submit the block to the blockchain network and update their database record. This layer consist of virtualization i.e. creation of virtual resources such as storage, network, servers etc. Fundamentally, nodes are the core of this layer. At the point when a device gets associated with a blockchain network, it is named and considered as a node. These nodes are decentralized and distributed on a blockchain network.

B. Data Layer

This section is concerned with the transactions which are arranged in blocks, and placed in a peer-to-peer network. The data structure of blockchain can be represented in the form of linked list, which are ordered. It consist of two primary components—pointers and a linked list. The pointers are the variables, whose value is the address of another variable, and linked list is a linear collection of blocks, where each block has data and pointers to the previous block. A hash tree or merkle tree is the one wherein each leaf node is marked with the cryptographic hash of the block of data, and each non-leaf node is a cryptographic hash of its child nodes. This data structure permits efficient and secure verification of the data. Hash trees, along with cryptography and consensus algorithms, are the central part of the blockchain technology.

C. Network Layer

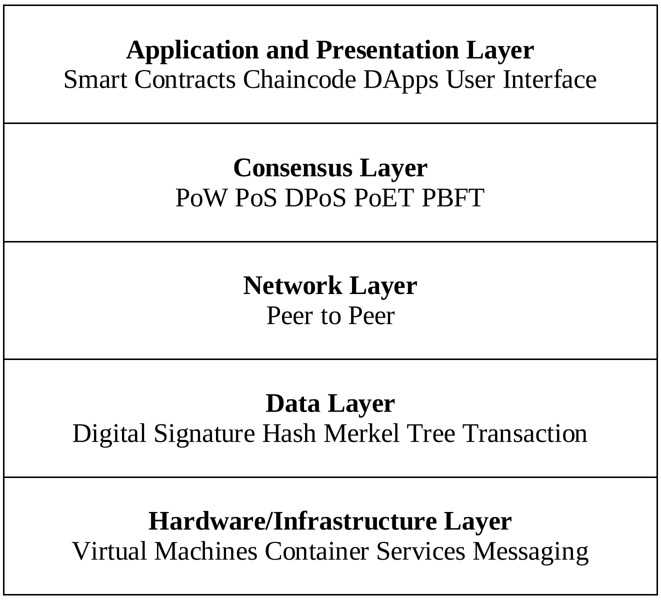
The network layer, is responsible for peer-to-peer communication between nodes. Its main functions are discovery of neighboring nodes and can communicate, making transactions, and propagating the block of transactions. A peer-to-peer network is a computer network where devices are distributed and share the network's workload to reach the goal. Nodes perform transactions on the blockchain. Nodes can be categorized as—full node and light node. Full nodes guarantees the verification and validation of transactions, mining, and the implementation of consensus rules. They are responsible for keeping trust in the network. The job of light nodes is only to keep the header of the blockchain (keys) and can make transactions [1].

D. Consensus Layer

The consensus layer is the very basic and important layer for any blockchain (Ethereum, Hyperledger, or any other). The consensus protocol ensures the stable working of blockchain technology. Behind every blockchain, there is a consensus algorithm. Consensus is responsible for validating the transactions, maintaining the order, and ensuring every block agrees on it. It ensures that power remains circulating and decentralized. No single node can control the whole blockchain network. The major goal of this protocol is to achieve reliability [7].

E. Application Layer

The application layer consists of Smart contracts, Chaincode, and DApps. This layer is further categorize: into two sub-layers –application layer and execution layer. Application layer involves the applications that are utilized by end clients to cooperate with the blockchain network. It consist of contents, APIs, UIs, frameworks. For these applications, blockchain network is the back-end framework and they frequently associate blockchain network by means of APIs. Another sublayer called as Execution Layer constitutes of smart contracts, predefined rules and chaincode. This sublayer has the genuine code that gets executed and rules that are executed. A transaction spreads from application layer to execution layer, however the transaction is approved and executed at the semantic layer (smart contracts and rules). Applications sends directions to execution layer, which carries out execution of transactions and ensure the deterministic nature of the blockchain [4].



Application and Presentation Layer
Smart Contracts Chaincode DApps User Interface

Consensus Layer
PoW PoS DPoS PoET PBFT

Network Layer
Peer to Peer

Data Layer
Digital Signature Hash Merkel Tree Transaction

Hardware/Infrastructure Layer
Virtual Machines Container Services Messaging

Fig. 1. Blockchain Layered Architecture

III. SECURITY ATTACKS ON EACH LAYER

With our layered blockchain architecture, different security threats appear at each layer. The summary of the major attacks and possible security approaches in different layers is described as follows.

At Hardware Layer, virtual machines are connected to each other in peer-to-peer manner. It manages transactions ordered in form of blocks. Threats like Malware and Rootkits, Physical Tampering, Supply chain Attacks occurs in this layer. Other threats of the this layer are associated with compromising privacy of information and user identities with defensive techniques like privacy-preserving cryptography methods, audit, formal verification, homomorphic encryption as well as usage of trusted hardware[9].

The primary function of network layer is neighboring node discovery and peer management, which depends on the factors of the network, such as routing protocols (e.g., IP for LAN, BGP for WAN) and domain name resolution (i.e., DNS). The attacks arising in this layer are man-in-the-middle attack, network decomposing, eclipse attack, Sybil attack, DDoS. Countermeasures include network authentication, security of available resources, anonymous routing, and data encryption.

At the consensus layer, presence of malicious nodes may modify the outcome of the consensus protocol by deviating from it. Additionally, if they are powerful enough, malicious nodes might take over the execution of the protocol or cause its disruption by violating assumptions of consensus protocols. The countermeasures includes strong consistency, well designed economic incentives, decentralization, and quick certainty solutions.

At the data layer transactions are performed between peer-to-peer nodes. It manages sequence of transactions, as per which the condition of blockchain is refreshed. The threats occurring at this layer are malicious information attack, cryptographic hack, collision attack, length extension attack, quantum and back door attack. The countermeasures includes privacy-preserving cryptography method and MD5 and SHA1 hash algorithms.

Table I: Layer wise Attacks and their Security approaches

Layer	Attacks	Security Approaches
Hardware/Infrastructure Layer	Malware and Rootkits Physical Tampering Supply chain Attacks	Formal Verification Audits Signature Scanning Homomorphic Encryption
Data Layer	Malicious Information Attack Cryptographic hack / Brute force attack Hash collision attack Length Extension attack Back door attack Quantum attack	Signature and Encryption Method SHA-1 and MD5 hash algorithms[12]
Network Layer	Man-in-the-Middle Attack Eclipse attack Sybil attack DDoS Double Spending Network Partitioning	Network authentication Encryption Algorithm
Consensus Layer	Protocol Deviation Violation of Assumptions Precomputing Attack Long-Range Attack Accumulation Attack	Economic Incentives Strong Consistency Decentralization Fast Finality
Application and Presentation Layer	Unauthorized Access Malicious Program Infection Tampering Attack Phishing attack Weak password attack Hash power forgery attack Selfish mining attack	Multifactor Authentication Application Level Privacy Reputation Approaches Preserving Constructs

At the application layer, threat agents are expansive and includes arbitrary internal or external intruders such as clients, malware, service providers, manufacturers of applications and services. The attacks on this layer can occur from false data injection, control by application-specific authorities (e.g., auctions, e-voting), front running attacks, disruption of the availability of centralized components, compromising application-level privacy, misbehaving of the token issuer, misbehaving of manufacturer or permanent hardware (HW) faults. Examples of mitigation techniques are multi-factor authentication, HW wallets with displays for signing transactions, redundancy/distributions of some centralized components, reputation systems, and privacy preserving-constructs as part of the applications themselves.

Blockchain technology is still in its primary stage of its development phase and securing it is far behind the needs of its development. The dangers may originate from internal or external intruders. The popularity this technology sets new expectations for security and protection of information storage, data transmission and sets new difficulties to existing security arrangements, verification systems, information insurance, security assurance and data guidelines. The details of major vulnerabilities, threats and its effect related to each layer of the stacked model is described in the following table.

Table II: Major attacks on Blockchain system

Attack Criteria	Attack Definition	Attack Effects
Double Spending Attack	A client tries to send two conflicting transactions in sequence i.e. it is ability of user to simultaneously spend the same assets in two separate transactions for a period of time [6].	• Blockchain network is disrupted • Cryptocurrency is essentially stolen. • Adversary would send a duplicate of the currency transaction to make it look genuine or might delete the transaction.
Finney Attack	It is a type of a double spending problem. Here attacker sends repeated transactions. Initially he spends some coins without broadcasting the transaction. Again he sends same coins in second transaction. In this way first transaction will become invalidate [3].	• Causes a successful double spending attack • Results in cancelled transaction.
Brute Force Attack	In this method attacker tries to obtain private user information by guessing possible combinations of password until it discovers the correct password.	• It is time consuming, difficult to guess the password if data is unclear, and sometimes it is impossible. • However, if the password is weak it could merely take seconds with hardly any effort.
> 50% hash power or Goldfinger Attack	When a miner or group of miners are able to take control of more than 50% of the hash power in Proof-of-Work, then the Gold finger attack may be launched[5].	• It prevents specific transactions or even reverse older transactions. • It destroys the stability of the entire network.
Block discarding or Selfish Mining	It occurs when group of miners stops releasing validated block into a network, thereby generating higher revenues [7] [11].	• It will damage the structure of blockchain. • Attacker will take control over the network and invalidate the transaction of the parties.
Fork after withholding (FAW) attack	It combines elements of block discarding and block withholding. The attacker holds onto the block privately without publishing it.	• Resources of individual miners are waste. • Pool revenue is decreased.
Precomputing Attack	It is a method of performing computation before run time. Intruder computes in advance which block is going to introduce inside the network by computing their hashes based on which attacker can alter the values of his own transaction.	• Intruder takes control over the entire chain. • It has ability to break weak passwords.
Long Range Attack	An attacker depending on its computational power can replace the main chain by creating his own blockchain from scratch. It is a kind of forking.	• It creates series of blocks. • Older nodes has ability to overtake the main chain as they have more coins to spend.
Accumulation Attack	An attacker desires to potentially take over the network by accumulating more currency.	• It results in deterioration of network transaction by accumulating more currencies.

IV. RESEARCH CHALLENGES

Even though, Blockchain technology has several advantages and potential to solve variety of problems in different areas, still there exists a challenge. These challenges can be in the form of overcoming the security and privacy issues. Following section briefly explains the upcoming research challenges.

A. Key Management

Key Management is a challenging issue for any cryptographic system. Private keys are used for verifying information from source node, which in case attacked by an intruder, will destroy all the data secured by these keys. Possibly encryption of messages across the distributed database can be done by using different private keys. If private key is lost by the user, then every information associated with it is lost.

B. Cryptography

Cryptographic approach is used in blockchain to validate the integrity of data. It manages public - private key pairs. This algorithm follows strict rules to generate strong keys as well as perform encryption and decryption of data

C. Privacy

Since Blockchain platform is distributed in nature, all the nodes in peer-to-peer network are able to access the shared database, which means they can extract the entire record of transactions, including non-member nodes of the network. This hampers privacy of data in the blockchain [5].

D. Storage capacity and Scalability

Due to the decentralized nature of the blockchain system, there is limitation on scalability of blockchain network. The core problem is the time taken to process a transactions in a block and rate at which block is validated through consensus protocol. Storage capacity of blockchain is growing continuously since its creation. Hence increasing the number of transactions doubles the number of cryptographic values inside those transactions. This increases transaction time and makes it bulky [8].

E. Throughput and Delay

The rate at which transactions are validated inside the blockchain network is called as throughput. Approximately 10 minutes are taken in blockchain network to create a block. In order to accomplish security requirements more time is spent in creation and validation of block to ensure that data within blocks is not accessed. Current blockchain platform needs to increase the efficiency in block generation and validation time in order to complete the transaction along with necessary security requirements [10].

V. CONCLUSION

Blockchain is the most innovative component which offers a decentralized mechanism for participants to agree upon data and computation. This paper describes in detail survey on blockchain technology. We initially present blockchain layered architecture consisting of five layers together with security threats in each layer. Next we have summarized some major attacks in blockchain along with its effects. Finally several research challenges are identified which have to be solved through continuous research.

VI. REFERENCES

[1] Homoliak I.,Venugopalan S., Hum Q., Reijsbergen D., Schumi R.,Szalachowski P (2019) The Security Reference Architecture for Block chains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses, arXiv.org.

[2] Tandon A. (2019).Challenges of Integrating Blockchain with Internet of Things, International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.8, Issue-9S3, pp1-14.

[3] Rathod N. and Motwani D. (2018) Security threats on Blockchain and its countermeasures, International Research Journal of Engineering and Technology (IRJET), pp 1-7.

[4] Wang H., Wang Y.,Cao Z., Li Z. and Xiong G. (2018) An Overview of Blockchain Security Analysis, Cyber Security, 15th International Conference, pp 55-72.

[5] Nallapaneni M., Mallick P. (2018) Blockchain technology for security issues and challenges in IoT ELSEVIER Procedia Computer Science pp 1-9.

[6] Ferrag M.,Derdour M., Mukherjee M., Derhab A, Maglaras L.,Janicke H (2018).Blockchain Technologies for the Internet of Things: Research Issues and Challenges IEEE pp 1-14.

[7] Zheng Z., Xie S., Dai H., Chen X., and Wang H. (2017).An Overview of Blockchain Technology: Architecture, Consensus and Future Trends IEEE 6th International Congress on Big Data pp 1-8.

[8] Kibet A. and Karume S. (2018) A Synopsis of Blockchain Technology" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) pp1-7.

[9] Maidamwar P., Chavan N., Yadav U. (2018) Internet of Things: A Review on Architecture, Security Threats and Countermeasures International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) Vol. 8, Issue 1 pp 1-10.

[10] Fernandez-Carames T. and Fraga-Lamas P (2018) A Review on use of Blockchain for the Internet of Things IEEE Access pp 1-23.

[11] Monrat A., Schelen O and Anderson K (2019) A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities IEEE Access pp 1-17.

[12] Jesus E., Chicarino V., Albuquerque C and Rocha A. (2018) A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack Journal of Security and Communication Networks pp 1-28.