Security vulnerabilities in Information communication technology: Blockchain to the rescue

(A survey on Blockchain Technology)

Himanshu Saini
Dept. of Computer Science and Engineering
HMRITM
New Delhi, India
saini56.himanshu@gmail.com

Bharat Bhushan
Dept. of Computer Science and Engineering
HMRITM
New Delhi, India
bharat_bhushan1989@gmail.com

Aman Arora
Dept. of Computer Science and Engineering
HMRITM
New Delhi, India
amanar98@gmail.com

Anureet Kaur
Dept. of Computer Science and Engineering
HMRITM
New Delhi, India
anureet021999@gmail.com

***Abstract*— With the increasing concerns about the security of data, Blockchain a decentralised public ledger, linked block structure which verifies and stores data and follows trusted consensus algorithms which ensure synchronisation of data in a distributed peer to peer network acquired a lot of attention as well as discussions recently. As it makes sure a tamper-proof digital platform for decision-making processes to store and share data among different individuals, authorities and organisations who do not trust each other. This technology is considered as the future of data security and integrity and is expected to serve in a lot of new or existing potential application, so the motive of this paper is to present insights of blockchain's architecture, it's security background, and it elaborate the two versions of blockchain: permissioned and permission-less. and some of its applications. Moreover, the first decentralized cryptocurrency and a public ledger named bitcoin are also elaborated in this paper. Furthermore, we summarize some typical implementations in blockchain, the lifecycle of bitcoin and explore future research challenges that still need to be addressed in order to preserve privacy when blockchain is used.**

Keywords— Blockchain, Consensus, Permissioned and Permissionless Blockchain, Bitcoin, PoW, PoS, PoB, Cryptocurrency.

I. INTRODUCTION

As the world is getting connected with time, a lot of data is being generated on a daily basis. The main concern is the security of this data. Researchers are coming up with the advancement of new technologies. Blockchain technology has been acquiring great flimflam lately. It is said to be the backbone of Digital Cryptocurrency BitCoin. Blockchain is a type of data structure which is a continuous growing link of transaction or record, these transactions or records could be interpreted by a block of transactions, which is securely linked with the help of cryptographic hash values in a decentralized manner.[1] Although this definition gives a very general overview of blockchain but this technology is much more complex. Blockchain is "accessible to all" *decentralized platform* where verifiable information is efficiently computed and shared amongst multiple authorities or anonymous users who do not trust each other in *decision-making processes.* It makes them work together using consensus protocols or set of instruction which ensures and maintains the integrity of the system or blockchain network. As blockchain is also considered as an immutable public ledger which has properties such as a protocol for commitment (which ensures that every valid data or transaction should be committed and included in the blockchain), Consensus among all nodes, Security (data needs to be tamper-proof or immutable because anyone in the network may act maliciously), Privacy and Authentication.[2,3].

Technology that was developed for serving major verification and authentication role behind bitcoin was Blockchain in order to make it a decentralized cryptocurrency. Blockchain requires some functionality such as storage, routing, mining and wallet services to operate upon.[4] Blockchain network can contain a different form of nodes depending on these functionalities. Even the idea of the smart contract is introduced by blockchain technology. A computer program that allows a contract to be implemented automatically under some prior conditions is Smart contract. For example, An application logic is implemented for a transaction to occur in cryptocurrency exchange. Ethereum and Hyperledger are examples of the fusion of blockchain and smart contracts. Hyperledger is also a blockchain but only developed for those companies where modules are deployed according to user needs. Etherium is made up of an inbuilt Turing-complete programming language that enables appropriate usage of smart contracts and devolved applications. Contracts are written in "Ethereum virtual machine code".[5] According to a

978-1-7281-0283-2/19/$31.00 ©2019 IEEE

recent survey done by PwC, the investment made by startups in this technology in 2016 is greater than 1.4 billion dollars. Since everything has its pros and cons, regardless of several advantages that blockchain offers and it's coherence, a great number of challenges are yet to be dealt with.

The remainder of the paper is organized as follows. Section 2 presents the Background of Blockchain technology and Architecture. The Permission-less vs Permissioned blockchain is elaborated and distinguished in section 3. Section 4 presents the various application areas of blockchain. Bitcoin: The first decentralized cryptocurrency and a public ledger are elaborated in section 5 of this paper. Section 6 concludes the paper with several open future research challenges in the field of security in information communication technology.

II. Background of Blockchain and Architecture

As blockchain technology is a peer to peer distributed network, it maintains the copy of the blockchain which is linked list type data structure which uses public-private key cryptography. Before getting into the details, the block of a blockchain is needed to be understood. Diving into the details of the block, data is being stored into the block as message digest (encrypted message) using secured cryptographic function. All the transactions of the block are digitally signed using peers private key and encrypted by verified peers. Inside a block, there could be multiple transactions and all are in an encrypted format or signed digitally which ensures that only authorised peer with unique decryption key are allowed to view the information or transaction of the ledger. The structure of the block is like a container data structure that carries multiple transactions. Bitcoin may contain more than 500 transactions on an average, the size of a block is around 1MB.

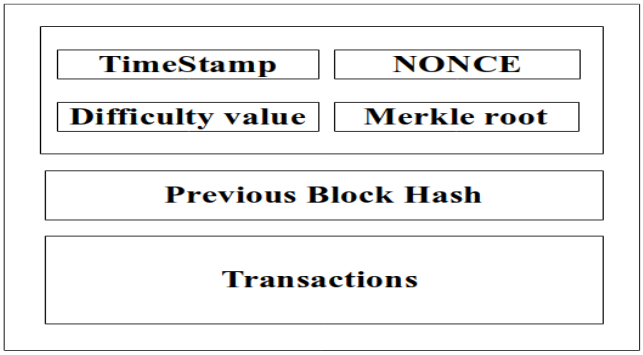

Fig. 1 - Block of Blockchain

Block header consists of three parts namely *the previous block hash, mining statics to construct the block and Merkle root tree*. The previous block-hash is used to create a new block to make blockchain tamper proof which means every new block inherits from its previous block. Mining statics is the mechanism to generate the hash, this mechanism is needed to be complicated enough to make sure blockchain is tamper proof. The equation below presents the bitcoin mechanism.

$$HASH^{k} = \text{HashingFunc}\langle \text{Nonce} \rangle$$

where $HASH^{k-1}$ represents the previous hash, T is the set of the transaction, *Nonce* is referred to as any random number which is used to generate the hash of the block, K is the current block. Here, the task of miner is to find out this nonce value such that it ensures the current difficulty on generating a hash value. For example, difficulty can be defined in terms of number of zeroes in the hashed value. Whatever be the hashed value, the first 20 bits of the obtained value must be zero. The blockhead of blockchain contains a timestamp value, Merkel root, difficulty target, nonce (random generated value to find out block-hash and difficulty). In Merkel tree root, the transactions are organized in Merkel tree structure, in which the root of the Merkel tree is verification of all the transactions. The first block of blockchain is known as genesis block which contains all the required and blockchain network configuration in it.

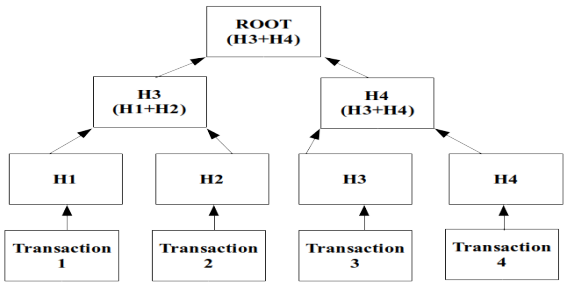

Fig. 2 - Merkel Tree of Transaction

Transaction in a block: the transaction is organised as a Merkle tree. The Merkle tree is used to construct the block hash. If any of the transaction is changed or tampered, all the subsequent block hash will require a computation again which is almost impossible. The difficulty of the mining algorithm will determine the robustness of the blockchain. Now the interesting part about this technology is the management of all the replica of blockchain in the entire network. The idea behind it is that there are multiple nodes in the network which are interconnected and every node contains the replica of the global blockchain so the necessity to maintain the integrity of the network is the condition that all the replicas require to be updated. There must exist a consistent and similar blockchain at every node or peers. In order to achieve this necessity distributed consensus algorithm comes into rescue which ensures that similar data gets visible to different nodes in the network at nearly the same point of time and it also ensures that there exists no single point of failure because data is decentralized so if one node fails the data can still be

recovered from other multiple nodes hence the system will still be able to provide services even if there exists a failure. The issue here is the management of consensus among a large number of participants in this permissionless environment where no one trusts each other. Here are some of the algorithms - PoW, PoS, PoB, PoET which will help to maintain the integrity. A brief overview of these algorithms is given in Table-1 below.

Table-1: Integrity Maintaining Algorithms

S. No.	ALGORITHM	Full form	WORKING
1.	PoW	Proof of work	In this type of algorithm if a block is to be affixed in the network then some mathematical puzzle is required to be solved which needs very high computation. Only the Peers who solved it first will be able to add to the existing longest chain, also known as most power hungry protocol.
2.	PoS	Proof of Stake	Proof of Stake algorithm is an energy efficient protocol in which peer needs sufficient stake to mine the block. This stake could be anything which is related to digital wealth.
3.	PoB	Proof of Burn	Proof of Burn Algorithm is similar to Proof of Stake Algorithm but the only difference is that in this algorithm, the miner needs to burn or spent their digital wealth to mine block. It is energy efficient but could consume a large amount of virtual currency or token.
4.	PoET	Proof of Elapsed Time	Proof of Elapsed Time is majorly used in permissioned environment. The basic idea behind this algorithm is every peer has to wait for a random amount of time, the peer whose time duration is finished first could mine block.

To Maintain reliability and fault tolerance in a distributed system, consensus is needed. Here reliability and fault tolerance means in the decentralised environment when you have multiple peers and they can take their own decision then it may happen that some nodes behave maliciously or faulty. Here Faulty nodes do not indicate a hacker or a potential harmer instead a failure in the network. Some of the failures which arise are *Crash fault* (peers suddenly crash or become unavailable to other peers), *Network fault*, and *Byzantine fault*.[6] The computational work can be reduced and the concept of a miner can also be removed. This process is called permission blockchain where all the nodes are trusted and known by the organisation. This concept is further explained in section 3 of this paper.

III. PERMISSIONLESS VS PERMISSIONED BLOCKCHAIN

As a single entity cannot serve all the possibilities of Computer Engineering, Business Logic, Economics (financial logic, banking), Supply chain, Cryptography. Every business has its own needs, their own protocols hence relying on a single technology is very difficult for developers. To overcome this situation, many new blockchain networks are created with a minimal change in protocols although the backbone remains the same. With advancements they are further divided into various types, two of its type i.e permissionless and permissioned are explained beneath.

Permissionless Blockchain is well known for its digital currencies like bitcoin and Ethereum. this blockchain allows all the participants to freely join the network, create their wallets, submit the transaction, read transaction other things without pre-authentication or authorization. This is the reason why we need a consensus mechanism. Even peers have their own choice of either acting as a node or helping in mining procedure to help to verify new transactions. The operation of the blockchain depends on a challenge which is expected to solve by the miner.[7] Whosoever solves the challenge is declared as the winner and the blockchain is then updated accordingly and broadcasted. Further, the major characteristic of permissionless blockchain is that it is *Decentralized* (It was proposed initially that blockchain must be decentralized so no central authority is allowed to edit, manipulate or shut down the network and try to change its protocols and access data. As all permissionless network relies on their consensus protocols so any change can be allowed only if more than 50% of peers agree on it) , *Anonymity* (refers to the fact that no person is required to submit or register their personal information to participate in the network), *Transparency* means that in the permissionless network, all the peers are allowed to access the information except the private key of other peers.

In *Permissioned Blockchain* the network cannot be easily accessed, unlike permissionless blockchain. It is more focused towards industry application where all the trusted members are in a closed environment and there is no central database. All the trusted members know each other but they don't trust each other and consensus is still required. So the authentication is required to join this type of network. Permissioned blockchain is said to be partially decentralised because the governance authority decides the type of consensus to be allowed to run on different types of peer because of the variation in the jobs of the peer. Similar to permissionless blockchain transparency is provided to everyone who has access to the network. Anonymity is totally dependent on the Organisation or blockchain architect. Due to its governance properties, it is easier to scale it up and reduce the cost for computation and the risks of failures in the network.

IV. BITCOIN : THE FIRST DECENTRALIZED CRYPTOCURRENCY AND A PUBLIC LEDGER

Satoshi Nakamoto proposed a completely decentralised cryptocurrency in 2008 which is referred to as *Bitcoin.*[10] It is a peer to peer automated mortgage system based on mathematical proof which is permissionless. The basic idea behind Bitcoin is to create a medium of exchange in which no central parties or authority are allowed to maintain or record the transaction which is propagated electronically in a peer-to-peer network in a secure, verifiable and immutable way.

On august 18, 2008, a domain name "bitcoin.org" was registered when Nakamoto started his journey to develop the concept of blockchain and cryptocurrency. On October 31, 2008, a white paper was released by Satoshi Nakamoto "Bitcoin - A peer to peer electronic cash system". Blockchain provides digital trust by recording important information as a public ledger and it is totally tamper proof, transparent in nature, time-stamped and decentralized. On january 3,2009, the first genesis block was mined Block 0, the genesis block, was established at 18:15:05 GMT. First client side code was released on January 9, 2009, through this anyone is allowed to commit transaction in bitcoin's blockchain. On January 12, 2009, Satoshi Nakamoto (Developer) sent Hal Finney (Bitcoin activist) 10 Bitcoins.

A. Working

In the Bitcoin network, every user is considered as a node that digitally signs the transaction using their private key after the node creation process. Transactions contain certain information such as addresses of sender and receiver, Bitcoin's logical values, some set of rules, etc. The transaction is further broadcasted in the network using predefined protocols (also known as gossip protocols). Then these set of transaction is validated by a miner and other nodes in the network. After this validation process, these transactions are in a ready state to get into the mined block[8]. The mined block will reflect all the valid transactions in sender's and receiver's wallet. the following paragraph will provide detailed knowledge about it.

Consider four nodes i.e Node_A, Node_B, Node_C, Node_D. As discussed in the previous section, blockchain is a public ledger. A transaction is being stored in a block hence, every block contains the transaction information. As per figure 1, the first block contains information of Node_A having $100 initially, then Node_A makes a transaction of $50 and transfers it to Node_B. So, the next block contains that particular transaction. Now Node_B transfers $30 to Node_C making a transaction, all these transaction nodes are connected with the concept called *Hash chain.* As the basic concept of Blockchain is to work on a decentralized network, the copy of the entire blockchain is available to all individual in the network (single node may contain multiple transactions).

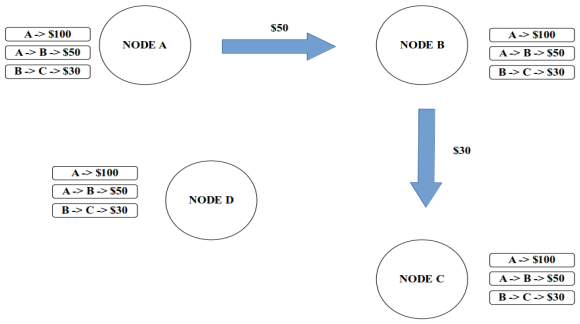

Fig. 3 - Transaction flow in a bitcoin

B. Bitcoin Transaction Lifecycle

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

1) The Sender

Let's suppose Node_A wants to send some money to another peer, so Initially, Node_A needs to open its bitcoin wallet and provide the address of that peer it wants to send (let say Node_B) and the amount to transfer and sends. Once Node_A sends then wallet create a transaction like "Node_A to Node_B $50", Sign the transaction using Node_A's "Private Key" (using Digital Signature concept) and Broadcast it to the network. Other Nodes in the network validate the transaction and sends to "Miner", "Miner" mines the next block which include those transactions.

2) The Miner

The miner collects all transactions for the time duration say 10 minutes. now miner constructs a new block and tries to connect it with the existing blockchain, through a cryptographic hash computation. Once mining is over and the hash is obtained, the block is included in the existing blockchain. Now the updated blockchain is propagated in the network.

3) The Receiver

The receiver is also a part of the blockchain network. It receives all transactions committed in the new block. As the transaction is for the receiver so the receiver's wallet reflects that transaction.

V. CONCLUSION

In this paper, Blockchain Technology is discussed in detail. This technology is advantageous since it is allowing information to be publicly available but, at the same time, is promising immutability and uprightness of data. Our review suggests that acclimating the blockchain technology in future development can totally change the scenario in security concern of data authenticity and integrity as it provides transparency and a ledger which is available publicly and free to access it with suitable authentications and immutability of

data among all those who don't trust each other but there are a lot of new challenges and research to be tackled and addressable in various area of privacy, public-private key protection, governance, stability, standardization, computing, and most important thing scalability. Peer-to-peer distributed or a decentralised system ensures privacy through the public-private key concept. Different integrity maintaining algorithms such as PoW, PoS etc are discussed. Fault tolerance and reliability are an important part of a distributed system. In the later section of this paper, we conclude the most famous application of blockchain which is bitcoin. Bitcoin incorporated blockchain from sending bitcoin to receiving as well as transmission phase very beautifully or we also can say bitcoin is the only one which submerged blockchain technology and helps in research and to explore further about this technology. As for further research, it would be of interest to explore blockchain technology's contribution within real world use cases. Hence, insights are to be generated by performing a large-scale empirical analysis on existing areas of application.

REFERENCES

[1]. Singhal, B., Dhameja, G., & Panda, P. S. (2018). How Blockchain Works. Beginning Blockchain,31-148. doi:10.1007/978-1-4842-3444-0_2

[2]. Daneshgar, F., Sianaki, O. A., & Guruwacharya, P. (2019). Blockchain: A Research Framework for Data Security and Privacy. Advances in Intelligent Systems and Computing Web, Artificial Intelligence and Network Applications,966-974. doi:10.1007/978-3-030-15035-8_95

[3]. *Buccafurri, F., Lax, G., Russo, A., & Zunino, G. (2018). Integrating Digital Identity and Blockchain. Lecture Notes in Computer Science On the Move to Meaningful Internet Systems. OTM 2018 Conferences,568-585. doi:10.1007/978-3-030-02610-3_32*

[4]. *Tikhomirov, S. (2018). Ethereum: State of Knowledge and Research Perspectives. Foundations and Practice of Security Lecture Notes in Computer Science,206-221. doi:10.1007/978-3-319-75650-9_14*

[5]. *Norvill, R., Pontiveros, B. B., State, R., & Cullen, A. (2018). Visual emulation for Ethereums virtual machine. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium. doi:10.1109/noms.2018.8406332.*

[6]. Hao, X., Yu, L., Zhiqiang, L., Zhen, L., & Dawu, G. (2018). Dynamic Practical Byzantine Fault Tolerance. *2018 IEEE Conference on Communications and Network Security (CNS)*. doi:10.1109/cns.2018.8433150.

[7]. Cash, M., & Bassiouni, M. (2018). Two-Tier Permission-ed and Permission-Less Blockchain for Secure Data Sharing. *2018 IEEE International Conference on Smart Cloud (SmartCloud)*. doi:10.1109/smartcloud.2018.00031.

[8]. Ghimire, S., & Selvaraj, D. H. (2018). A Survey on Bitcoin Cryptocurrency and its Mining. *2018 26th International Conference on Systems Engineering (ICSEng)*. doi:10.1109/icseng.2018.8638208 .