IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue, 5, March 2019 E-ISSN: 2347-2693

Compendious Summary of Blockchain

Sumathy Kingslin[1*], Rafath Zahra[2]

[1]Dept. of Computer Science, Quaid-e-Millath Government College for Women(A), Chennai-600 002, TamilNadu, India
[2]M. Phil Scholar, Dept. of Computer Science, Quaid-e-Millath Government College for Women(A), Chennai-600 002, TamilNadu, India

DOI: https://doi.org/10.26438/ijcse/v7si5.161166 | Available online at: www.ijcseonline.org

Abstract—Where there is technology there is always a scope for innovation. Blockchain technology is one such innovation that provides a decentralized solution for storage and immutable transactions that is hardly possible to fake. Blockchain is a subject undergoing intense study that has gained universal attention being the foundation of the most happening cryptocurrency. It is a distributed ledger that uses the appropriate consensus algorithm for secure transactions and records them all in an immutable chain of blocks hence forming a blockchain. Each block in a blockchain can be considered as page of a record that includes all the necessary details of any transaction. The transactions could be of any type based on the application the blockchain technology is being used for. The security and integrity of blockchain is achieved by using hashing and consensus algorithm. Hash is a unique number that determines a specific block. Each block contains the hash of the current block and also the hash of the previous block, any tampering with a block affects the validity of the following blocks making them invalid. Nodes in a blockchain are interconnected using peer-to-peer network and play a decisive role to validate any new transaction. Nodes come to a consensus using complex mathematical calculations after which the validated transaction records are added to the blockchain. Blocks that are once added to a blockchain can never be modified. A single node or a single network cannot control the entire database providing security in a trust less network. These spectacular features of blockchain has gained popularity in various fields other than cryptocurrency, to name a few real-estate, supply chain management and health care etc., This paper gives a compendious summary of blockchain with an overview of its fundamentals, its working and its diverse applications.

Keywords- Blockchain, Decentralized, Security, Consensus, Transactions, Hashing, Digital Signatures.

I. INTRODUCTION

William Mougayar, the author of "The Business Blockchain" said "The blockchain cannot be described just as a revolution. It is a marching phenomenon, slowly advancing like a tsunami, and gradually enveloping everything along its way by the force of its progression [1]. He rightly said because blockchain is considered as a game changer in various industries. It has gained widespread population within a short period of time. Earlier Blockchain was considered as the technology that could be useful only for the financial services. But many public and private sectors are exploring the vast potential of blockchain [11]. Various fields such as supply chain management, healthcare, real-estate, entertainment, insurance sectors, etc., have already joined in the revolution of blockchain and has started taking the advantages of this promising technology. The objective of this paper is to provide a complete summary of how the blockchain works, in order to understand its benefits and the reason for it being a game changer technology.

Any technology that provides transaction or information sharing facility must assure secure transactions, easier access, and unchangeable permanent transactions [7]. Before the dawn of Blockchain technology all the transactions were only possible with the help of an intermediary who is responsible for managing the transactions in a secure manner. This intermediary is a trusted party and is answerable for any failure or fraud in the transactions. The entire data interchange happens through this middle man. This kind of netwok used for information sharing or transactions is known as the Centralized system. In the centralized system a middleman gets the central authority and privilege of decision making to validate any transaction [2]. Following are the problems of a centralized system

- The central authority has the access of the entire data and can use it whenever required.
- All the rules of the network communication and transactions are set by this central authority.
- The middleman must be a trusted source for secure data interchange.
- The central authority can be a single point of failure. If the server crashes the entire network will face a breakdown.

Blockchain offers solution to the above-mentioned issues. Blockchain is a decentralized system that uses peer -to - peer networking to offer information sharing between nodes [8]. Following are the solutions offered by blockchain

- Since it is a decentralized system there is no central authority who can access the data of the database.
- All the rules are predetermined and every node knows the operation mode of and rules of this network. Consensus of every node in the blockchain is required to modify the rules of the blockchain.
- Blockchain provides a trust less secure transaction environment. This system works by assuming that the nodes of a blockchain do not trust each other for any transaction. Since it is a decentralized system, and every node maintains an updated copy of the transactions the need of a trusted central authority is removed.
- Since each node has the updated copy of the database, even if one part of network fails, data can be retrieved form the other nodes of the blockchain.

This paper structure is arranged in a way to provide a detail understanding on the working of blockchain giving a detailed view on how it is beneficial for secure transactions. Section I included the introduction with a bird's eye view on the blockchain technology. Section II contains a brief history of blockchain. Section III working of blockchain followed by Section IV that briefs on applications of Blockchain, Section V concludes the research work with future directions

II. WHERE IT ALL BEGAN?

In 2008, Satoshi Nakamoto released a paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [3]. This paper introduced a secure way of online transactions between two parties without the need of a trusted third party in the middle. It proposed a public ledger that maintains all the required details of timestamped transactions. After each transaction all the nodes/users of this system are intimated about this transaction. This ensures that every node in the network are aware of the transaction and they validate the chain of transactions. This method of validating transactions ensures that a third party is not required and the bitcoin system is completely decentralized. With this decentralized system emerged the concept of blockchain.

III. WORKING OF BLOCKCHAIN

Blockchain technology is a combination of various promising technologies, all put together to provide a secure, distributed sharing and transaction system.

A. Significant Terms

Before the detail explanation on working of blockchain it is necessary to build familiarity with these technologies that are part of the blockchain systems. The understanding of the following terms is highly required in order to understand the working of blockchain and its application.

Nodes in a Decentralized Peer – to – Peer Network-In blockchain there are peer nodes that hold the copies of the updated ledger. Each peer is a computer system in the network that is equally important and is referred to as node. Whenever a transaction occurs, the nodes of the network verify it with the help of the updated ledger copy. In this system data is not stored in one centralized point ensuring it is not hacked or lost.

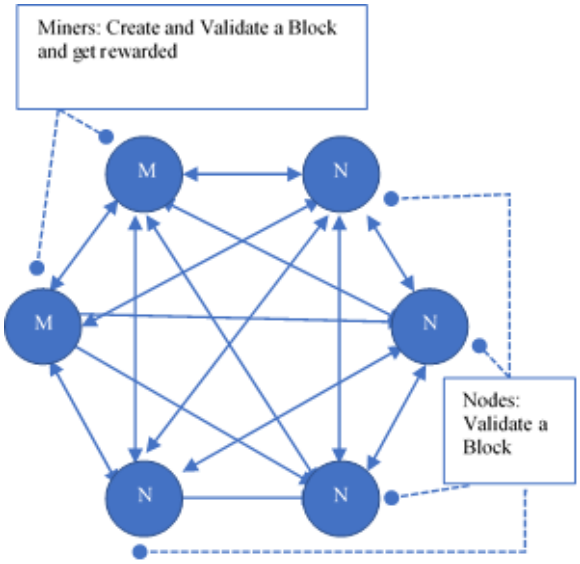

Figure1: Nodes and Miners Connected in a Peer – to- Peer Network

Miners-Miners are nothing but nodes of the blockchain network that hold the copies of transaction records. The job of the miner is to add the transactions to the unchangeable distributed ledger. Miners invest powerful resources to compute complex algorithms and validate these transactions [2]. As a reward miner gets some incentives based on the blockchain application. Figure 1. Illustrates the difference between a node and a miner.

Blocks-A block includes the details of all the recent transactions occurred in a particular time period. Miners create a hash code using all the transaction details and store it in a block. Once a hash value is calculated and verified this block is added to the blockchain and the chain keeps growing. Figure 2. Shows the contents of a block. The first block of a blockchain is known as "Genesis block" [4].

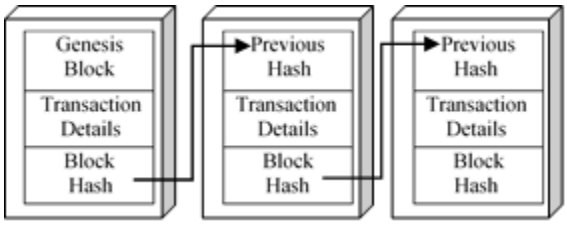

Figure 2. Contents of a Block

Hashing-Hashing is the process of transforming any input into a fixed length output using cryptographic algorithms. Hash values are unique to each block and serve as the identifying factor. Each block contains transactions, that when combined and validated, produce a unique hash. Fig 3 illustrates that even a minute change in the input will show a drastic change in the calculated hash value.

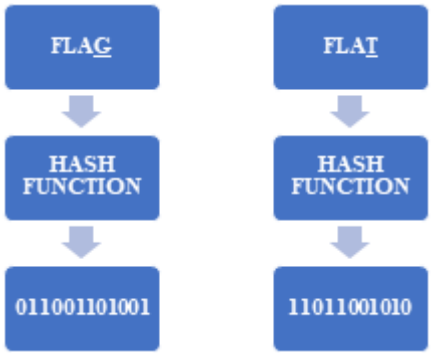

Figure 3. Hash Function

This makes the blockchain secure as no one can modify the transactions. Hashing algorithm also ensure that the concept of reverse engineering cannot be applied. A hacker cannot retrieve the input details by viewing the hash value .

Consensus Algorithm-As mentioned earlier the nodes come to consensus to validate a block by following a set of rules. All the nodes follow one consensus mechanism. The main objective is to ensure unanimous acceptance between nodes on the network, even if some nodes are unreliable [6].

Digital Signatures-Digital Signatures are used to ensure security and validity of data in blockchain. Digital signatures use asymmetric cryptography. Every user in a blockchain has a unique private key and a public key. These keys are a string of 1s and 0s. Figure 4. shows that producing a digital signature involves a function that includes both the message and the private key. Altering the message even slightly will change the digital signature. Any information that needs to be transacted is digitally signed using the private key of the sender. On the receiving end the digitally signed content is validated for its authenticity using the shared public key of the sender [4] Figure 4. illustrates the same.

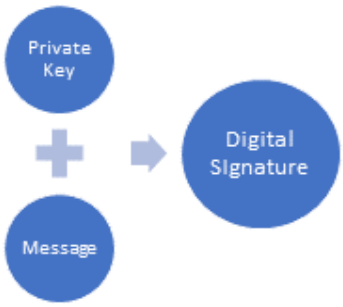

Figure 4. Digital Signatures

Figure 5. Application of Digital Signatures

B. Consensus approaches

Solving Byzantine Fault Tolerance is a big challenge addressed by blockchain technology. According to "Byzantine General Problem" no two nodes of a network can guarantee that the data they communicated has arrived. The solution is to achieve consensus in a network where some of the nodes can be malicious or even if some attackers are trying to undermine the network [6]. Following are the various approaches to reach consensus in blockchain

Proof - of- work (PoW)-This is the consensus mechanism used in Bitcoin systems [3]. In this system, each node uses complex calculations to obtain the hash value of the block [5]. The calculated hash must be equal or smaller than the already fixed target value. Once a node successfully calculates the hash of that block it is broadcasted to all other nodes in the network. All the other nodes check the correctness of that hash value. Once the nodes validate the calculated hash value, the corresponding block is added to the blockchain. All the nodes add this block to their records. At a time if more than one node calculates the hash value, a conflict occurs and this is resolved by considering the longest chain of blocks. It is impossible that two nodes will generate blocks simultaneously as the miners have to use a lot of resources to calculate the hash of each block.

Proof-of-Stake (PoS)-In this algorithm the validator of the next block is chosen based on its wealth, coin-age or by random selection. Here the miners can be considered as validators as they can add the blocks to the network by showing their stakes as proof [5]. If an application uses coin-age PoS for its network, the coins get weightage based on the its value multiplied by the time period since its creation. The nodes holding such coins have more rights is in the network in validating a block. This method is a solution to vast usage of resources in PoW. In few application validators are chosen randomly in order to avoid malicious attacks.

Practical Byzantine Fault Tolerance (PBFT)-This model works as a state machine that is replicated at different nodes in the distributed network. The nodes in this network are sequenced, with one node considered as the master node and the other nodes as clients. Nodes communicate with each other to ensure that all the nodes come to a consensus on the state of the system using a majority rule [6]. For this system to function the malicious nodes must not equal or exceed one third of all nodes in the system. This model works in four rounds known as views:

1. A client requests the master node to start a service operation.
2. The master node broadcasts this service message to the nodes.
3. The nodes process the request and reply to the client.
4. The client awaits f+1 reply from different nodes with the same results, where f is the maximum number of possible faulty nodes. The master or the leader node is changed for every view.

Delegated Proof of Stake (DPoS)-Delegated Proof of stake is similar to PoS except it combines voting power to appoint delegates. The role of the delegates is to validate the transactions and maintain the network. Any node that holds stakes can cast its vote to choose the delegate. The validator with maximum votes becomes a delegate and validates the transactions [5].

Delegated Byzantine Fault Tolerance (DBFT)-Majority of nodes are ordinary nodes and these nodes vote to choose a delegate known as Book keeping node based on certain mandatory requirements. One of these delegates is randomly selected as a speaker. To verify a block, the speaker broadcast its block to other delegates. These delegates match their own block with the speaker's block to check its validity. A block that receives consensus from 2/3 nodes is added to the network.

Table 1 gives an overview of different types of consensus algorithms.

Table 1. Types of Consensus Approaches

Consensus Approaches	
Algorithm	*Overview*
PoW	Involves Complex Computing
PoS	Assets at stake
PBFT	Splits as Master and Client Nodes
DPoS	Combination of Voting and Proof of Stake
DBFT	Choose Delegates based on Majority votes

Newer and modified consensus algorithms are being experimented with the blockchain.

C. Working of Blockchain

This section aims to explain the working of blockchain technology in stages. This paper illustrates the steps involved with a sample transaction. The transactions could be of any time based on the application, for example, claiming tokens in a charity network or giving access to digital art. The terms required to understand the working of blockchain are explained in the previous section. As mentioned earlier Blockchain provides a clever system of decentralized trust less verification based on cryptography [9]. Figure 6. demonstrates the working of blockchain, the detail explanation is as follows

1. A ledger to record all transactions is maintained. Since it is a public ledger anyone in the network can initiate and add a transaction to it.
2. Blockchain provides a solution of authenticity of the transactions by the means of Digital Signatures. With the help of the digital signature the sender proves its approval. The system verifies the digital signature with a verify function that includes message and digital signature and decrypt it using the public key of the sender. For every new transaction the signature also includes a unique transaction ID for enhanced security.
3. Even though the authenticity is checked for a requested transaction, blockchain also checks for the availability of the requested transaction in the ledger.
4. A verified transaction is broadcasted in the network and all the nodes of the network update their copy of the ledger by adding this transaction to their record.

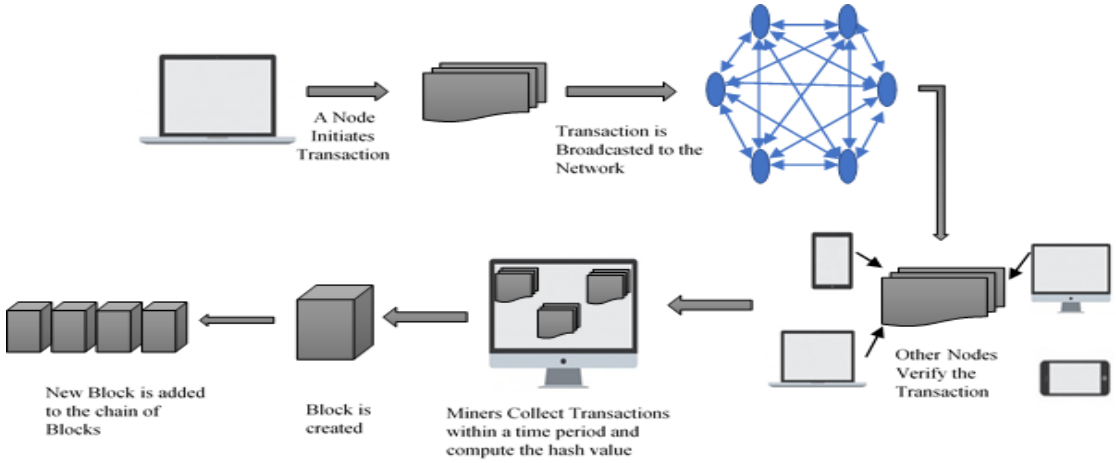

Figure 6. Working of Blockchain

5. If all the nodes are broadcasting a transaction, there needs to be a mechanism for all the nodes to agree on one correct ledger and ensure all the nodes maintain same copy of transactions.
6. Blockchain uses the core idea of all the nodes trusting the ledger that has more amount of work put into. To ensure this blockchain organizes a given ledger in blocks and each block includes a list of transactions together with PoW. This PoW is nothing but a special number so that the hash of that block starts with a specified number of zeros, for example 50 Zeros.
7. Each block also includes hash of the previous block at its header to ensure the transactions are organized in a standard order [9]. With the help of this systematic protocol of creating blocks, this system allows any node to be a block creator also known as miners.
8. Miners collect few transactions that are broadcasted in a block and do the computations to find the special number that makes the hash of the block begin with the specified number of zeros.
9. Once they compute the hash, they broadcast their version of block in the network. The other nodes of the network do not trust the block immediately, the nodes wait for the longest chain and update their copy of blockchain with the newly verified blocks.
10. For successful creation of a block the miners are rewarded.

This paper covers the core steps involved in blockchain transactions but there is more to understand about blockchain.

IV.APPLICATIONS OF BLOCKCHAIN

Due to all the mentioned promising features of blockchain, this technology has been adopted by various industries. It has revolutionized the security and transparency in a decentralized network. Following are some of the main fields where blockchains are being used other than cryptocurrencies.

Blockchain for Humanitarian Crisis - Building block is the program started in 2017 that helps the World Food Program (WFP) to distribute cash – for – food aid to over 100,000 Syrian refugees. With the collaboration of UNHCR's existing biometric authentication technology any Syrian refugee can prove their identity and purchase things they require [12].

Blockchain in HealthCare – Blockchain can be used to maintain immutable patient's records [10]. MedRec is one among the others who have implemented Blockchain to maintain the Electronic Health Records facilitating easy access to past records of the patients [13].

Supply Chain Management – Traceability and transparency is highly required in Supply Chain Management. Blockchains are being used in this field to maintain a shared ledger that is updated and validated to determine the condition, location and other details of any asset at any given time [10].

Blockchain in Real Estate – Blockchain is used in the real estate industry to sell and maintain the details of the properties. The aspects of legal issues, occupancy, financial dues, loan, ownership, contracts etc., can be maintained using blockchain [9].

Blockchain for Government – Governments can use Blockchain to maintain public records, process inventory, information exchange etc., [16].

Blockchain in the Media- Kodak has proposed to use blockchain technology for payments to photographers and tracking property rights [14].

Blockchain in Event Management – KickCity is one of the event management platforms that provides incentive-based event influencer community on blockchain. Users are incentivized to share events with their network and help vendors sell out tickets [15].

V. CONCLUSION

Blockchain is a distributed ledger system that uses the consensus mechanism for secure transactions. This paper covers all the main ideas of the blockchain system. First, we explained the definition of Blockchain System followed by a brief history and a brief explanation of all the key terms involved in this technology. We then enlightened on few of the widely used Consensus algorithms used in various blockchain applications. The process of transactions in Blockchain is explained with a detail step by step procedure and a clear diagram. In future we plan to perform in-depth investigation on the types of blockchains and alternate design methods.

REFERENCES

[1] W. Mougayar," *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*", Wiley Publisher,2016.

[2] A. Kaushik. A. Choudhary, C. Ektare, D. Thomas, S. Akram, "*Blockchain- Literature Survey*" In the Proceedings of the 2nd IEEE Conference on Recent Trends in Electronics Information & Communication Technology, India, pp.2145-2148, 2017.

[3] S. Nakamoto, "*Bitcoin: A Peer – to – Peer Electronic Cash System*", 2008

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "*An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*" In the Proceedings of the IEEE 6th International Congress on Big Data, pp.557-563,2017.

[5] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun, "*A review of Consensus Algorithm of Blockchain*" In the proceedings

of the IEEE International Conference on Systems, Man, and Cybernetics (SMC), Canada, pp. 2567 – 2572, 2017.

[6] M. Castro, B. Liskov, "*Practical Byzantine Fault Tolerance*", In the Proceedings of Third Symposium on Operating Systems Design and Implementation, USA, pp. 1 – 14, 1999.

[7] S. Seebacher, R. Schuritz, "*Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review*", In the Proceedings of Exploring Service Science: 8th International Conference, Italy, pp.12-23, 2017.

[8] K. Sultan, U. Ruhi, R. Lakhani, "*Conceptualizing Blockchains: Characteristics & Applications*", In the Proceedings of 11th IADIS International Conference on Information Systems, Portugal, pp. 49 – 57, 2018.

[9] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, G. Das, "*Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes and Problems*", IEEE Consumer Electronics Magazine, Vol.7, Issue.4, pp. 6 – 14, 2018

[10] S. Thakur, V. Kulkarni, "*Blockchain and Its Applications – A Detailed Survey*", International Journal of Computer Applications, Vol.180, No.3, pp.29 -35, 2017.

[11] P. Tasatanattakool, C. Techapanupreeda, "*Blockchain Challenges and Applications*" In the Proceeding of International Conference on Information Networking", Thailand, pp. 473 – 475, 2018.

[12] https://innovation.wfp.org/project/building-blocks

[13] https://medrec.media.mit.edu/

[14] https://www.kodak.com/kodakone/default.htm

[15] https://kickcity.io/

[16] S. Olnes, J. Ubacht, M. Janssen, "*Blockchain in Government: Benefits and implications of distributed ledger technology for information sharing*", Government Information Quarterly, Vol. 34, Issue. 3, pp. 355 -364, 2017.

