ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse109922020.pdf
https://doi.org/10.30534/ijatcse/2020/109922020

Blockchain Technology, Use cases and Content Delivery Network

Vijaya Murari T[1], **Dr. Ravishankar K.C.**[2]
[1]NMAM Institute of Technology, Nitte affiliated to Visvesvaraya Technological University, Belagavi, India,
vijayamurari.t@nitte.edu.in
[2]Government Engineering College, Hassan affiliated to Visvevaraya Technological University, Belagavi, India,
kcr@gechassan.ac.in

ABSTRACT

Blockchain is a distributed public ledger that contains all the digital transactions which is shared amongst the parties who participate in those transactions. It stores these transactions in such a way that it does not undergo any changes. Bitcoin is the popular application which makes use of the block chain technology. Many other applications like finance, real estate, IoT, supply chain etc use blockchain technology. The idea of the blockchain can be used by the content delivery networks to deliver the content to the customers in the reliable and secure manner. This technology has its own challenges and business opportunities which make it a fascinating concept from the perspective of research.

Key words: Blockchain, Distributed consensus algorithms, Content Delivery Network, use cases.

1. INTRODUCTION

Crypto currency is the term used for all peer to peer financial transactions that are secured with help of cryptography in a distributed environment. Traditionally, the security for the financial transactions is provided by the trusted central entity. The idea of crypto currency that is Bit coin was developed by Satoshi Nakamoto in 2008 [1]. Bitcoin makes use of the block chain technology to provide security to the transactions carried out by the two parties. It doesn't make use of the trusted third party applications to provide security to the online transactions of the users. In this technology, all the transactions that are carried out by the customers are stored in blocks which are immutable. If additional transactions are carried out then they are added as additional blocks to the chain and the block chain grows. Public key cryptography provides security to the user and the consistency of the blocks is looked after by the distributed consensus algorithm like Proof of Work and Proof of State. Blockchain technology can be used in different financial services like online payment, digital transactions related to assets, remittance etc. Rest of the paper is organized as follows: Section 2 describes the block chain architecture and distributed consensus algorithms, Section 3 introduces the different use cases in the block chain technology, Section 4 describes the blockchain based content delivery networks and section 5 lists the challenges faced by the blockchain technology. Section 6 provides the conclusion of the paper.

2. BLOCKCHAIN ARCHITECTURE AND DISTRIBUTED CONSENSUS ALGORITHMS

Block chain is made up of blocks which are arranged in a sequence. Each block in the sequence stores the transactions that have been carried out. Figure 1 shows the structure of a block within the block chain. The first block in a block chain is referred to as the genesis block. The subsequent blocks contain the hash value of the previous parent block.

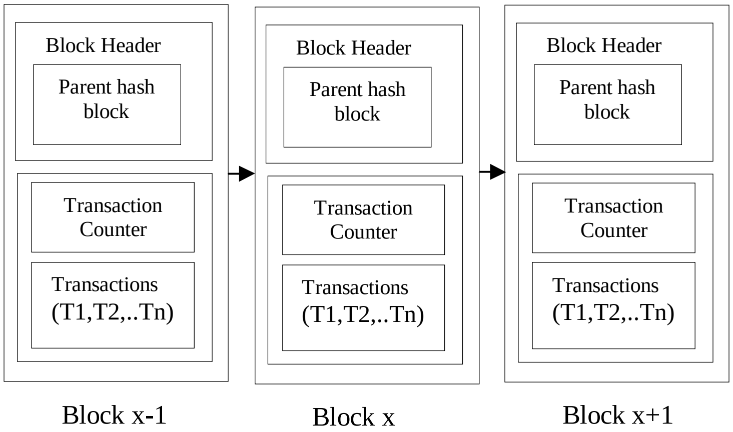

Figure 1: Structure of a block chain

The structure of a block present in the block chain is as shown in the Figure 2. It consists of the header and the body. The header of the block has following fields:
Block version: specifies the set of validation rules to be adhered by the block.
Merkle Tree Root Hash: contains the hash value of all the transactions in a block.
Timestamp: provides current time in seconds since epoch, i.e since January 1, 1970.

nBits: sets the hash value of the valid block with a target value.

Nonce: is value which starts from zero and increases with every hash value calculation.

Parent Block hash: contains a 256 bit hash value of the previous block.

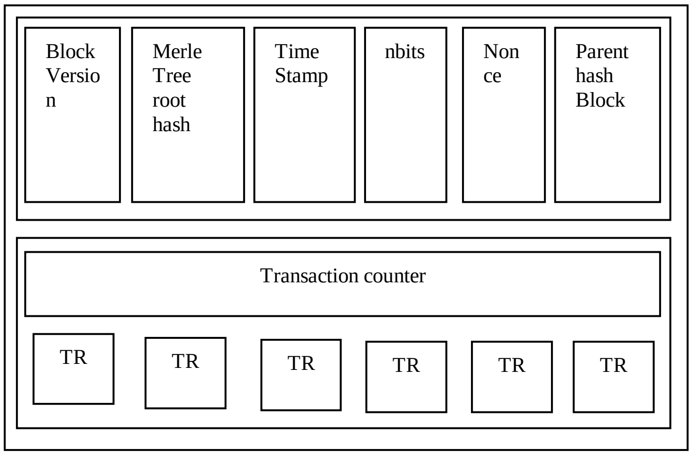

Figure 2: Structure of a single block

The body of the block contains the counter for transactions and all the transactions that have been carried out. Size of the block and size of each transaction determine the maximum number of transactions that can held in a block. Authentication of transactions in the block is carried out with the help of digital signature which belongs to the type known as public key cryptography [3][13].

Block chain systems can be classified into three categories:

1. Public blockchain: can be used by miners, developers, community members or any other users which provide transparency for the transactions carried out by them. In this type of block chain, no individual or an entity is in control of the way in which the transactions are recorded and processed. It is implemented in a decentralized manner. Public blockchains provide incentives or rewards to participants in the network with help of tokens. Anyone can join this type of blockchain without revealing their identity. Bitcoin and Ethereum are examples for the public blockchain.
2. Private blockchain: can be used by the users after they have been granted permission by an entity running the blockchain to join the network. In private blockchain all the transactions of the participants are private. It is more centralized than the public blockchain. Involvement of tokens is not mandatory in this type of blockchain. Hyper ledger and R3 corda are examples for the private blockchain.
3. Consortium blockchain: is looked after by a group not by a single entity. It provides the space for collaboration among different entities doing their business. Central banks, governments and supply chain companies can be the users of the consortium blockchain. Partial decentralized implementation takes place in the case of consortium blockchain. Ethereum and Hyperledger are helping in building consortium blockchains [4][12].

Differences between three types of blockchain are given in Table1:

Table 1: Differences among three types of blockchain

Issue	**Public blockchain**	**Private blockchain**	**Consortium blockchain**
Control over Transactions	No individual or group entity	Individual entity	Group entity
Access to transactions	Public	Private	Collaborative
Implementation	Distributed	More centralized	Partial decentralized
Tokens	Mandatory	Not mandatory	Not mandatory

Blockchain operates in a distributed environment. Distributed system is bothered by the Byzantine Generals Problem i.e. how to achieve consensus among different transacting nodes. Consistency among the transactions stored in different nodes is provided by the distributed consensus algorithm. Consensus in a blockchain is obtained through following approaches:

- Proof of Work: Bitcoin network achieves consensus using this strategy. Nodes that are involved in the process of Proof of Work are known as miners and the process is called as mining. Every node in the network computes the hash value of the header of each block. Each block header contains a nonce which will be changed by miners frequently to obtain different hash values. In order to achieve the consensus, the hash value that is computed must be less than or equal to a threshold hash value. Then the block containing this value is broadcasted to all the nodes in the network. After their validation of this hash value of the new block, miners will add this block to their blockchains. Lot of computations are carried out in this strategy which leads to high energy consumption [3].
- Proof of Stake: Blackcoin, PPcoin, Nxt applications use this strategy. In this strategy, the age of the coin is used to determine the rights in the network. Age of the coin is product of its value and time after the coin was created. If a node holds the coins for longer duration, it will be rewarded and it gets more rights in the network. This makes block chain independent

of the Proof of Work strategy which consumes more resources. Initially blockchains adapt the Proof of Work strategy and then move on to the Proof of Stake [3].

- Practical Byzantine Fault Tolerance: consensus algorithm is used by the Hyperledger. It uses replication to handle Byzantine faults. With the help of rules, primary block responsible for ordering the transactions is identified in a round. There are five different states in this process:
  1. Request: Master server receives a request from the client and a time is appended to the request by the master server.
  2. Pre-prepare: The message received by the master server is recorded and an order number is given to it. Then the pre-prepare message is broadcasted to all the other server nodes which follow the master server. To accept the request or not is initially decided by the other server nodes.
  3. Prepare: If the request message is accepted by the server node then pre-prepare message is broadcasted to all the other server nodes by it. Other nodes send messages to the server node which is then received by it. If it receives messages from 2/3 of all the nodes, then it will move on to the commit state.
  4. Commit: All the server nodes will receive the messages from the node which are in commit state. At the same time if the server node receives the message from 2/3 nodes then it comes to a conclusion that there is a consensus among the nodes to accept the request and the instructions in the request message are executed.
  5. Reply: Client receives the reply from the server nodes. If the reply is not received by the client due the delay in the network, then request is resent to the server node. The server will then send the reply continuously if the execution of the instructions in the request message has been executed [5].
- Delegated Proof of Stake: is used by BitShares. Generation and validation of blocks are carried out by the delegates selected by the stakeholders. Transactions are confirmed quickly as there as only few nodes to validate the blocks. Size of the block and interval of the block generation can be varied by the delegates. Malicious delegates are identified and blacklisted in this strategy [5].

3. BLOCKCHAIN TECHNOLOGY: USE CASES

Different use cases can leverage the blockchain technology for the solutions to their problems. They are listed below [6][14]:

1. Banking: Blockchain technology was primarily used by the Cryptocurrency applications. So, the concept of blockchain can be used extensively in the banking sector. Banking applications are bothered by the problem of double spending i.e. the amount sent from one person's account reaches the account held by the other person but the amount doesn't get deducted from the sender's account. This problem can be solved problem by maintaining a shared public transaction ledger as it is done in BitCoin.
2. Retail and consumer goods: can use blockchain to trace the origin of the product in the supply chain. The use of blockchain in supply chain and logistics makes the supply chain more transparent. This helps the retail stores to provide information about the product to the consumers very quickly. It also enables to guarantee the safety of the food items that are supplied through a supply chain. The food items which require cold storage of certain temperature can be supplied by recording the temperature through IoT temperature sensors put at every link in the cold storage supply chain. Also, smart contracts can be written to reject the delivery if the required level of temperature is not maintained in any one of link in the cold storage supply chain.
3. Supply Chain and logistics: The use of blockchain in this area helps the pieces of information contained within the different entities of the supply chain to be stored in public ledger which provides transparency to all the stakeholders of that supply chain. Blockchain accurately tracks the availability of the material in a location which in turn helps the companies to provide quality items to their customers in line with their ethical policies. It helps controlling the introduction of fake goods in between the links of supply chain. Since the information in the public ledger is same to all the entities in the supply chain, validation of information can be done quickly.
4. Health care: Medical records related to the individual patients can be stored using blockchain. Patients can permit the doctors, hospitals and other

third parties like insurance companies to access their medical records stored in the blockchain. The log of this access by the permitted entities will be there in the blockchain so that the patients could see the history of those entities that have accessed their medical records.

5. Entertainment: Blockchain paves way for the way in which payments and digital rights are handled in the entertainment field. Consumers can get the required content directly from the artist or content providers. Consumers can download, stream, remix or use a piece of content from the content provider. The artists and content providers have their say in the content rights and how their content has to be monetized.

4. BLOCKCHAIN BASED CONTENT DELIVERY NETWORKS

Content Delivery Networks (CDN) has the required infrastructure and mechanisms to provide the services to both the content providers like Netflix and the users in a time bound manner [7]. CDN has to transfer the very large multimedia media files in a secure and reliable manner to its users. The service providers in CDN can use the blockchain technology to store the data securely in a distributed environment.

Thanh X. Vu et al have proposed a blockchain based CDN that uses a private blockchain to provide services to the content providers and users. It helps the users to maintain the privacy as the virtual identity is used to obtain the services of the content providers. Here content providers can be any entity like Netflix, AmazonPrime and the users are the ones who subscribe to the contents and services provided by the content providers. By using the blockchain based CDN, the users need not to subscribe multiple times to different services provided by the different content providers. Benefits of this method have been enumerated by them. 1) Content providers can gauge the popularity of content and user preference as they have transaction history in their blockchain.2) Content providers can do away with the investment on identity and authentication infrastructure.3) Virtual identity helps the users to obtain services different content providers with a single registration to the blockchain.4) Content providers can provide improved service to their users by going through the preference stored in the blockchain [8].

Currently, digital content provided by the content providers over the network is protected with the help of the Digital Rights Management (DRM) system. This system is a centralized entity which can be compromised and when it happens it leads to piracy of the multimedia content which in turn causes heavy loss to the multimedia content generators. Information on copy rights and transaction information is not public to the users in DRM system. In this scenario, according to Jay Kishigami et al, block chain technology can be used for content distribution system. The blockchain based DRM can be used to provide security to the digital content stop the piracy of the digital content. They describe a public blockchain to implement the decentralized digital content distribution system which makes use of Proof of Work as its distributed consensus algorithm [9].

Zehao Zhang and Li Zhao use blockchain technology to describe the mechanism for digital rights management. They use the idea of smart contract to automatically distribute the license to the required customers of the respective content providers. Smart contracts are created by publishing a transaction to the blockchain. Smart contracts have unique addresses and they are the instances of computer program executing within a blockchain. Price of the content is decided by the content provider based on some rules. Based on the needs, the customer will do the price estimation and send the information to the smart contact for purchasing the content. The smart contract would then bundle the license as per customer’s request and send it to his account. The price settings, transaction of the copyrights are all carried out by the smart contracts [10].

5. CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Blockchain technology helps in solving problems in diverse areas ranging from financial to non financial services. But even this technology has the challenges and problems to overcome which are listed below:

1. Scalability: All the transactions have to be stored in the blockchain. As the transactions increase day by day the blocks in the blockchain will become heavy and count of the blocks in blockchain will also increase. The first time users have to download all the blocks and validate these blocks before executing the first transaction. This may consume a lot of time and the propagation speed of the blocks would become slow. So scalability of the blocks has to be addressed.
2. Migration: Lot of tasks related to migration may be required to move the existing contracts, business documents and frameworks to new blockchain based solution. This may incur lot of time and money.
3. Malicious Activities: The users involve in the blockchain with virtual identity. This may motivate money trafficking by the malicious users.

4. Selfish mining: Selfish miners can collaborate and reverse the transactions happened in the blockchain. They will not publish the transactions in the blockchain until some requirements are met by the public and a private branch of the chain will be created. Then this private branch outgrows the public blockchain all the miners will accept this private chain. The honest miners will be mining through the useless branch and malicious users will mine with their private branch and make more profit [2][11].

6. CONCLUSION

Blockchain technology provides a reliable and secure way of carrying out the transactions by different applications in a distributed environment. The transactions carried out cannot not modified by any participating entity in the blockchain. In this paper, we have described the structure of the blockchain, different algorithms used in obtaining the consensus in the distributed environment, different use cases related to the blockchain technology. We have also focussed on the details of how blockchain technology can be leveraged in the content delivery networks. Finally, we have listed the challenges to be faced by the applications or services while using blockchain technology.

REFERENCES

1. Nakamoto, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**, https://bitcoin.org/bitcoin.pdf as accessed on 2/03/2020.
2. Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, **Blockchain Technology: Beyond Bitcoin**, Applied Innovation Review, Issue No.2 2016.
3. Z.Zheng et al, **An Overview of Blockchain Technology: Architecture**, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data, DOI 10.1109/BigDataCongress.2017.85.
4. https://dragonchain.com/blog/diffrences-between-public-private-blockchains/ as accessed on 13/03/2020.
5. Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun, **A Review on Consensus Algorithm of Blockchain**, 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8, 2017. https://doi.org/10.1109/SMC.2017.8123011
6. Peter Soldner, **Examining and Evaluating Potential Blockchain Applications in Manufacturing and R&D**, M.S. Thesis, Industrial Management and Innovation, Uppsala University, Sweden, February, 2019.
7. Vijaya Murari T, Dr.Ravishankar K C, A **Dynamic Data Delivery Through Content Delivery Networks**, *International Journal of Engineering & Technology*, 7 (3.34) (2018) 786-793.
8. Thang X. Vu, Symeon Chatzinotas, and Bj¨orn Ottersten, **Blockchain-based Content Delivery Networks: Content Transparency Meets User Privacy**, 2019 IEEE Wireless Communications and Networking Conference (WCNC).
9. Jay Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, Akihiko Akutsu The **Blockchain-based Digital Content Distribution System**, Conference Paper · August 2015, DOI: 10.1109/BDCloud.2015.60.
10. Zehao Zhang and Li Zhao, **A Design of Digital Rights Management Mechanism Based on Blockchain Technology**, *Springer Nature*, 2018. https://doi.org/10.1007/978-3-319-94478-4_3
11. Z.Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang, **Blockchain challenges and opportunities: a survey**, *Int. J. Web and Grid Services*, Vol. 14, No. 4, 2018. https://doi.org/10.1504/IJWGS.2018.095647
12. Mark Renier M. Bailon, Lawrence Materum, **International Roaming Services Optimization Using Private Blockchain and Smart Contracts,** *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, No.3, pp. 544-550, May-June 2019. https://doi.org/10.30534/ijatcse/2019/32832019
13. Sang Young Lee, **PHR System using Blockchain,** *Technology International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, No.6, pp. 3188 - 3193, November-December 2019. https://doi.org/10.30534/ijatcse/2019/84862019
14. Monica Thomas, Dr. Varghese S Chooralil, **Security and Privacy via Optimised Blockchain**, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, No.3, pp. 415-418, May-June 2019. https://doi.org/10.30534/ijatcse/2019/14832019