Analysis of Blockchain and its Working Principle

S. Banupriya[1], G. Renuka Devi[2]

[1, 2]SRM Institute of Science and Technology, Department of Information Technology, Kattankulathur, Kancheepuram, Tamilnadu, India

Abstract: ***Blockchain is currently booming technology, which links the people over the world to do future finance through various types of cryptocurrency. Blockchain is a decentralised technology where people are connected in peer-peer network and data are shared in a distributed manner. The data in the block depend upon the type of blockchain used. For example, number of transactions are made in to block, each block is validated and these validated blocks are connected to previous blocks, because each block contains the data of the previous block and thus it makes a block chain architecture. Since this technology deals with numerous users, there is few issues regarding security, non repudiation, consistency and power supply while communicating between the users in the blockchain network. In this paper, the overall working principles and the algorithms used to subdue the above mentioned limitations in the blockchain technology are discussed and analysed. As in case of security, Elliptical Curve Cryptography (ECC) is used. For non repudiation, hashing algorithm in which particularly SHA 256 is used. For consistency, consensus algorithm is used. In real time various consensus algorithms are used but only Proof of Work (PoW) and Proof of Stake (PoS) algorithms are used widely.***

Keywords: Blockchain, Elliptic Curve Cryptography, Proof of Work, Proof of Stake.

1. Introduction

Blockchain is a distributed ledger of transaction record which facilitates trustworthy system of digital assets and interchange with no central or dominant authority. The records are distributed and accessed by anyone in the network although the individual can completely own their assets and power to control the asset. The blockchain helps to achieve the following features.1) All peer-to-peer transactions are made over the internet without need of central authority.2) Anonymous users are recognised by their virtual identity. Single user can have several identities and user cannot deny of any transaction initiated by him. 3) The transactions are validated and attached to the system in the well-organised way which makes it secure and reliable. Once the transactions are added it becomes tamper free and no one able to amend it 4) Consistency is maintained even if there are bad actors in the network.

Blockchain concept can be applied in both financial and non-financial services. It can be classified as public blockchain, private blockchain and hybrid blockchain. In a Public or permissionless blockchain, anyone on the network can read or write the record by showing the proof of work for the same[1]. This is fully decentralised and results in high rise of potential users. Crypto currencies like Bitcoin, Ethereum and Block stream are built with public blockchain methodology[9]. In a private blockchain, only the owner has the option to change the record/transaction[10]. This infrastructure is alike with existing centralised authority system and can be replaced to private blockchain to reduce cost and increase efficiency. The hybrid or permissioned blockchain is mix of both public and private blockchain, where few nodes/people in the network are allowed to change the record. This concept can be used by group of organisation for collaboration. Throughout this paper the permissionless blockchain technology is considered with an example of Bitcoin cryptocurrency[7]. The blockchain is accumulation of numerous technologies like RSA encryption, Merkle tree, distributed computing, game theory and mathematical proof. Blockchain elements and technologies. Following section briefs about the basic elements of blockchain and its technologies.

1.1 Block

Primary element of blockchain is a block, which contains the number of transactions limited to the capacity defined by the respective application. Once the block is validated, it is attached to the latest added block in irreversible chain. Attaching the hash value of previous block to the current block forms the chain of valid transactions as displayed in the Fig.1.1.

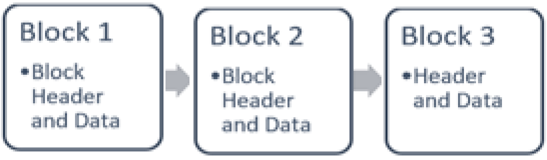

Figure 1.1: Structure of Blockchain

Each block is a combination of block header and data, where block header is used to store metadata of block like the block number, timestamp, hash of previous block, hash of current block, Merkle tree root and mining statistics like nonce and difficulty as mentioned in the Fig.1.2. The data part contains the list of valid transactions added into the block in chronological order. Every block header ties the transactions by Merkle tree root and any alteration in one transaction or even changes in the transactional order can be identified easily, because every block inherits from the previous block[12]. Previous block's hash is included with current block to make the blockchain tamper proof.

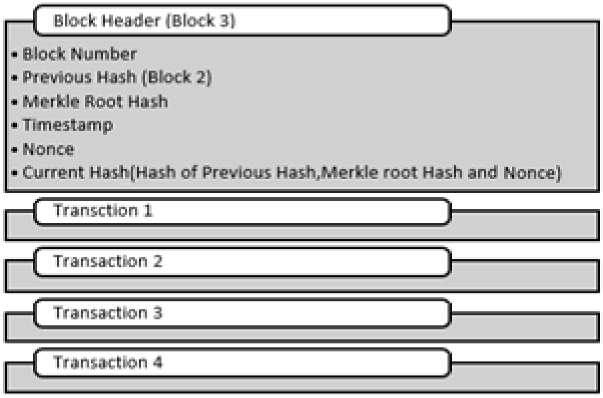

Figure 1.2: Structure of a Block

1.2 Merkle Tree

Merkle tree is used to enable secure verification of large amounts of data in efficient manner. A Merkle tree summarizes the transactions and produces the digital fingerprint for all the transactions included in that particular block. Structure of Merkle tree is a binary tree where every leaf-node stores the hash value of individual transaction and non-leaf nodes stores the hash value of its child nodes. Transactions are added in chronological order from left most leaf of the tree. The tree is constructed from bottom up by repeatedly hashing pairs of nodes. When the odd number of transactions included in a block, hash value of last transaction will be duplicated. Merkle tree is preferred in many blockchain applications like bitcoin cryptocurrency as it required less storage space, easy and fast computation, reduces data size shared over the network.

1.3 Mining

Miners are playing vital role in blockchain, whose main responsibility is to produce hash for the new block and attach the new block into the blockchain. Each and every active miner records the transactions for predefined duration, validates the transactions, create a new block by calculating hash for the recorded transaction and add the newly created block. Challenge is distributed to all miners and one and only the winner is allowed to add a new block among the multiple miners. The winner of challenge gets the incentive for the computation power spent for the mining process.

Every block contains both block header and data parts as given in the figure. Hash of the current block is calculated by combining the Previous Hash, Merkle Tree Root and Nonce which are stored in the block header as given in the Fig 1.3. The hash of the block header is predefined with number of prefixed zeros to make the competition tougher. The Nonce value is founded by series of hit and trails to get the requisite hash prefix. Defining the number of predefined zero is called as difficulty level and the first miner who computes the hash is called winner of the challenge. Bitcoin cryptocurrency protocol sets difficulty level in every 2 weeks for the challenge to average the number of new block which is 6 blocks per hour.

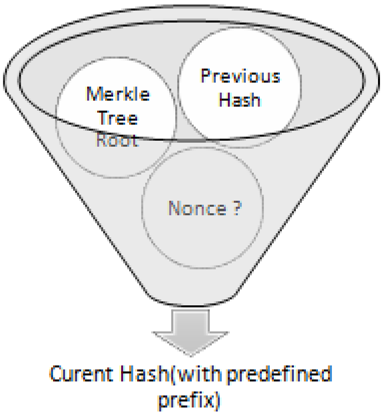

Figure 1.3: Mining Process

1.4 Consensus Algorithm

Consensus mechanism is used to preserve a certain principles or rules within the distributed environment[2]. Since the blockchain is distributed database, consensus algorithm is necessary whenever a new block is appended to the blockchain. Before the new block gets added, the winner who solves the challenge announces that he computed the hash for the given difficulty. All the remaining miners in the network start validating the work done by him and share their views (agreed/not agreed). The new block gets added into blockchain only when a majority of views given are agreed. There are lot of consensus algorithm are available and are discussed in section.

2. Architecture of Blockchain

A blockchain is a distributed ledger where each node is interconnected in the network and agreed with the common conditions. The network grows over the period of time and works independently without central authority where each node acts as a verifier [4]. To participate into this network every user are assigned with Public Key and Private Key using common encryption algorithm. Public key of the user is used as the address for transaction [13]. Fig 2.1 is the given architecture.

User initiates the transaction – End user initiates the transaction included with receiver's address. This transaction is signed by sender's private key and this digital signature is a finger print of the transaction. The Transactional data is broadcasted to all the participants in the network along with digital signature.

Transactions are added into the block – Every miner start adding the transactions into a block for the particular period of time. Miners spend his computation power to find the predefined hash prefix(puzzle) by combining the previous hash, current Merkle tree root, nonce. The nonce value gets incremented and modified until the prefix found.

Challenge winner broadcast the block – The miner who solved the puzzle broadcast the new block hash as proof of work into the network for validation.

Other miners validate the new block– The remaining miners validate the transactions and approve it.

Verified block added into blockchain – All the active nodes attach this new block into the latest added block in the blockchain.

Transaction process completed – The transaction gets executed and completed once the block is attached.

3. Elliptic Curve Cryptography

Generally public key cryptography will be implemented using integers or any polynomial equations which enforces a significant load in storing and analysing particular message and key. In the polynomial equation category, it provides same level of security with smaller size in key. ECC (Elliptic Curve Cryptography) uses the public key cryptography method. It is based on the use of elliptic curves over finite fields. ECC has both private key and public key. Both types of keys are based on the use of asymmetric algorithms one key for encryption and one key for decryption. These key pairs are created using Elliptic Curve Digital Signature Algorithm(ECDSA)[3].

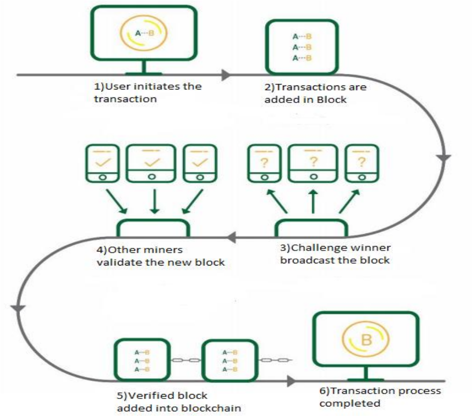
1)User initiates the transaction
2)Transactions are added in Block
4)Other miners validate the new block
3)Challenge winner broadcast the block
5)Verified block added into blockchain
6)Transaction process completed

Figure 2.1: Architecture of Blockchain

The public key is a point on the curve and the private key is a random number. The public key is obtained by multiplying the private key with a generator point in the curve. The Equation(1) is the curve equation.

$$y^2 = x^3 + ax + b \qquad (1)$$

Elliptic curve will have points which will satisfy the above equation. ECC private key is used for the creation of digital signature and it is 256 bit integer where as ECC public key is used for the verification of the digital signature and it is calculated by the private key but private key cannot be found from the private key[5].

3.1 Working of ECCDSA

Suppose a sender wants to send a signed message to the receiver. Firstly, both of them should agree with some parameter of the curve such as (curve, n, g), whereas curve is the equation of the ECC, n is g’s multiplicative order and g is the base point of the elliptic curve such as (x_0, y_0).

3.1.1 Creation of signature

To sign a message m, sender does the following steps:

1) Calculate e= $Hash(m)$, where HASH is a cryptographic hash function, such as SHA-2.
2) Let *z* be the L_n leftmost bits of *e*, where L_n is the bit length of the group order [1, n-1].
3) Select a cryptographically secure random integer *k* from [1, n-1].
4) Calculate the curve point (x_1, y_1)=*k**g.
5) Calculate r=$x_1\ mod\ n$. If ,*r*=0 go back to step 3.
6) Calculate *s*=$k^{-1}(\,z + rd_a)mod\ n$. If , *s*=0 go back to step 3.
7) The signature is the pair (*r*, *s*).

3.1.2 Verification of Signature

a) To authenticate the sender’s signature, receiver authenticates the signature. To do that he must have duplicate public key curve point q_a and verifies as follows:

1) Check whether q_a is not equal to the identity element *O*, and its coordinates are otherwise valid.
2) Check whether q_a lies on the curve
3) Check whether n*q_a=*O*.

b) After that, Bob follows these steps:

1) Verify that *r* and *s* are integers in [1, n-1]. If not, the signature is invalid.
2) Calculate e= $Hash(m)$, where HASH is the same function used in the signature generation.
3) Let *z* be the L_n leftmost bits of *e*.
4) Calculate *w* =$s^{-1}mod\ n$
5) Calculate *w* = *zw mod n* and *w* = *rw mod n*.
6) Calculate the curve point $(x_1, y_1) = u_1 * g + u_2 * q_a$. If$(x_1, y_1)$ =*O*,then the signature is invalid.
7) The signature is valid if *r* =$x_1 mod\ n$, invalid otherwise.

Commonly used algorithm for certificates is RSA-keys. But the recommended size of the key will grow to maintain the strength of sufficient certificate and cryptography. However, ECC brings the same level of cryptographic strength, while keeping the keys much smaller, what allows to increase security and reducing the computational requirements. The most important difference in ECC from RSA is the key size compared with the cryptographic resistance. ECC provides the same cryptographic strength as the RSA-system, but with much smaller keys. For example, a 256-bit ECC key is the same as 3072-bit RSA key (which are 50% longer than the 2048-bit keys used today). Finally, the most secure symmetric algorithms used in TLS (for example, AES) uses a minimum of 128-bit keys, so that the transition to asymmetric keys seems very reasonable.

4. Hashing

Hashing is a process of converting a message in to a hash value. This hash value will consist of letters and numbers, which is also called as message digest. It takes arbitrary length of input and fixed size length of output. Hashing is a one way function where once the message digest is created, using the same message digest original message cannot be driven. Due to this property, it has been used by blockchain network for secure storing of sensitive data. In blockchain, each block which consist of many transaction have to hashed. This hashing will be done by the miners in the network. Based on who is solving the challenges given, will get the block for hashing. Even though many Secure Hashing Algorithms exists for hashing. SHA-1 and SHA-2 are two different versions of that algorithm.SHA 256 which is a subset SHA-2 is highly used in the blockchain. Each SHA differs from the length of signature bit and also the construction. SHA-2 is the enhanced version of SHA-1. SHA-2 hashing is used to hash bulks of transaction i.e., whole blocks in the blockchain. Consequently, any hash value will be used to point the previous hash value in the chain of block.

4.1 Merkle Tree

Merkle tree is a tree in cryptography which is consist of leaf node and non leaf node[11]. Leaf node consist of the hashed value of the data such as a transaction and it is labelled as leaf node. Non leaf node consist of the hashing of the labels of its child node. As shown in Fig.5.

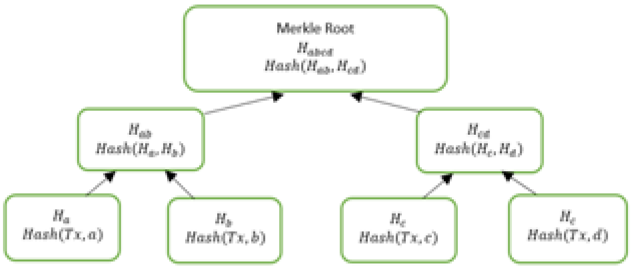

Figure 5: Merkle tree and Formation of Merkle root

The data structure is maintained to track and consolidate the transaction in the whole blockchain. Generally, it is inefficient to store processed data about all past transaction. So only some of the transaction and its information is maintained in the form of Merkle tree. The top most node in the Merkle tree is the root node which gives the summarized data of all hashed transaction. Also, the integrity is maintained here. It maintains the Avalanche effect, such that a very small change in any node of data, it will affect the information in the root node. It is enough to validate the integrity of each branch in the tree, by reading one branch at a time. It means that each files can be split in to small data blocks such that if any original information is damaged, a small piece of block is enough to validate the whole.

4.2 Hashing inside a Block

SHA 256 is used in two major way in the blockchain network. One is mining and other one is bitcoin address creation. Mining is a process in which among the bitcoin supply protocol, new coin will be introduced[6]. For each blockchain network miners are there. They are eligible to add each block in to previous chain only if challenges are solved that particular miner. Inside each block, which is known as block header is constructed using six parameter which is filled by miner.Those six parameters are mentioned below.

Version: Current bitcoin software's version Previous Block Hash: Hash value of the previous block.
Merkle Root: Hash value that representation all the transaction in the block.
Time Stamp: The block created time.
Target: Algorithm for the block such as Proof of Work(POW).
Nonce: Number of variable used in the POW process.
Merkle root's hash is created by SHA 256 which is added in to the block header. The previous block has is obtained by performing twice SHA to the previous block.

4.3 Creation of Bitcoin Address

To produce a bitcoin address, random number is selected which is known as private key and it is multiplied withelliptic curve to produce a public key. The public key is sent through both SHA 256 and RIPEND160 hashing algorithm which is given in Equation(2), where k = the public key A=bitcoin Address

$$A=RIPEMD160(SHA256(K)) \qquad (2)$$

The shorter address is the major advantageous property where as the hashed version is 160 bit long i.e., bitcoin address, but public key is 256 bit long. It is convenient to use due to the shorter length by the user of blockchain.Base58check encoding is performed in the hashed public key. Base58check encoding compresses the hashing address and check sum is added in order to avoid the address damage or mistyping of bitcoin address.

4.4 Comparison of Consensus Algorithms

Consensus algorithms are used to verify and validate the transaction before the block is appended to the blockchain[8]. Once the blocks added it cannot be modified. Various consensus algorithm are available are given in Table 4.1

Table 4.1: Various Consensus Algorithm and Its Concepts

S. no	Consensus Algorithm	Concept
1	Proof of Work (PoW)	The first miner who solve the difficult puzzle gets rewards and allowed add a new block
2	Proof of Stake (PoS)	Miners gets the chance to add new block based on the fraction of tokens he holds
3	Proof of Activity	Combination of PoW and PoS, where PoW is used to construct a new block with cryptographic puzzle and PoS is used to validate the transactions by group of nodes. Rewards are split into both winner and validators.
4	Proof of Burn	The new block gets added from the miner who spent more tokens from his wallet
5	Proof of Capacity	The chance is given to the miner based on the storage space or computation power he owns
6	Proof of Authority	Validation is done by the specific admin node who owns the authority to accept or reject the transaction
7	Proof of Elapsed Time	Waiting time is distributed to miner randomly before giving the chance
8	Delegated Byzantain Fault Tolerance	66% of nodes participated in consensus select the miner to add a new block
9	Proof of Importance	Miners get the chance based on the miner's support in the past

5. Conclusion

In the evolution of distributed technology, blockchain plays a vital role. The main aim of the blockchain is to transmit digital information such as ledger which is distributed among the users as public ledger. Blockchain starts to aggregate millions of strangers and start to connect them by their consistency and honesty. Due to this, blockchain starts to spread among the world as global economy. Digital ledger consist of transactions are not maintained centrally like bank ledger, instead these ledgers are collected as blocks. These blocks are given to the miners who are connected together. To validate this block, a challenge is given to these miners. One who wins the challenge gets the block for validation. When the winner gives the solution for the challenge, all other miners in the network verify whether it is correct solution or not. If the solution is correct, then that block is added to the chain of blocks and that miner gets the reward for finding the correct solution. To validate the integrity of the ledger, the existing Elliptic Curve Digital Signature Algorithm is used. Transaction inside a blocks are hashed and Merkle tree data structure whereas each transaction are hashed using SHA 256. Consensus is maintained by many protocol but Proof Of Work (POW) is mainly used in bitcoin. Blockchain is mainly used for cryptocurrency. But it can also be used in many application like blockchain finance, smart property, smart contract, asset management. Due to this drastic development in blockchain, future technologies can be implemented through blockchain.

References

[1] Akanksha Kaushik, Archana Choudhary, Chinmay Ektare, Deepti Thomas, Syed Akram.2017, "Blockchain — Literature survey," 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT),pp:2145-2148.
[2] Lakshmi Siva Sankar, Sindhu M, Sethumadhavan.M.2017, "Survey of Consensus Protocols on Blockchain Applications," 4th International Conference on Advanced Computing and Communication Systems (ICACCS),pp:1-5.
[3] Pratyush Dikshit, Kunwar Singh,2017, "Efficient Weighted Threshold ECDSA for Securing Bitcoin Wallet," ISEA Asia Security and Privacy (ISEASP),pp:1-9.
[4] Qi Li, Kenli Li.2018, "Decentration Transaction Method Based on Blockchain Technology," International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS),pp:416-419.
[5] Sachchidanand Singh, Nirmala Sing,2016, "Blockchain: Future of Financial and Cyber Security," 2nd International Conference on Contemporary Computing and Informatics (ic3i),pp:463-467.
[6] Sang-Hyun Lee, Kyung-Wook Shin.2018, "An Efficient Implementation of SHA processor Including Three Hash Algorithms (SHA-512, SHA-512/224, SHA-512/256)," International Conference on Electronics, Information, and Communication (ICEIC),pp:1-4.
[7] Yi Liu , Xingtong Liu, Chaojing Tang, Jian Wang, And Lei Zhang,2018, "Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin," IEEE Access, pp:23261-223270.
[8] Yue Hao1, Yi Li1, Xinghua Dong2, Li Fang1, and Ping Chen,2018, "Performance Analysis of Consensus Algorithm in Private Blockchain," 2018 IEEE Intelligent Vehicles Symposium (IV),pp:282-285.
[9] What is Blockchain? https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348
[10] Cryptography and Blockchain. https://blockchainhub.net/blog/blog/cryptography-blockchain-bitcoin/
[11] Understanding Merkle tree. https://www.codeproject.com/Articles/1176140/Understanding-Merkle-Trees-Why-use-them-who-uses-t
[12] Understanding blockchain technology. https://medium.com/@mattdlockyer/understanding-blockchain-technology-2cb5636823eb
[13] Working of blockchain. https://www.investopedia.com/terms/b/blockchain.asp

Author Profile

S. Banupriya received the M.Tech Degree in Information Technology from SRM IST, Chennai,India 2013. She is currently working as Teaching Associate in SRM Institute of Science and Technologies, India. Her research is focusing on Blockchain technologies and Cryptography.

G. Renuka devi received the M.Tech Degree in Information Technology from Madras Institute of Technology, Anna University, Chennai- India 2018. She is currently working as Teaching Associate in SRM Institute of Science and Technology, India. Her research is focusing on Blockchain technologies and Cloud Computing.