A STUDY ON ALGORITHMS USED IN BLOCKCHAIN APPLICATIONS

Ms. Rashmi Dongre Research Scholar Dept. of Computer Science Tilak Maharashtra Vidyapeeth, Pune
Dr. Vikas Prasad Research Guide Dept. of Computer Science Tilak Maharashtra Vidyapeeth, Pune
Mail: rashmibichkar15@gmail.com ; drvikaspd@gmail.com

Abstract

A blockchain is a distributed database of records, often known as a public ledger, that contains all transactions or digital events that have been completed and shared among various entities. Each transaction in the public ledger is validated by the majority of the system's members. Information can't be deleted once it's been entered. Every transaction ever made is recorded in the blockchain, which is certain and provable. The most well-known example of blockchain technology is Bitcoin, a decentralized peer-to-peer digital currency. The immutability of the stored records is a unique property that sets it apart from previous technology. It employs consensus and cryptographic approaches to achieve immutability. This technology is also known as "Distributed Ledger Technology (DLT)" since the data is kept in distributed nodes. As more scholars and practitioners become interested in blockchain, some are curious about the algorithms that are utilized to execute the technology. A lot of study is being done to better understand the blockchain's adoption and diffusion stages. The details of numerous techniques used to implement blockchain in any domain application are presented in this study.

Keywords: Hashing, immutability, database, cryptography etc

1 Introduction

The goal of blockchain technology is to create a decentralized ecosystem in which no third-party controls transactions or data. In general, the blockchain is a time-stamped sequence of blocks that all participating nodes collectively manage. Blocks are essentially containers that hold transactions together. The blocks are cryptographically linked together: each block is digitally signed and 'chained' to the preceding block by containing the hash value of the previous block. The blockchain provides immutable data storage since new blocks may only be added at the end of the chain.

As a result, several blockchain-based systems enable secure distribution of digital assets among untrustworthy clients. Due to the benefits of distributed data storage and immutable audit trails, blockchain has been applied in a variety of fields. Blockchain has evolved into a highly effective technology. However, if it is applied indiscriminately to use cases without considering the technology's strengths and weaknesses, we will fall short of realizing the technology's entire potential.

This paper presents an overview of various algorithms that are used to implement blockchain technology. This study will give an insight to the new researchers about technology perspective of blockchain and its implementation method

1.1 Blockchain architecture

Like a traditional public ledger, blockchain might be a series of blocks that carry a whole list of transaction records. Figure 1 shows an example of a blockchain for an associate degree. A block has just one parent block if the block header contains a preceding block hash. It's worth mentioning that hashes from uncle blocks (children of the block's forebears) will be retained in the Ethereum network. The genesis block, which has no parent block, is the first block in a blockchain. The internals of blockchain are then explained in detail.

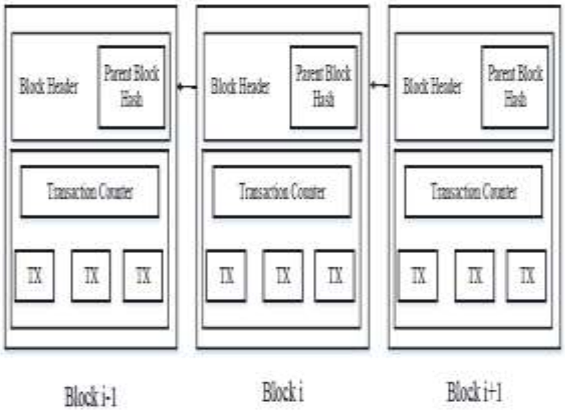

Fig.1 A typical Blockchain

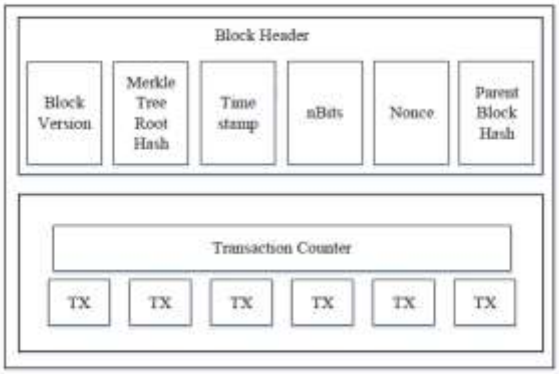

Fig.2 A block in a Blockchain

A block consists of the *block header* and the *block body* as shown in Fig 2. In particular, the block header includes:

(i) *Block version*: It indicates that set of block validation rules to follow.
(ii) Merkle tree root hash: the hash worth of all the transactions within the block.
(iii) Timestamp: current time as seconds in Greenwich Mean Time since Jan one, 1970.
(iv) nBits: target threshold of a legitimate block hash.
(v) Nonce: associate degree 4-byte field that at times, starts with zero and which increase for each hash calculation
(vi) Parent block hash: A 256-bit hash worth that points to the previous block.

2 Literature review

2.1 Blockchain Revolution

The market's enthusiasm for blockchain technologies is expanding, and the tagline "blockchain revolution" is becoming increasingly widespread. The blockchain market is expected to increase from $210 million in 2016 to over $2 billion by 2021, according to estimates. Blockchain technology has the potential to transform the financial industry, supply networks, government record-keeping, and a variety of other industries. The origin of the term, blockchain, has caused some confusion. The term "blockchain" was used to refer to a "chain of blocks of transactions" that was a feature of the Bitcoin system. As a result, in the context of Bitcoin, it referred to a "distributed ledger of transactions." Later, "blockchain" got its own name in media discussions over whether distributed ledgers of transactions could be used for purposes other than Bitcoin. Since its inception in 2009, the Bitcoin system has been successful in preventing fraud on its blockchain, despite the lack of a trusted third party. That is, Bitcoin's blockchain has shown to be "immutable" for all intents and purposes.

As a result, it is frequently referred to as safe. The blockchain of Bitcoin is also open to the public (all transactions are accessible) and permissionless (any computer may participate in validating transactions and adding them to the ledger). The blockchain revolution could provide us with new tools and alter the landscape of certain sectors. However, because the advantages of encryption and smart contracts may be realized without a distributed ledger, the world after the blockchain revolution may very well be a world without the blockchain.

2.2 Blockchain applications

Bitcoin was the first application and use of Blockchain. The financial sector has been the most affected by blockchain technology in the current situation. "Smart Contracts" is another application. The idea of making contracts and agreements smart has been around for a long time, but now it can be achieved thanks to blockchain technology. The fact that finance is the most active user of blockchain is due to the transparency it provides to dealers and businesspeople while dealing and transacting.

Transactions that occur in any entity, whether private or public, can be saved in blocks and their legality afterwards validated. Bringing Blockchain into the mainstream and broadly adopting technology in various sectors, such as elections and banking, can help to eliminate corrupt and malafied procedures and realize the dream of a corruption-free nation.

3 Research methodology

This study refers the secondary data collection and type of research is qualitative. The Secondary data collection includes the published white papers, thesis on blockchain implementation and other sources

4 Research findings

Asymmetric-key algorithms and hash functions are the two types of cryptographic algorithms used in blockchains. Hash functions are employed to give each participant with the capability of a single view of the blockchain. The SHA-256 hashing method is commonly used as the hash function in blockchains.

The practical Byzantine fault tolerance algorithm (PBFT), the proof-of-stake algorithm (PoS), and the delegated proof-of-stake algorithm are all frequent consensus techniques (DPoS). The SHA-256 hash algorithm is used by Bitcoin. This approach produces verifiably random numbers using a predictable amount of computer processing power.

4.1 Asymmetric-key algorithm/RSA Algorithm

Asymmetric-key algorithms, also known as the Rivest-Shamir-Adleman algorithm, are like symmetric-key algorithms in that plaintext is combined with a key, fed into an algorithm, and the result is ciphertext.

As seen in Fig 3, the sender encrypts the communication with the recipient's public key, allowing only the receiver to decrypt it with his or her own private key.

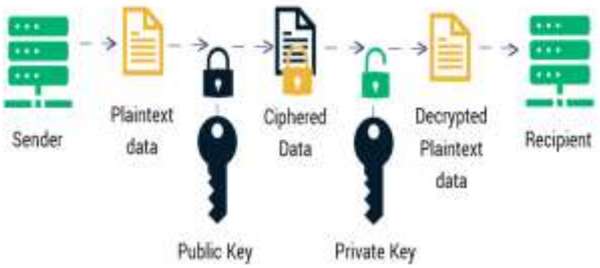

Fig.3 Asymmetric key algorithm

The information is then encrypted using the public key and decrypted using the private key, as in typical asymmetric encryption. The Digital Signature Algorithm (DSA) is used in the DSS, which is an excellent example of asymmetric digital signature authentication.

Asymmetric key algorithms, often known as public key algorithms, are used to tackle two difficulties that symmetric key algorithms are unable to solve: key distribution and nonrepudiation. The first aids in the resolution of privacy issues, while the later aids in the resolution of authenticity issues.

4.2 Hash function/Hashing algorithm

A hash is a function that satisfies the encrypted demands required for a blockchain computation to be solved. Because it's practically hard to guess the length of a hash if someone were trying to crack the blockchain, hashes are of a constant length. The hashed value will always be the same for the same data. A hash function turns an input data into a compressed numerical value known as a hash or hash value.

Hash functions in the mining process

A block is packed and comprises numerous transactions as well as information about the preceding block after being quickly validated on the Bitcoin network. This means that if someone wanted to modify the ledger or double-spend a transaction, they'd have to update the hash in every preceding block, as seen in Fig 4.

Miners must identify a hash that meets the target difficulty for the packaged block to be added to the blockchain. Each block has a block header that provides the block number, the previous block's hash, and a "nonce" that includes a timestamp. A nonce is used to change the input to a cryptographic hash function to increase the randomness of the computation during the mining process.

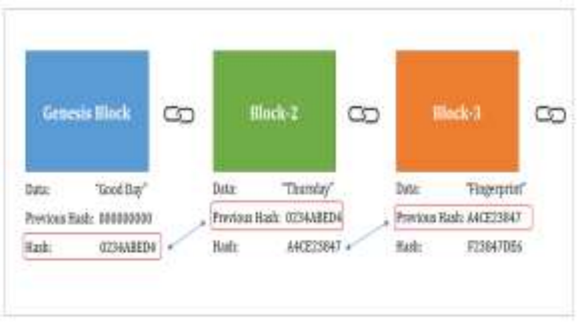

Fig 4 Hashing in Blockchain

Solving the hash

The data is then "hashed" by the node, which converts it into a hash value or "hash," which must always contain a particular number of zeros. The node determines whether a hash meets the difficulty criteria. The hash must begin with the appropriate number of zeroes. If the hash meets the criteria of difficulty, it is disseminated to the other miners in the network. The first miner to find a valid hash converts the block into a new block and is compensated in Bitcoin for the block reward and fees. If the hash fails to match the network difficulty criteria, a new nonce is chosen and hashed. Miners will most likely have to construct many hashes with many nonces before they find one that meets the difficulty.

Bitcoin mining is a time-consuming and energy-intensive operation that necessitates a lot of computing power. The Proof of Work process relies heavily on hash functions. The blockchain would not be tamper-proof and inalterable without confirmation and production of hash transactions, and it would be impossible to verify who possessed how much Bitcoin at what moment.

4.3 Consensus Algorithm

A consensus algorithm is a method through which all peers in a Blockchain network reach a consensus on the current state of the distributed ledger. The goal of a consensus algorithm is to identify a common accord that benefits the entire network.

As demonstrated in fig 5, the consensus procedure entails first establishing a process for validating, verifying, and confirming transactions, then recording the transactions in a vast, distributed directory, building a block record (a chain of blocks), and finally implementing a consensus protocol.

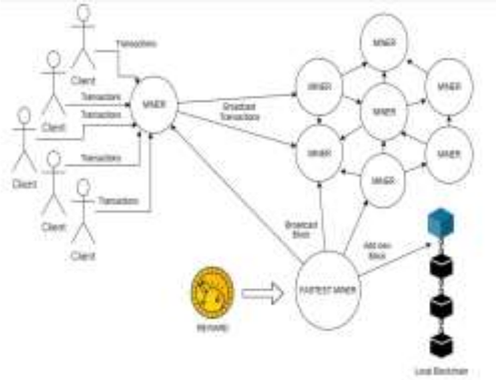

Fig.5 Consensus Algorithm mechanism using PoW

Transaction rules, transaction statuses, and Bitcoin values are all part of the Bitcoin consensus [4]. It's an agreement on the rules that determine whether blocks and transactions are valid or not, on which transactions have occurred, and on the fact that bitcoins have value and that players desire to take bitcoins as payment.

A long list of consensus processes that must be ranked. The greatest of the others are Byzantine Fault Tolerance (BFT) and Ripple Protocol Consensus Algorithm (RPCA). They only account for around 4% of the market capitalization. All the others make up roughly 2% of the total. Most blockchain projects employ one of three consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), or Delegated Proof of Stake (DPoS) (DPoS)

PoW:

Proof of work (PoW) is a method of adding fresh blocks of transactions to the blockchain of a cryptocurrency. In this example, the job is creating a hash (a long string of characters) that matches the desired hash for the current block (see fig 6).

Proof of work is a consensus process that ensures network users, known as miners, generate acceptable alphanumeric codes referred to as hashes to verify Bitcoin transactions and add the next block to the blockchain.

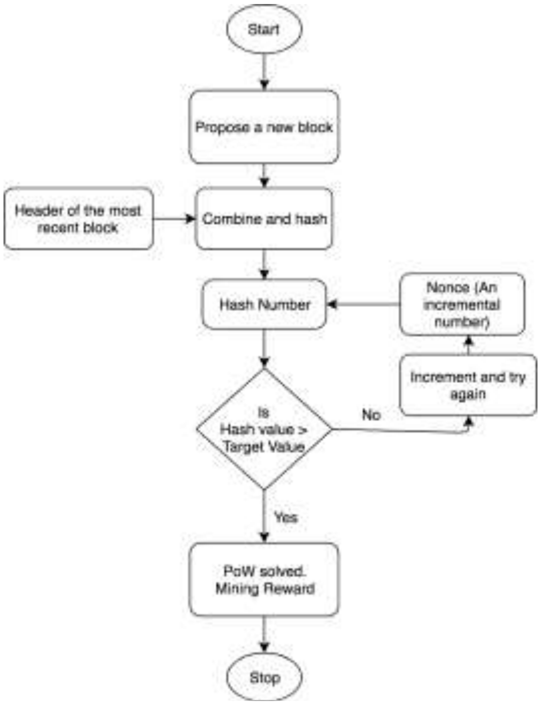
Start
Propose a new block
Header of the most recent block
Combine and hash
Hash Number
Nonce (An incremental number)
Increment and try again
Is Hash value > Target Value
No
Yes
PoW solved. Mining Reward
Stop

Fig 6. Proof of Work mechanism

PoS:

Proof of stake is a type of consensus mechanism used to validate cryptocurrency transactions. With this system, owners of the cryptocurrency can stake their coins, which give them the right to check new blocks of transactions and add them to the blockchain. Proof-of-stake minimizes the amount of computational labor required to verify blocks and transactions, ensuring that the blockchain, and therefore a cryptocurrency, remains secure. Proof-of-stake modifies the way blocks are confirmed using coin owners' devices. A coin owner must "stake" a certain number of coins to become a validator.

Delegated Proof of Stake (DPoS):

Delegated Proof of Stake (DPoS) is a popular variant of the Proof of Stake (PoS) idea, in which network users vote and elect delegates to validate the next block. You can vote on delegates using DPoS by putting your tokens into a staking pool and attaching them to a specific delegate. Delegated proof of stake (DPoS) is a sort of blockchain consensus technology that allows users to vote for multiple delegates using their currency. Once elected, these delegates have the authority to make important choices that affect the entire network.

The DPos system is kept running by an election system that selects nodes to validate blocks. "Witnesses" or "block makers" are the terms used to describe these nodes. BitShare is a decentralized exchange that was founded by Daniel Larimer himself (DEX). EOS, Lisk, Arky Tron are among of the other projects that utilize DPoS. All these blockchains have one thing in common: they're all scalable.

4.4 SHA256 Algorithm

The Secure Hashing Method (SHA) -256 is the Bitcoin protocol's hash function and mining algorithm, referring to a cryptographic hash function that returns a 256-bit number. As demonstrated in fig 6, it regulates the creation and management of addresses, as well as transaction verification. Every item of data generates a unique hash that is completely indistinguishable from that of any other piece of data.

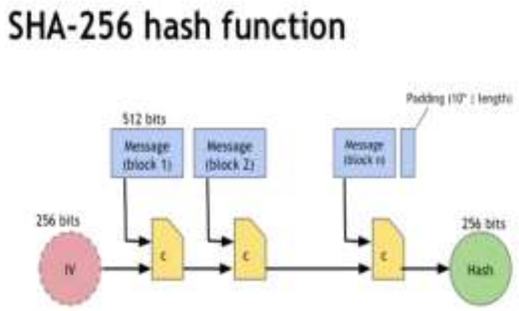

Fig.6 SHA 256 algorithm

V Conclusion

Apart from finance, blockchains have the potential to transform a variety of industries. The algorithms utilized to implement blockchain technology are described in this paper. It also highlights the algorithms' methods and relevance in the context of blockchain implementation.

References

[1] Malin Fiedler, Philipp Sandner, "*Identifying Leading Blockchain Startups on a worldwide level*", FSBC Working Paper, Frankfurt School, Blockchain Centre, December-2017

[2] Debabrata Ghosh, Albert Tan W. K, "*A Framework for Implementing Blockchain to Improve Supply Chain Performance*", MIT Global Scale Network Working Paper Series, Malaysia Institute for Supply Chain Innovation

[3] Rajesh Sharma, Rajhans Mishra, "*A Review of Evolution of Theories and Models of Technology Adoption*", IMJ, Volume 6, Issue 2, December-2014

[4] Uri Klarman et al, "*A Scalable Trustless Blockchain Distribution Network*", BLOXROUTE LABS, WHITEPAPER, VER. 1.0, MARCH 2018.

[5] Iuon-Chang Lin, Tzu-Chun Liao, "*A Survey of Blockchain Security Issues and Challenges*", International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017

[6] A.V. Bogucharskov, I.E. Pokamestov, et al, "*Adoption of Blockchain Technology in Trade Finance Process*", Journal of Reviews on Global Economics, 2018, 7, 510-515

[7] Franziska Wahl, "*Adoption of Blockchains – A Cross Cultural Comparison*", Thesis Submitted to DMCC (Dialogue Marketing Competence Centre), UNI Kassel Versitat

[8] Francesco Parino, Mariano G. Beiró, "*Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption*", EPJ Data Science (2018) 7:38, https://doi.org/10.1140/epjds/s13688-018-0170-8

[9] Chibuzor Udukwo, Aleksander Kormiltsyn, "*An Exploration of Block chain enabled Smart-Contracts Application in the Enterprise*", Technical Report published by Research gate, https://www.researchgate.net/publication/326060734, June 2018

[10] Yitong Zhou, " *Announcement effect of Blockchain investment on stock prices for Financial Companies*", 11th IBA Bachelor Thesis Conference, July 10th, 2018, Enschede, The Netherlands. Copyright 2018, University of Twente, The Faculty of Behavioral, Management and Social sciences.