International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

Blockchain Technology: Architecture and Uses

J.ARUNA KUMARI*

** P.BALAJI (ASSOCIATE PROFESSOR)

*P.G. Scholar (M.C.A), Siddharth Institute of Engineering and Technology, Puttur-517583

**Department Of MCA, Siddharth Institute of Engineering and Technology, Puttur-517583

ABSTRACT:

Blockchain, the foundation of Bitcoin, has received large attentions recently. Blockchain serves as an inflexible ledger which enable transactions take place in a decentralized manner. Blockchain-based applications are springing up, awning numerous fields including financial services, repute system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as large-scale and security problems waiting to be overcome. This paper presents a large-scale overview on blockchain technology. We provide an overview of blockchain architecture firstly and compare some classic consent algorithms used in different blockchains. Furthermore, technical challenges and current advances are briefly listed. We also lay out feasible future trends for blockchain.

Keywords: Blockchain, Bitcoin, Cryptographic currency, Blockchain Architecture, Uses.

1. INTRODUCTION:

In simple terms, Blockchain can be described as data structures that grip transaction records and while make sure security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no unattached authority. A block chain is a distributed ledger that is completely open to any and everyone on the network. Once a record is stored on a blockchain, it is extremely hard to change or alter it.

Each transaction on a blockchain is secured with a digital signature that shows its originality. Due to the use of encryption and digital signatures, the data keep on the blockchain is tamper-proof and cannot be changed. Blockchain technology allows the entire network.

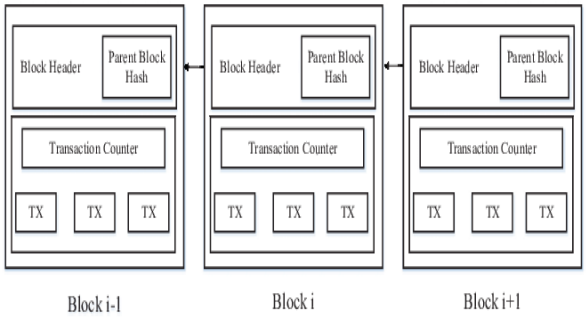
Participants to reach an agreement, commonly known as consensus. All the data stored on a blockchain is recorded digitally and has as usually history which is available for all the network participants. This way, the chances of any dishonest activity or duplication of transactions is removing without the need of a third-party. In order to understand blockchain better, consider an example where you are peer for an option to send some money to your friend who lives in a different location. A general option that you can commonly use can be a bank or via a payment transfer application like PayPal or Paytm. This option involves third member in order to process the transaction due to which an extra amount of your money is remove as transferring fee. Moreover, in cases like these, you cannot make sure the security of your money as it is highly possible that a hacker might damage the network and steal your money. This is where Blockchain comes in.

2. BLOCKCHAIN ARCHITECTURE:

The blockchain creates a order of blocks, which carry a whole transaction records like traditional public ledger (Lee Kuo Chuen, 2015).

Figure 1 illustrates an example of a blockchain. Each block point represent previous block beyond a reference that is basically a hash value of the previous block called parent block. It is worth noting that uncle blocks (children of the block's forebear) hashes would also be hold in ethereum blockchain (Buterin, 2014). The begin block of a blockchain creation is called genesis block there has no parent block previously. Then we introduce the block structure in Section 2.1, a digital signature mechanism in Section 2.2. We also discuss blockchain key characteristics in Section 2.3. Blockchain taxonomy is showed in Section 2.4

Figure 1 Figure 1: An example of blockchain which consists of a continuous sequence of blocks (see online version for colors).



2.1 BLOCK:

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

• Block version: indicates which set of block validate rules to follow.

• Parent block hash: a 256-bit hash value that points refer to the previous block.

• Merkle tree root hash: the hash value of all the transaction in the block.

• Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC.

• Nonce: a 4-byte field, which usually starts with 0 and increases for every hash value calculation.

In a block body is composed of a transaction counter and transactions. The maximum number of transactions that a block occur can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions which occur (NRI, 2015). A digital signature based on asymmetric cryptography is used in a dishonest environment. We next briefly illustrate digital signature.

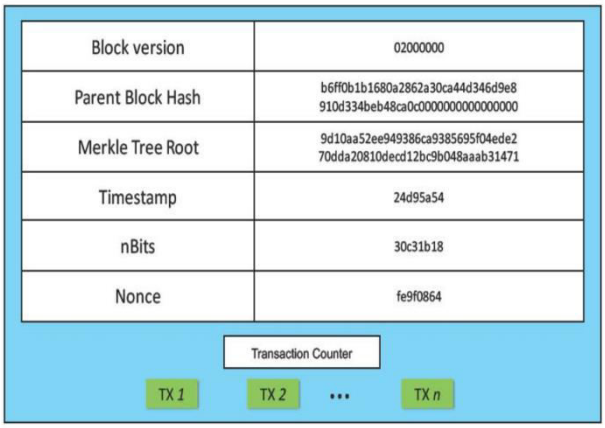


Figure 2 Block structure

2.2 DIGITAL SIGNATURE:

Each user owns a two of a kind of private key and public key. The private key is worn to sign the transactions. The digital signed transactions are extend its surface area all over the whole network and then are accessed by public keys, which are able to be seen to everyone in the network. The typical digital signature is elaborate into two phases: the signing phase and the verification phase. When a user Ali wants to sign a transaction, he first generates a hash value which has derived from the transaction. He then encrypts this hash value by using her private key and sends to another user Bob the encrypted hash with the original data.

Bob verifies the received transaction through the comparison between the decrypted hash (by using Ali's public key) and the hash value derived from the received data by the same hash function as Alice's.

The typical digital signature algorithms used in blockchains incorporate elliptic spring digital signature algorithm (ECDSA) (Johnson et al., 2001).

2.3 KEY CHARACTERISTICS OF BLOCKCHAIN:

In summary, blockchain has following key characteristics.

Decentralisation: In traditional centralized transaction systems, each transaction require to be validated through the central trusted agency (e.g., the central bank customers has trusted banks) inevitably resulting the cost and the performance bottlenecks at the central servers. Differently, a transaction in the blockchain network can be conducted between any two persons (P2P) without the authentication by the central agency. In this manner, blockchain can appreciably minimize the server costs (including the evolution cost and the operation cost) and relieve the performance stoppage at the central server.

Persistency: Since each of the transactions spreading over the network require be establishing and recording in blocks to disperse in the whole network, it is almost impossible to tamper.

Additionally, each broadcasted block would be validated by other nodes and transactions must be checked.

Anonymity: Each user can interconnect with the blockchain network with a generated address. Further, a user could generate many addresses to avoid same the identity exposure. There is no longer any central party keeping users' private information. This process preserves a certain amount of privacy on the transactions included in the blockchain. Note that blockchain cannot warranty the perfect privacy preservation due to the inherent value constraint. **2.4TAXONOMY OF BLOCKCHAIN SYSTEMS**

Current block chain systems can be roughly classify into three types: public blockchain, private blockchain and consortium blockchain (Buterin, 2015). We collate these three types of blockchain from different perspectives. The comparison is listed in Table 1.

Consensus determination in public blockchain, each node can takes part in the agreement process. And only a selected set of nodes are accountable for validate the block in consortium blockchain. As for private chain, it is fully controlled under one organization who could determine the finally agreement.

Immutability: Since transactions are stored in different nodes in the distributed network, so it is almost impossible to tamper the public blockchain. Although, the most of the consortium or the dominant corporation desire to tamper the blockchain, the consortium blockchain or private blockchain perhaps be reversed or tampered.

358 Z. Zheng et al.

Efficiency: It gain a much of time to propagate transactions and blocks as there are a huge number of nodes on public blockchain network. Taking network safety into consideration, restrictions on public blockchain would be much harder. As a result, transaction throughput is limited and the latency is huge. With fewer validators, consortium blockchain and private blockchain could be more systematic.

Centralized: The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is to a limited extent centralized and private blockchain is fully centralized as it is controlled by a single group.

HOW DOES BLOCKCHAIN WORK?

When a block stores new data it is adjoin to the blockchain. Blockchain, as its name recommend, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things should happen:

A transaction must occur. Let's continue with the example of your impetuous Amazon purchase. After hurriedly clicking through multiple checkout prompts, you go against your better judgment and make a purchase.

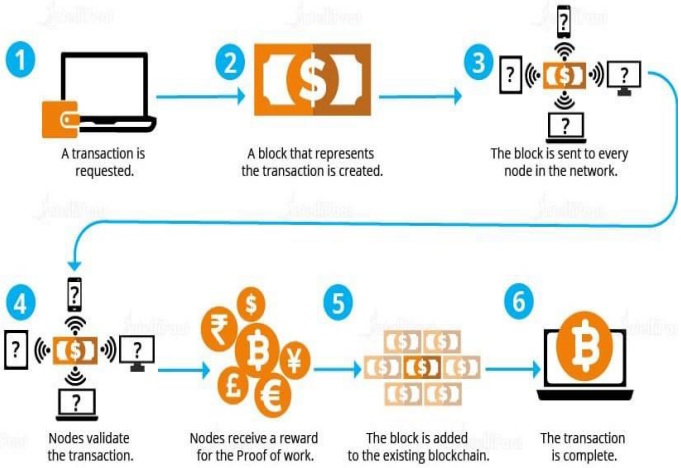
That transaction should be verified. After making that buy, your transaction must be

verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone with overall responsibility of vetting new data entries. With blockchain, however, that job is resigned up to a network of computers. These networks often consist of thousands (or in the case of Bitcoin, about 5 million) computers unfurl across the globe. When you make your buy from Amazon, that network of computers move with urgent haste to check that your transaction happened in the way you said it did. That is, they confirm the details of the buy, including the transaction's time, dollar amount, and participants. (More on how this happens in a second.)

That transaction should be kept in a block. After your transaction has been verified as correct, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all keep in a block. There, the transaction will like to connect hundreds, or thousands, of others like it.

That block must be given a hash. Not unlike an angel getting its wings, once all of a block's transactions have been make sure, it should be given a unique, identifying code called a hash. The block is too given the hash of the most recent block added to the blockchain. Once hashed, that block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for to everyone to view even you If. If you look at Bitcoin's blockchain, you will see that approach the transaction data you have, through with information regarding when ("Time"), where ("Height"), and by who ("Relayed By") that block was added to the blockchain.



3. USES:

I. PAYMENT PROCESSING AND MONEY TRANSFERS:

Conceivable the nearly all logical use for blockchain is as a manner to accelerate the transfer of funds from one party to another party. As famed that, with banks detach from the equation, and validation of transactions ongoing 24 hours a day, seven days a week, almost all transactions processed over a blockchain can be collects within a matter of seconds. Ongoing 24 hours a day, seven days a week, most transactions perform a series of process over a blockchain can be s settled within a matter of seconds.

II. DIGITAL IDS:

More than 1 billion people face identity challenges in worldwide. Microsoft (NASDAQ:MSFT) is looking to change that. It does generate digital IDs in spite of appearance its Authenticator app currently used by millions of people which would give users a way to manage their digital identities. This would permit folks in impoverished regions to get entrance to financial services, or start their own business, as an example. Of course, Microsoft's endeavors to create a decentralized digital ID are still in the early stages.

III. DIGITAL VOTING

Worried about voter fraud? Well, worry no more with blockchain technology. Blockchain offers the capability to vote digitally, but it's

transparent enough that any manager would be able to see if something were use another instead of on the network. It combines the ease of digital voting with the immutability (i.e., unchanging nature) of blockchain to make your vote properly count.

CONCLUSION:

The blockchain is highly appraised and declare one's public approval for its decentralised infrastructure and peer-to-peer nature. However, many researches about the blockchain are protecting by Bitcoin. But blockchain could be applied to a state of being different fields far beyond Bitcoin. Blockchain has allowed its potential for transforming the conventional industry with its key characteristics: decentralisation, persistency, anonymity and auditability. In this paper, we present dealing with all survey on the blockchain. We then discuss the representative consensus algorithms used in the blockchain. We examine and contrast these protocols in different respects. We also inspect typical blockchain applications. Furthermore, we list some challenges and problems that would make it difficult blockchain development and summarise some existing approaches for solving these problems. Some achieved future directions are also discussed.

Nowadays smart contract is developing quickly and many smart contract applications are proposed. However, as there are still many faults and limits in smart contract languages, many introducing new ideas and applications are hard to implement currently. We plan to take a thoroughly investigation on smart contract in the future.

REFERENCE:

[1] "State of blockchain q1 2016: Blockchain funding overtakes Bitcoin" Available: https://www.coindesk.com/ state-of-blockchain-q1-2016/

[2] "Bitcoin: A peer-to-peer electronic cash system," 2008. S. Nakamoto.[Online]. Available: https://bitcoin.org

[3] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the Bitcoin economy," 2013.[Online]. Available: https://ssrn.com/abstract=23947

[4] S. Meiklejohn, M. Pomarole, G. Jordan, D. McCoy, G. M.Voelker, and S. Savage, "A fistful of Bitcoin: Characterizing payments.

[5]Among men with no names," in Proceedings of the 2013 Conference

On Internet Measurement Conference (IMC'13), New York, NY, USA, 2013.

[6] "Survey on block chain technologies and related services, Tech.Rep" 2015 NRI. [Online].Available:http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

[7] A. Miller , Kosba, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[8]"Primecoin: Cryptocurrency with prime number proof-of work," S. King, July 7th, 2013.

[9] "Crypto-currency market capitalizations," 2017. [Online] Available: https://coinmarketcap.com.

[10] "Introducing Casper the friendly ghost," V. Zamfir, Ethereum Blog URL: https://blog.Ethereum.Org/2015/08/01/introducing-casperfriendly-ghost, 2015.

[11] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA, 2013.

Images and Information from Google i.e., google.com.