IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 5, June 2022

Review Paper on Blockchain Technology and Possible Future Directions

Ankit Mishra
Student
Dronacharya College of Engineering, Gurugram, India

Abstract: *Blockchain has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architecture firstly and Taxonomy of blockchain systems. Furthermore, technical challenges and recent advances are listed. We also lay out possible future trends for blockchain.*

Keywords: Blockchain

I. INTRODUCTION

The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency. Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment.

Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services. Those fields favor blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain

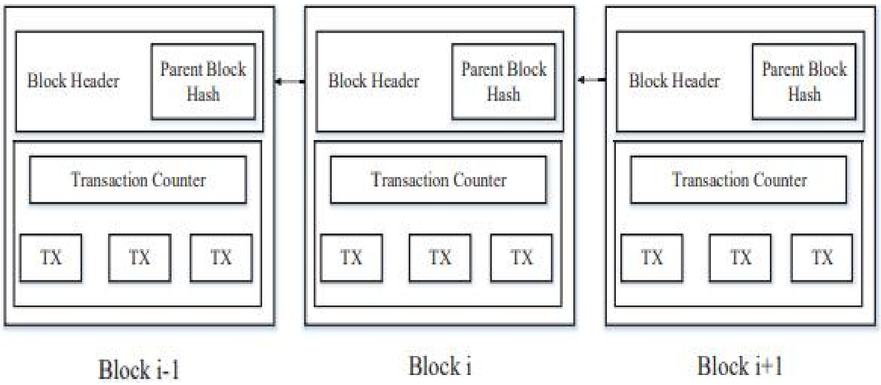

Figure 1: Blockchain Architecture

An example of blockchain which consists of a continuous sequence of blocks.

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [14]. Figure 1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details.

DOI: 10.48175/568

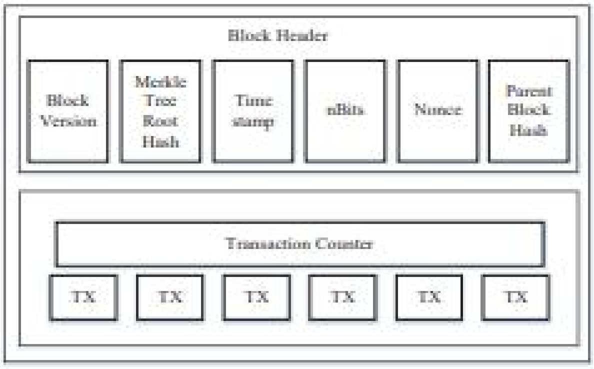

Figure 2. Block Structure

2.1 Block

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

1. Block version: indicates which set of block validation rules to follow
2. Merkle tree root hash: the hash value of all the transactions in the block.
3. Timestamp: current time as seconds in universal time since January 1, 1970.
4. nBits: target threshold of a valid block hash.
5. Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation.
6. Parent block hash: a 256-bit hash value that points to the previous block.

2.2 Digital Signature

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase.

2.3 Imp Characteristics of Blockchain

Majorly, Blockchain has following key characteristics.

- Decentralization - In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.
- Persistency - Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.
- Anonymity - Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint
- Auditability - Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked.

2.4 Taxonomy of Blockchain Systems

Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain

- Consensus determination - In public blockchain, each node could take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for private chain, it is fully controlled by one organization and the organization could determine the final consensus.

- Read permission - Transactions in a public blockchain are visible to the public while it depends when it comes to a private blockchain or a consortium blockchain.
- Immutability - Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered easily as there are only limited number of participants.
- Efficiency - It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain could be more efficient.
- Centralized - The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.
- Consensus process - Everyone in the world could join the consensus process of the public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are permissioned.

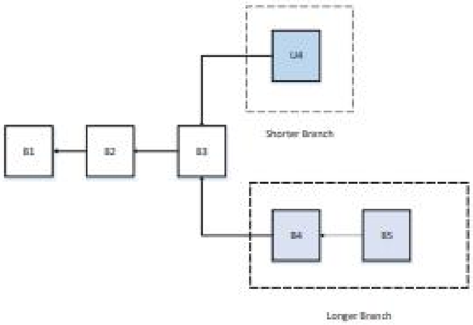

Fig. 3: An scenario of blockchain branches (the longer branch would be admitted as the main chain while the shorter one would be deserted)

III. POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its potential in industry and academia. We discuss possible future directions with respect to four areas: blockchain testing, stop the tendency to centralization, big data analytics and blockchain application.

3.1 Blockchain Testing

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed up to now. However, some developers might falsify their blockchain performance to attract investors driven by the huge profit. Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains

3.2 Stop the Tendency to Centralization

Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network [53]. Apart from that, selfish mining strategy [10] showed that pools with over 25% of total computing power could get more revenue than fair share

3.3 Big Data Analytics

Blockchain could be well combined with big data. Here we roughly categorized the combination into two types: data management and data analytics. As for data management, blockchain could be used to store important data as it is distributed and secure. Blockchain could also ensure the data is original.

DOI: 10.48175/568

3.4 Blockchain Applications

Currently most blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. A smart contract is a computerized transaction protocol that executes the terms of a contract

IV. CONCLUSION

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability.

In this review paper, we present a comprehensive overview on blockchain. We first give an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. We then discuss the typical consensus algorithms used in blockchain.

We analyzed and compared these protocols in different respects. Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed.

REFERENCES

[1]. V. Buterin, "On public and private blockchains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[2]. 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=2394738

[3]. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014

[4]. "Antshares digital assets for everyone," 2016. [Online]. Available: https://www.antshares.org

[5]. Zibin Zheng, Shaoan Xie An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trend

[6]. D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," Stellar Development Foundation, 2015.

DOI: 10.48175/568