IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 3, Issue 1, January 2023
Impact Factor: 5.731

Blockchain Technology: Architecture, Consent, and Expectations Trends

Vaibhav Shewale and Mohd Ahfaz Khan
Sinhgad Institute of Technology, Lonavala, Maharashtra, India

Abstract: *Blockchain, which is the backbone of Bitcoin, has recently received a lot of attention. Blockchain functions as an immutable ledger that enables decentralized transactions. Numerous fields, such as the Internet of Things (IoT), reputation systems, and financial services, are being covered by blockchain-based applications. However, blockchain technology still faces numerous difficulties, such as scalability and security issues, that need to be resolved.*

Keywords: consensus, scalability

I. INTRODUCTION

In today's world, cryptocurrency is a buzzword in both business and academia. Bitcoin has been one of the most successful cryptocurrencies, with its capital market reaching $10 billion in 2016 [1].The Bitcoin network's core technology is blockchain, which was first proposed in 2008 and implemented in 2009 [2]. With a specially designed data storage structure, transactions could take place without the involvement of any third parties. As a public ledger, the blockchain stores all committed transactions in a list of blocks.As new blocks are continuously added to this chain, it gets longer. For the purposes of user safety and ledger consistency, asymmetric cryptography and distributed consensus algorithms have been implemented. The decentralization, persistence, anonymity, and auditability that the blockchain technology typically possesses are fundamental characteristics. Blockchain has these characteristics, which make it capable of significant cost reduction and efficiency enhancement.

Even though the blockchain technology has a lot of potential for building the next Internet systems, it faces a lot of technical problems. First and foremost, scaling is a major concern. The size of a Bitcoin block is currently limited to 1 MB, and a block is mined approximately every ten minutes. As a result, the Bitcoin network can only process seven transactions per second, making it unable to handle high-frequency trading. However, larger blocks entail more storage space and slower network propagation. Because fewer users want to manage such a large blockchain, this will eventually result in centralization. As a result, balancing security and block size has been a difficult task. Second, it has been demonstrated that miners can use a selfish mining strategy to generate more revenue than their fair share [10].To make more money in the future, miners cover up their mined blocks. This allows for frequent branches, which impedes blockchain development. As a result, there must be a solution to this issue. In

addition, it has been demonstrated that privacy leakage can occur in a blockchain even when users only use their public key and private key to transact [11].Additionally, there are significant issues with current consensus algorithms like proof of work and proof of stake. For instance, the process of proof of stake consensus may result in the phenomenon of the rich getting richer, while proof of work wastes too much electricity and energy.

There is a lot of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. [12] made a technical survey about decentralized digital currencies

1.1 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. Merkle tree root hash: the hash value of all the transactions in the block.
2. Timestamp: Current time as seconds in universal timesinceJanuary1,1970.
3. nBits: Target threshold of a valid block hash.
4. Nonce: An 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in SectionIII).
5. Parent block hash: a 256-bit hash value that points to the previous block.

A transaction counter and transactions make up the block body. The block size and the size of each transaction determine the maximum number of transactions that can be contained in a block. Blockchain validates the authenticity of transactions by employing an asymmetric cryptography mechanism [13].In an unreliable setting, digital signatures based on asymmetric cryptography are utilized. The digital signature is then briefly demonstrated.

1.2 Digital Signature

Each user owns a pair of private key and private key The transactions are signed with the private key that must be kept secret. The entire network receives broadcasts of the digitally signed transactions. There are two phases to the typical digital signature: phase of signing and phase of verification. For instance, Alice wants to send a message to Bob, another user.1) Alice sends Bob the encrypted result and the original data during the signing phase after encrypting her data with her private key.2) Bob uses Alice's public key to verify the value during the verification phase. Bob would be able to quickly and easily determine whether or not the data had been altered. The elliptic curve digital signature algorithm (ECDSA) is the typical digital signature algorithm utilized in block chains. [16].

In PoS (Proof of Stake), miners must demonstrate ownership of the currency amount in order to participate in the energy-efficient alternative to PoW. It is hypothesized that individuals with more currencies would be less likely to attack the network. Because the single richest person in the network will always be in charge, the selection based on account balance is extremely unfair. As a result, numerous solutions are proposed that combine the stake size to choose which block to forge. Blackcoin [26] in particular makes use of randomization to anticipate the subsequent generator. It makes use of a formula that takes into account the stake's size and the lowest hash value. Coin age based selection is favored by Peercoin [21].In Peercoin, larger and older sets of coins have a greater chance of being mined for the following block. PoS is more efficient and saves more energy than PoW.Sadly, attacks may occur as a result of the nearly zero cost of mining. Initially adopting PoW, many blockchains gradually transition to PoS. For instance, ethereum intends to switch from Ethash, which is a type of PoW, [27] to Casper, which is a type of PoS, [28].

A replication algorithm that can tolerate byzantine faults is known as PBFT (Practical Byzantine Fault Tolerance) [29].Because the PBFT is capable of handling up to one-third of malicious byzantine replicas, Hyperledger Fabric [18] uses it as its consensus algorithm. A round determines a new block. A primary would be chosen in accordance with certain guidelines in each round. Additionally, it is accountable for arranging the transaction. There are three phases to the entire procedure: committed, prepared, and pre-prepared A node would advance to the next phase in each phase if it received votes from more than two-thirds of all nodes. Therefore, every node in PBFT must be known to the network. Stellar Consensus Protocol (SCP) [30] is a Byzantine agreement protocol as well as PBFT.SCP allows participants to choose which set of other participants to believe, whereas in PBFT, each node must query other nodes. Antshares' dBFT (delegated byzantine fault tolerance) was implemented using PBFT. Some professional nodes in dBFT are chosen by vote to record the transactions. Delegated proof of stake, or DPOS The primary distinction between PoS and DPOS is that PoS is representative democracy while DPOS is direct democracy. Block generation and validation delegates are selected by stakeholders. The block could be confirmed quickly if there were significantly fewer nodes to validate it, which would result in the quick confirmation of transactions. Meanwhile,

The parameters of the network such as *block size* and *block intervals* could be tuned by delegates. Additionally, accepted by the network within a maximum time interval. Within Zero Block, selfish miners cannot achieve more than its expected reward.

II. POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its potential in industry and academic-

We talk about four possible directions for the future: blockchain application, big data analytics, halting the tendency toward centralization, and blockchain testing.

2.1 Blockchain Testing

Over 700 cryptocurrencies have been listed in [52] up to this point, and new types of blockchains have emerged in recent years. However, in order to entice investors motivated by the substantial profit, some developers may falsify the performance of their blockchain. In addition, users must determine which blockchain best suits their needs when integrating blockchain into their businesses. Therefore, a testing mechanism for blockchains must be in place to evaluate various blockchains.

The testing of the blockchain could be broken down into two phases: testing phase and standardization phase. During the standardization phase, each criterion must be created and agreed upon. If a blockchain performs as developers claim, it can be validated by testing it against the established standards. In terms of the testing phase, blockchain testing must be carried out using various criteria. For instance, a user who is in charge of an online retail business is concerned about the throughput of the blockchain. As a result, the investigation needs to test the average time it takes for a user to send a transaction to the blockchain, the capacity for a blockchain block, and so on.

2.2 Stop the Tendency to Centralization

Blockchain is intended to be a distributed system. However, miners are increasingly concentrated in the mining pool. Over 51% of the Bitcoin network's total hash power has been owned by the top five mining pools so far [53].In addition, selfish mining strategy [10] demonstrated that pools with more than 25% of computing power could generate more revenue than their fair share. The selfish pool would eventually attract rational miners, and it could easily reach 51 percent of the total power. Given that the blockchain is not meant to be used by just a few organizations, some solutions to this issue should be suggested..

2.3 Big Data Analytics

Big data and blockchain could work well together. In this section, we roughly divided the combination into two categories: analytics and data management. Because it is distributed and secure, blockchain could be used for data management to store important data. The data's originality could also be guaranteed by blockchain. For instance, if blockchain is used to store patients' health data, the data cannot be altered and it is difficult to steal that private data. Big data analytics could benefit from blockchain transactions when it comes to data analysis. User trading patterns, for instance, maybe extracted. Users can predict their potential partners' trading behaviours with the analysis.

III. CONCLUSION

Due to its key features, blockchain has demonstrated its potential to transform traditional industry: persistency, anonymity, decentralization, and auditability. We provide a comprehensive overview of blockchain in this paper. First, we provide an overview of blockchain technologies, including its architecture and most important characteristics. The usual blockchain consensus algorithms are then discussed.

REFERENCES

[1]. "State of block chain q12016:Block chain funding over takes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1-2016/

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

[3]. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theoryandregulationperspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2646618

[4]. G.ForoglouandA.-L.Tsilidou,"Furtherapplicationsoftheblockchain,"2015.

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

[6]. 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

[7]. Y. Zhang and J. Wen, "An iot electric business model based on theprotocol of bitcoin," in Proceedings of 18th International Conference onIntelligence in Next Generation Networks (ICIN), Paris, France, 2015,pp.184–191.

[8]. M. Sharples and J. Domingue, "The blockchain and kudos: A distributedsystem for educational record, reputation and reward," in Proceedings of11th European Conference on Technology Enhanced Learning (EC-TEL2015),Lyon,France,2015,pp.490–496.

[9]. C.Noyes,"Bitav:Fastanti-malwarebydistributedblockchainconsensusandfeedforwardscanning,"ar Xivpreprintar Xiv:1601.01405,2016.