IJARSCT

ISSN (Online) 2581-9429

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

Impact Factor: 7.301

Volume 3, Issue 3, April 2023

Journal on Blockchain

Avdhi Pagaria[1], Mandvi Thakur[2], Prof. Vandana Kate[3], Prof. Nidhi Nigam[4]

Students, Department of Computer Science and Information Engineering[1,2]
Associate Professor, Department of Computer Science and Information Engineering[3]
Assistant Professor, Department of Computer Science and Information Engineering[4]
Acropolis Institute of Technology and Research, Indore, MP, India
RGPV University, Madhya Pradesh, India

Abstract: *Blockchain is the underlying technology of a number of digital cryptocurrencies. Blockchain is a chain of blocks that store information with digital signatures in a decentralized and distributed network. The features of Blockchain, including decentralization, immutability, transparency and auditability, make transactions more secure and tamper proof. Apart from cryptocurrency, blockchain technology can be used in financial and social services, risk management, healthcare facilities, and so on. A number of research studies focus on the opportunity that blockchain provides in various application domains. This paper presents a comparative study of the tradeoffs of blockchain and also explains the taxonomy and architecture of blockchain, provides a comparison among different consensus mechanisms. In addition, this paper also notes the future scope and highlights the potential of blockchain technology.*

Keywords: Blockchain, Distributed ledger consensus procedures, cryptocurrency, smart contract

I. INTRODUCTION

The term "cryptocurrency" has recently gained popularity in both business and academics. Bitcoin has been one of the most successful cryptocurrencies, with its capital market surpassing $10 billion in 2016. The blockchain, which was first proposed in 2008 and put into use in 2006, is the primary technology used to establish the Bitcoin network and allows transactions to take place without the involvement of a third party. All committed transactions are recorded in a list of blocks, which may be thought of as a public ledger for the blockchain. This chain expands as additional blocks are consistently added to it. For user security and ledger consistency, asymmetric cryptography and distributed consensus algorithms have been used. Decentralization, persistency, anonymity, and auditability are four essential properties of blockchain technology. With these characteristics, blockchain can significantly reduce costs and increase productivity.

Unlike traditional methods, blockchain enables peer-to-peer transfer of digital assets without any intermediaries [1]. Since then, it has seen huge growth with the capital market, reaching 10 billion dollars in 2016. Blockchain is basically a chain of blocks that store all committed transactions using a public ledger [2]. Blockchain was a technology originally created to support the famous cryptocurrency Bitcoin. Bitcoin was first proposed in 2008 and implemented in 2009 by Nakamoto [3]. The chain grows continuously when new blocks are appended to it. Blockchain works in a decentralized environment that is enabled by comprising several core technologies, such as digital signatures, cryptographic hash, and distributed consensus algorithms. All the transactions occur in a decentralized manner that eliminates the requirement for any intermediaries to validate and verify the transactions [4].

The first feature of blockchain is immutability. Once a transaction is stored in a blockchain, it cannot be altered. Blockchain has some key characteristics, such as decentralization, transparency, immutability, and auditability [5]. In addition, because blockchain is distributed, it can prevent single points of failure. When a smart contract is launched on a blockchain, miners may automatically carry it out. Although the blockchain technology offers a lot of potential for the development of future Internet services, there are a number of technical difficulties it must overcome. Scalability is a major concern, to start. A block of bitcoin can only be 1 MB in size right now, and one is mined every 10 minutes or so. As a result, the Bitcoin network can only process 7 transactions per second, making it unable to handle high frequency trading. The blockchain is poised to innovate and transform a wide range of applications, including goods transfer (supply chain), digital media transfer (sale of art), remote services delivery (travel and tourism), platforms for example, moving computing to data sources and distributed credentialing [6].Larger blocks, however, require more storage space

DOI: 10.48175/568

and propagate more slowly over the network. When fewer people are willing to maintain such a big blockchain, this will gradually lead to centralization. Thus, balancing block size and security has proven to be a difficult task. Second, it has been demonstrated that miners might generate more income than their fair share via self-serving mining tactics. Blockchain is a series of blocks that, like a traditional public ledger, contains a comprehensive list of transaction data. A block only has one parent block if the block header contains a preceding block hash. It's important to note that uncle blocks' hashes, or the children of the block's forebears, would also be kept on the Ethereum block chain. A block-Chain's genesis block, which has no parent block, is the very first block. The internals of block-chain are then thoroughly explained.

Further problems with blockchain include interoperability, privacy, energy use, egotistic mining, security, and regulatory policy. The lack of a standardised protocol for business adoption and integration of blockchain-based solutions causes the interoperability issue.

This journal focuses on the most recent research on blockchain technology, covering its architecture, consensus algorithms, applications, trade-offs, and difficulties. This survey paper's remaining sections are structured as follows. Chapter IIintroduces you with bloackchain architecture. Chapter III introduces you with consensus algorithm. The study is concluded in Section IV after Section V examines some potential future steps.

II. BLOCKCHAIN ARCHITECTURE

The technology behind a lot of digital cryptocurrencies is called blockchain. Blockchain is a network of decentralised, distributed blocks used to store information with digital signatures. Transactions are more secure and tamper-proof thanks to the characteristics of blockchain, including decentralisation, immutability, transparency, and auditability. Blockchain technology has applications outside of cryptocurrencies, including risk management, healthcare facilities, and financial and social services. Several studies have focused on the potential that blockchain technology offers in numerous application domains. Once the transaction is verified and validated by the miners, it is included in a block. Peers who use their computational power to mine for blocks are called miners [7]. This paper compares several consensus techniques, describes the taxonomy and architecture of blockchain, and covers obstacles including scalability, privacy, interoperability, energy consumption, and regulatory issues. It also includes a comparative examination of the tradeoffs of blockchain. This paper also discusses the potential applications of blockchain technology in the future. Blockchain, distributed ledger, consensus techniques, cryptocurrency, smart contract, egotistical mining, and energy use are all terms found in the index.

Miner nodes must complete a mathematical puzzle and use enough of their processing power to publish a block. The first miner to complete the riddle successfully wins and gets the chance to add a new block. A little incentive is provided after a new block is successfully created.Double spending refers to using the same input amount for two or more different transactions [8]. A consensus mechanism, a method for a decentralised network to reachconsensus on specific issues, is then used by all the peers in the network to validate the new block. The new block will then be added to the chain that already exists and to each peer's local copy of the immutable ledger. The deal is now officially completed. The next block associates itself with the recently formed block bywith the use of a cryptographic hash pointer.In general, a transaction needs six confirmations in the network to be considered final [9]. The block now receives its first confirmation, and the transaction now receives its second confirmation. The transaction will also be reconfirmed every time a new block is added to the chain.

2.1 Transition process for Blockchain

A Blockchain transaction is a discrete task that is recorded in public databases. Blockchain is the underlying technology of Bitcoin, and it facilitates transactions that occur within a peer to peer global network in a decentralized fashion. That makes Bitcoin a borderless, censorship-resistant digital currency. In general, trust may be the main concern regarding traditional centralized systems, such as a banks, where people need to put their solemn confidence in the system. Bitcoin can take any type of input, such as text, numbers, string or even a computer-generated file of any length, to produce 256 bits or the 64 characters output called hash [10]. This is the sweet spot for public blockchain technology, in that it does not require any trust while handing over the ownership of digital assets from one peer to another.The converted hash result will always be identical given the same input. The term "one-way function" refers to a function where even a little change in the input dramatically alters the result, making it impossible to calculate the input from the output. One can only speculate as to what the input was, and the chances of getting the guess correct are extremely remote, hence it is secure.

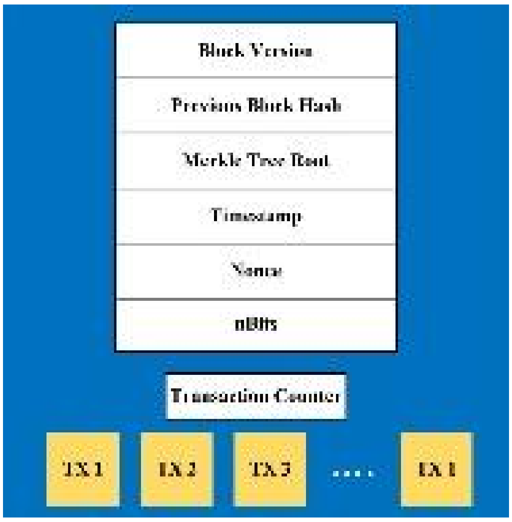
Verifying the sender's identity is the initial stage in the transaction process, indicating that only the sender and not anybody else is requesting the transaction between the sender and the receiver. With the aid of a straightforward example of a transaction between Bob and Alice, Figure 2 illustrates the verification procedure. Assume that both
Bob and Alice both have bitcoin balances, and Alice wishes to give Bob 10 bitcoins.. Transaction validation is carried out independently by all miners based on different criteria that we have discussed later in this section. Elliptic curve digital signature algorithm (ECDSA) is used by blockchain [11]. Currently, transmit theAlice will send a message to the blockchain network with the details of the transaction including money.

Each transaction includes a 256-bit signature. To forge this signature in order to conduct a fraudulent transaction, a hostile peer or attacker would need to guess 2256 cases, which is both infeasible and a waste of resources [12]. The verifier must not only verify the sender's legitimacy but also the transaction's legitimacy, including whether the sender has enough funds to transmit to the recipient or not. That might be done by consulting the ledger, which contains details about each previous successful transaction.

2.2 Block Structure

The Blockchain is made up of a series of blocks that operate as a public ledger-like database for all transactions. These blocks are connected to one another by a reference hash that is a part of the parent block, the block that came before. The genesis block, which has no parent blocks, is referred to as the initial block. The block header and block body make up a block. As demonstrated in Table 1 and Fig. II, the block header contains metadata such as the block version, parent block hash, Merkle tree root hash, timestamp, nBits, and nonce.A transaction counter and transactions make up the block body. Transactions are the list of recorded transactions in the block, and the transaction counter indicates how many transactions have come after.

TABLE 1. Block header attributes.



Depending on the block size and the size of each transaction, a block can contain a maximum number of transactions. Blockchain verifies the authenticity of transactions via an asymmetric cryptography technique. Asymmetric cryptography-based digital signatures are employed in unreliable environments, like the blockchain network. Each participant in this process has a private key and a public key pair. The public key is distributed throughout the network and is available to everyone, whereas the private key is used to sign or encrypt the transaction to decrypt the transaction after that.

2.3 Blockchain Taxonomy

Public, private, and consortium blockchains are the three different types [13]. These systems can be contrasted from several angles, as will be discussed below:

1) Read Permission

Users on public blockchains can read data, however those on private and consortium distributed ledgers can only have limited access. As a result, the business or consortium can determine whether or not the information stored needs to be made available to everyone.

2) Centralized

The primary distinction between these three forms of Blockchain is that the public blockchain is decentralised, whilst the consortium and private blockchains are both partially centralised. Public blockchain can draw a lot of users because it is accessible to everyone. Also, communities are quite active. Every day, new public blockchains are created. Many business applications could be used with the consortium blockchain.

3) Efficiency

Any node can join or leave the network in the public blockchain, which greatly enhances its scalability. The flexible access of new nodes to the network and growing complexity of the mining process, however, have a restricted throughput and rising latency. Yet, private and consortium blockchain can enable improved performance and energy efficiency with fewer validators and elective consensus mechanisms.

2.4 Characteristics of blockchain

1) Persistency

Blockchain provides the infrastructure by which truth can be measured [14] and enables the producers as well as consumers to prove their data are authentic and not altered. For example, if a Blockchain consists of 10 blocks, then block no. 10 contains the hash of the previous subsequent block, and to create a new block, the information of the current block is used. Therefore, all the blocks are linked and connected with each other in the existing chain. Even the transactions are related to the prior transaction. Now, a simple update on any transaction will significantly change the hash of the block. If someone wants to modify any information, he has to change all the previous block's hash data which is considered an astronomically difficult task considering the amount of work that needs to be done. In addition, after generating a block by a miner, it is confirmed by other users in the network. Hence, any manipulation or falsification of data will be detected by the network. For this reason, blockchain is almost tamper proof and considered as an immutable distributed ledgertask, especially in light of the volume of work required. Also, after a miner creates a block, it is verified by other users on the network. Hence, the network will be able to identify any data tampering or falsification. Because of this, blockchain is almost impervious to tampering and is regarded as an immutable distributed ledger.

2) Decentralization

In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank). Therefore, decentralization requires trust, which is the main issue, along with lift resilience, availability and fail over, where the decentralized peer-to-peer blockchain architecture could be a better solution. Unlike a centralized system, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency. In this manner, blockchain can reduce the trust concern by using various consensus procedures. Moreover, it can reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the central server. In contrast, in many cases, blockchain has some tradeoffs. For example, PoW cases such as Bitcoin and Ethereum, the server and energy cost are orders of magnitude higher, while the performance are also several orders of magnitude lower.

3)Auditability

A digital distributed ledger that tracks every transaction made in a blockchain network is verified by aelectronic timestamp. As a result, by gaining access to any network node, it is feasible to audit and trace earlier records [15]. For instance, all transactions in Bitcoin may be tracked repeatedly, facilitating auditability and transparency of the

DOI: 10.48175/568

blockchain's data state. Yet, it becomes exceedingly challenging to track down the source of the money when it is spread across numerous accounts.

4) Anonymity

A randomly generated address can be used to connect with the blockchain network [16]. To prevent his identity from being revealed, a user on a Blockchain network can have many addresses. As it's a decentralised system, nobody in charge is keeping an eye on or collecting user data. Blockchain's trustless environment contributes to some degree of anonymity.

III. CONSENSUS ALGORITHM

The Byzantine Generals (BG) Problem has been transformed into a blockchain problem in order to establish consensus among the unreliable nodes [17]. A group of generals in charge of a section of the Byzantine army circle the city in the BG issue. If only some of the generals attack the city, the attack would fail.

To decide whether or not to attack, generals must consult one another. But among the generals there might be traitors. The traitor might give each general a different decision. This is an unreliable setting. It can be difficult to come to a consensus in such a setting. The decentralised nature of the blockchain network presents another difficulty. Blockchain does not have a central node to maintain distributed ledgers.Every node is the same. Nodes are not required to have mutual trust. Hence, some techniques are required to guarantee the consistency of ledgers across different nodes. Next, we outline a number of popular strategies for achieving blockchain consensus.

1) PROOF OF WORK (POW)

Proof-of-work (PoW) is a consensus algorithm that relies on proofs. The fundamental idea behind the consensus technique is to locate and select the node that will be granted permission to add a new block to the existing chain by supplying the necessarythe consensus algorithm known as proof-of-work (PoW) depends on proofs. The primary goal of the consensus mechanism is to identify and choose the node that will be given authorization to add a new block to the current chain by providing the required information.

The fundamental issue with the PoW strategy is that it requires considerable processing resources from miners to solve the problem and produce a block. Additionally, only one miner will ultimately succeed, which explains why this procedure cannot be sustained. Some PoW protocols with potential side uses have been developed to lessen the loss. Prime coin, for instance, looks for unique prime number chains that can be applied to mathematical study. Proof of burn urges miners to send their coins to addresses where they cannot be redeemed, preventing them from using electricity to mine the PoW block.

2) PROOF OF STAKE (POS)

Proof-of-stake (PoS) can be a more energy-efficient alternative to proof-of-work (PoW). The miner doesn't have to use a lot of computer power to solve the mathematical challenge using this consensus approach. Instead, taking part in the production of blocks depends on having a large enough interest in the system. The stake or wealth of the participating node solely determines the likelihood of being given the chance to validate a block.An adequate stake is thought to prevent the probability of a malicious assault on the network. The competition between the peers is eliminated since the validator is selected according to the stake it holds in the network. As a result, a validator wagers on a block using its stake. The validator gets the fees from the block's transactions if the block is approved.

IV. CONCLUSION

Blockchain is a distributed, P2P technology that offers data protection and immutability. It also has aspects of decentralisation. The creation and use of Bitcoin drives up demand for Blockchain Technology as a security solution. Although BT offers strong data security, the verification and validation of transactions takes a long time. The fundamental attributes of its privacy and security, traceability, and time-stamping have been observed in its acceptance alongside its main application areas. BT can change how individuals establish trust by moving away from relying on outside parties and towards technological means. There is no requirement for communication with third parties or payment of transaction fees to third parties. The openness, freedom from restrictions, and borderlessness of Because BT gives everyone access to the technology, a blockchain network was able to be created using it. Anyone with access to the public blockchain can utilise an electronic wallet for personal or professional purposes. When using an electronic wallet or cryptocurrency, we must undertake the CPU and GPU-intensive mining operation that produces the coins. The blockchain technology is constrained by the extensive time and energy needs for comprehensive verification. In the future, we'll work on it and make an effort to cut the computing time and energy required for the mining and verification processes.

V. FUTURE SCOPE OF BLOCKCHAIN TECHNOLOGY

Blockchain, in the opinion of the researchers, has enormous promise in both academia and business. We have briefly covered the various potential applications of blockchain technology in this area, including standardisation, asset protection, big data, and smart contracts. Blockchain performance to entice investors with the prospect of enormous profits. Before incorporating this technology into a business solution, it is essential to understand whether it satisfies the criteria. As a result, there has to be a common testing procedure for blockchain-based solutions to assess both their value and their trade-offs. The standardisation and testing steps of this procedure can be divided into two categories. Based on a set of predetermined criteria, the initial phase will validate developers' claims on their blockchain-based solutions. The testing phase is used to evaluate how well the blockchain-based solution works. For instance, the operation of the blockchain-based system is important to the owner of an online retail company. Therefore, the throughput, capacity, and latency of the platform used for the acquired solution should be tested and standardized. Blockchain technology enables businesses to keep a digital record of their discoveries and can produce a certificate after registering new ideas, proof-of-concepts, and designs that might demonstrate the legitimacy, existence, and ownership of any intellectual property (IP) asset. All notarized information, including trade secrets and copyright claims, might be kept private and secure by using the special cryptography layer. Blockchain-based smart contracts can be used in a variety of contexts, including banking services and IoT platforms. There are two categories of smart contract research: development and evaluation. The creation of a platform for smart contracts is possible. Car auctions, online trade, and other solutions based on smart contracts are all possible thanks to Ethereum's architecture. Evaluation includes code analysis and performance. It has been predicted that even a minor error in creating smart contracts could have catastrophic results. The DAO hack, when over $60 million in funds were taken as a result of the recursive call flaw, might serve as the exact illustration. Analysis of the smart contract attacks is crucial as a result. On the other hand, the effectiveness of the smart contract can develop into a crucial research area. More smart contract-based applications would be used as blockchain technology continues to draw significant attention from both the public and private sectors.

REFERENCES

[1]. T. Aste, P. Tasca, and T. D. Matteo, ‘‘Blockchain technologies: The foreseeable impact on society and industry,’’ Computer, vol. 50, no. 9, pp. 18–28, Jan. 2017.

[2]. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ‘‘Blockchain for AI: Review and open research challenges,’’ IEEE Access, vol. 7, pp. 10127–10149, 2019.

[3]. S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System. Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[4]. A. Litke, D. Anagnostopoulos, and T. Varvarigou, ‘‘Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment,’’ Logistics, vol. 3, no. 1, p. 5, Jan. 2019.

[5]. M. Kouhizadeh and J. Sarkis, ‘‘Blockchain practices, potentials, and perspectives in greening supply chains,’’ Sustainability, vol. 10, no. 10, p. 3652, Oct. 2018.

[6]. F.Casino, T.K.Dasaklis, and C.Patsakis, ‘‘A systematic literature review of blockchain-based applications: Current status, classification and open issues,’’ Telematics Inform., vol. 36, pp. 55–81, Mar. 2019.

[7]. J.A.Kroll, I.C.Davey, andE.W.Felten, ‘‘the economics of bit coin mining, or bitcoin in the presence of adversaries,’’ in Proc. WEIS, Jun. 2013, p. 11.

DOI: 10.48175/568

[8]. G. Karame, E. Androulaki, and S. Capkun, ‘‘Two bitcoins at the price of one? Double-spending attacksonfastpaymentsinbitcoin,’’IACR Cryptol. ePrint Arch., vol. 2012, no. 248, Oct. 2012.

[9]. M. del Castillo. (2017). Chain is Now Working on Six ‘Citi-Sized’ Blockchain Networks. [Online]. Available: https://www.coindesk.com/ chainnow-working-six-citi-sized-blockchain-networks

[10]. A. Manimuthu, R. V. Sreedharan, R. G, and D. Marwaha, ‘‘A literature review on bitcoin: Transformation of crypto currency into a global phenomenon,’’ IEEE Eng. Manage. Rev., vol. 47, no. 1, pp. 28–35, 1st Quart., 2019.

[11]. Y. Yuan and F.-Y. Wang, ‘‘Blockchain and cryptocurrencies: Model, techniques, and applications,’’ IEEE Trans. Syst. Man, Cybern., Syst., vol. 48, no. 9, pp. 1421–1428, Sep. 2018.

[12]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, ‘‘Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2016, pp. 839–858.

[13]. J. Wang, P. Wu, X. Wang, and W. Shou, ‘‘The outlook of blockchain technology for construction engineering management,’’ Frontiers Eng. Manage., vol. 4, no. 1, pp. 67–75, 2017

[14]. D. Shrier, W. Wu, and A. Pentland, ‘‘Blockchain & infrastructure (identity, data security),’’MassachusettsInst.Technol., Cambridge, MA, USA, 2016, vol. 1, no. 3.

[15]. H. Yu, Z. Yang, and R. O. Sinnott, ‘‘Decentralized big data auditing for smart city environments leveraging blockchain technology,’’ IEEE Access, vol. 7, pp. 6288–6296, 2019.

[16]. Q. Wang, X. Li, and Y. Yu, ‘‘Anonymity for bitcoin from secure escrow address,’’ IEEE Access, vol. 6, pp. 12336–12341, 2018.

[17]. L. Lamport, R. Shostak, and M. Pease, ‘‘The Byzantine generals problem,’’ ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382–401, Jul. 1982