International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 07, 2020
ISSN: 1475-7192

An extensive review on block chain

Ravendra Kumar*, Dhara Upadhyay, Poonam Agarwal, Janvi Rathore

Abstract:

The blockchain technology is the most recent technology in the current monetary system. Blockchain technology arranges blocks separately identified linked transaction history into a chain. As it is a chain it includes the order of blocks. It would be beneficial as it is reliable. Also, it can be making use like assured money transactions, tracing items and make cocksure of data veracity. Blockchain makes it almost impossible to hack transactions. A huge number of industries can benefit from this growing technology as it has the ability to make a cheap cost by gathering the processes and breaking form or paperwork.

Keywords: blockchain, IoT, cryptocurrency, internet of things, smart contract, consensus algorithms, Supply chain, Logistics, Integration, Applications, Literature review.

Introduction:

Blockchain was first introduced by Satoshi Nakamoto with the invention of bitcoin in 2008 and then with its practical implementation in 2009. Transactions between two people or companies are usually centralized and controlled by a third party. In digital payments or currency transfers required a middleman can be a bank or credit card provider to complete the transaction. A transaction from a bank, credit card company or in several other domains like games, software, music etc. Causes a fee. All the data and information are managed by a third party, rather than the entities involved in the transaction.

Block chain Technology:

Blockchain technology is developed to solve this type of issue. Blockchain was considered as the public ledger which stored all the transaction in chain of blocks. All the information is shared and available to all nodes about every transaction in blockchain. The blockchain has many problem-solving features like decentralization, auditability and persistency. In blockchain technology decentralization refers to the transfer of control and decision making from a centralized entity [individual, organization or group] to a distributed network. Decentralized networks try hard to reduce the level of trust that participants must place in one another. The main goal of blockchain technology is to build an environment where the transactions were not in control of third party. The introduction of blockchain was first launched by bitcoin, making it the first application to utilize this innovative technology. Bitcoin established a decentralized environment for cryptocurrency from where the user can buy and exchange goods by digital money. In blockchain technology records cannot be edited without previous records [with the permission of majority of involved party], because of it blockchain technology is safe for business operation. Smart contracts in blockchain are used to track frauds in finance or share medical records between healthcare specialists. Smart contracts are computer programs that are stored on a blockchain and are made to execute automatically when conditions are satisfied. Smart contracts are mainly used to automate the execution of agreements, hence there is no need for intermediaries, and it takes less time to reach a resolution. Smarts contracts can be programmed to automate workflows, activate the next action when conditions are met.

The speed, efficiency, and accuracy of smart contracts are the main benefits. Once a condition is satisfied, the contract is executed immediately. Due to the automated behavior of smart contracts, there is no need for paperwork to process, hence reducing the time spent on reconciling errors that often happens because of manual filling of documents. Transaction records of blockchain technology are encrypted, thereby make them very hard to hack and each record within the distributed ledger is connected to the previous and successive records, so to hack a single block hacker would have to alter the entire chain.

Corresponding Author: Ravendra Kumar

Assistant Professor, Computer Science Engineering, Arya Institute of Engineering and Technology, Jaipur, Raj

Assistant Professor, Computer Science Engineering, Arya Institute of Engineering And Technology, Jaipur, RajScience Student, St. Paul School, Nagaur, Raj

Science Student, Bright Land Jaipur, Raj

Internet of Things (IoT):

The usage of blockchain technology provides a decentralized consensus mechanism, which allows all participants entities to receive update of every event and transaction by generating an unerasable record in public ledger. It has caused notable disruptions in various sectors such as supply chain, real state, operations, banking, electronic health records, insurance, healthcare, music, copyright and renewable energy and is continues to expand its impact and presence in these sectors due to its decentralized, verified, and immutable behavior. There have been multiple examples of SCs undergoing successful transformations through the usage of blockchain technology. However, certain problems appear in terms of usability, security, privacy and cost. Despite these barriers, the usage of blockchain technology shows many benefits in enhancing the functionality and security of digital platforms including internet of things (IoTs) and other technology associated with industry 4.0. have highlighted the positive effect of blockchain technology on these sectors. For diverse requirements, blockchain can be classified into three structures: public (non-permissioned), private (permissioned), and consortium (hybrid). Public blockchain allows all network users to access it and is used through a peer-to- peer network. Private blockchains give role-based data access and utilize cloud networks to increase flexibility. Blockchain has the capability to support social media analytics. Consortium blockchain combines the features of both public and private blockchains, striking a balance between the two. Supply chain management, interbank and international transactions, and decentralized autonomous organizations. These use cases highlight the potential applications of blockchain technology in various industries.

Design of blockchain:

The blockchain is a digital ledger that consists of a sequence of blocks, each of which contains a complete list of transaction records. Each block is linked to the previous block via a hash value, and the first block is called the genesis block.

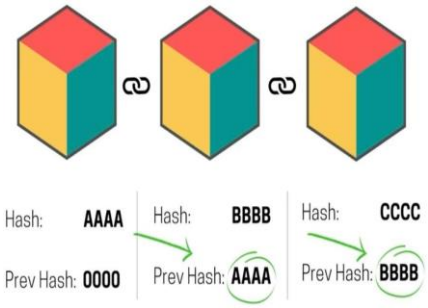


Fig1: Genesis block

Block:

The composition of a block comprises of two essential components, namely the block header and the block body, as illustrated in Figure 2. The block header encompasses various elements, including:

- The block version refers to the specific set of block validation rules that are to be adhered to.
- The parent block hash refers to a 256-bit hash value that serves as a reference to the preceding block.
- The Merkle tree root hash refers to the cryptographic hash value that represents all the transactions contained within a particular block.
- Nonce is a 4-byte field that typically commences with 0 and progressively increments with each hash computation.
- The current hashing target in a compact format is represented by the term 'nibs'.
- The given text can be rephrased as follows: The timestamp is represented as the number of seconds that have elapsed since January 1, 1970, at 00:00 UTC.

Digital signature

In the context of blockchain, each user possesses a private key and a public key. The private key is utilized to sign transactions, which are then distributed throughout the network and accessed by public keys that are visible to all network participants. An example of a digital signature used in blockchain is illustrated in Figure 3, which involves two phases: signing and verification. To elaborate, when a user, such as Alice, intends to sign a transaction, she generates a hash value from the transaction and encrypts it using her private key. The encrypted hash, along with the original data, is then sent to another user, such as Bob. Bob verifies the transaction by comparing the decrypted hash, which is obtained using Alice's public key, with the hash value derived from

They received data using the same hash function as Alice's. The digital signature algorithms commonly employed in blockchains include the elliptic curve digital signature algorithm (ECDSA) (Johnson et al., 2001).

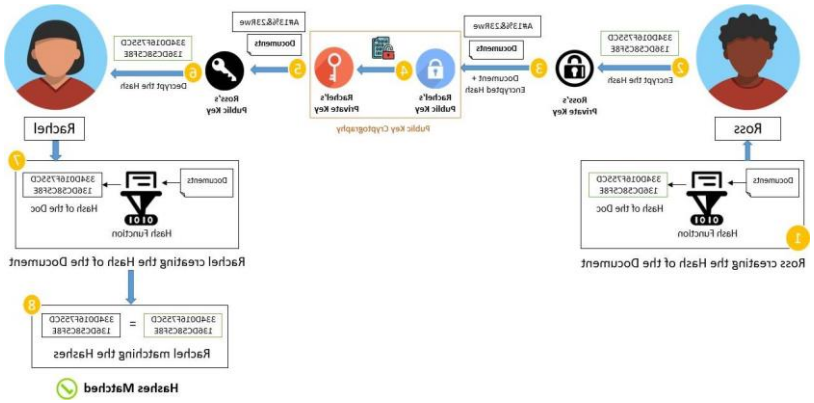


Fig 2: Flow chart

Features of blockchain

blockchain has following features.

- Decentralization: - In conventional centralized transaction systems, the validation of each transaction is reliant on a central trusted agency, such as the central bank. This process inevitably leads to both cost and performance bottlenecks at the central servers. In contrast, within a blockchain network, transactions can be conducted directly between any two peers (P2P) without the need for authentication by a central agency. Consequently, the utilization of blockchain technology can substantially decrease server costs, encompassing development and operation expenses, while also alleviating performance bottlenecks at the central server.

- Auditability: - The blockchain technology ensures the validation and timestamp recording of every transaction, thereby enabling users to effortlessly verify and track the preceding records by accessing any node in the distributed network. In the case of Bitcoin blockchain, each transaction can be traced back to the previous transactions in an iterative manner, thereby enhancing the traceability and transparency of the data stored in the blockchain.

- Persistency: - The concept of persistency is crucial in the context of transaction verification and recording within a distributed network. As each transaction is required to be confirmed and documented in blocks that are distributed throughout the entire network, the likelihood of tampering becomes exceedingly difficult. Moreover, the validation of each broadcasted block by other nodes, along with the verification of transactions, further enhances the security measures. Consequently, any attempt at falsification would be promptly identified and exposed.

- Anonymity: - Anonymity is a fundamental feature of the blockchain network, wherein each user is able to engage with the network through a unique address that is generated for them. Moreover, users have the ability to generate multiple addresses, thereby ensuring the avoidance of identity exposure. Consequently, the absence of a central authority responsible for storing users' private information is a notable characteristic of this system. This mechanism plays a crucial role in safeguarding a certain level of privacy for the transactions that are incorporated within the blockchain. However, it is important to acknowledge that the blockchain technology is inherently limited in its ability to guarantee absolute privacy preservation, owing to its intrinsic constraints.

Categorization of blockchain system

Current blockchain systems can be classified into three main types: public blockchain, private blockchain, and consortium blockchain (Buterin, 2015). A comprehensive analysis of these three types of blockchain is presented in Table 1, where various perspectives are considered for comparison.

- Consensus determination: - The process of determining consensus varies across different types of blockchain networks. In a public blockchain, all nodes have the ability to participate in the consensus process, whereas in a consortium blockchain, only a specific group of nodes are responsible for validating the block. In contrast, a private chain is solely controlled by a single organization, which has the authority to determine the final consensus.

- Centralized: - The three types of blockchains differ primarily in terms of centralization. The public blockchain operates in a decentralized manner, while the consortium blockchain exhibits partial centralization. On the other hand, the private blockchain is fully centralized, as it is under the control of a single entity or group.

- Immutability: - Given the distribution of transactions across various nodes within the network, the preservation of the integrity of the public blockchain becomes highly challenging. Nevertheless, the potential for tampering with the blockchain arises when a significant portion of the consortium or the prevailing organization expresses the intention to manipulate it. In such cases, the consortium blockchain or private blockchain may be susceptible to being reversed or tampered with.

- Efficiency: - The propagation of transactions and blocks on a public blockchain network is a time-consuming process due to the vast number of nodes involved. In order to ensure network safety, stringent restrictions are imposed on public blockchains, resulting in limited transaction throughput and high latency. Conversely, consortium and private blockchains, which have fewer validators, are more efficient in terms of transaction processing.

- Read permission: - Transactions in a public blockchain are readily accessible to the general public, whereas the extent of read permission is contingent upon the utilization of a private blockchain or a consortium blockchain. In the case of a consortium or an organization, the determination of whether the stored information is publicly available or restricted lies within their purview.

- Consensus process: - The consensus process of the public blockchain allows for the participation of individuals worldwide. In contrast, the consortium blockchain and private blockchain operate under a permissioned system. In order to partake in the consensus process of the consortium or private blockchain, a node must undergo certification.

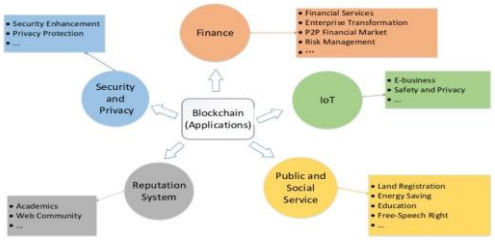
Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission Read	Public Class	Could be public or restricted	May be public or restricted
Determination of Consensus	All miners	Only one organization	Designated set of nodes
Efficiency	Low	High	High
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Consensus	Permissionless	Permissioned	Permissioned

Consensus algorithms:

The process of achieving consensus among untrustworthy nodes in blockchain is a complex problem that can be traced back to the Byzantine Generals (BG) Problem, as described by Lamport et al. (1982). The BG problem involves a group of generals who command a portion of the Byzantine army that surrounds a city. The success of the attack depends on all generals agreeing to attack or not. However, the presence of traitors among the generals makes it difficult to reach a consensus. This scenario is similar to the trustless environment of blockchain, where there is no central node to ensure that the ledgers on distributed nodes are consistent. To address this challenge, various protocols have been developed to ensure that the ledgers in different nodes are consistent.

Applications of blockchain:

The utilization of blockchain technology is vast and varied. This segment aims to provide a concise overview of some of the most common applications of blockchain.



Conclusion

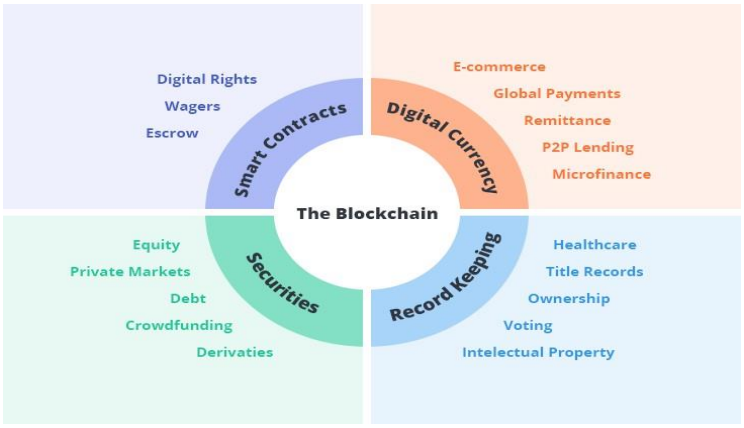
The decentralized infrastructure and peer-to-peer nature of blockchain have earned it high appraisal and endorsement. However, research on blockchain is often overshadowed by Bitcoin, despite its potential for application in various fields beyond cryptocurrency. Blockchain's key characteristics, including decentralisation, persistency, anonymity, and auditability, have demonstrated its potential for transforming traditional industries. This paper presents a comprehensive survey on blockchain, beginning with an overview of blockchain technologies, architecture, and key characteristics. The typical consensus algorithms used in blockchain are also discussed, with an analysis and comparison of these protocols in different respects.

Additionally, typical blockchain applications are investigated, and challenges and problems hindering blockchain development are listed, along with existing approaches for solving these issues. Finally, possible future directions are discussed, including the fast development of smart contracts and proposed applications. However, due to defects and limitations in smart contract languages, many innovative applications are currently challenging to implement.

Future Scope

The blockchain has shown its potential in industry and academia. Possible future directions are: blockchain testing, stop the tendency to centralization, big data analytics, smart contract and artificial intelligence.

Fig 3: The Blockchain



References

1. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.
2. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59, 183-187.
3. R. K. Kaushik Anjali and D. Sharma, "Analyzing the Effect of Partial Shading on Performance of Grid Connected Solar PV System", 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-4, 2018.
4. R. Kaushik, O. P. Mahela, P. K. Bhatt, B. Khan, S. Padmanaban and F. Blaabjerg, "A Hybrid Algorithm for Recognition of Power Quality Disturbances," in IEEE Access, vol. 8, pp. 229184-229200, 2020.
5. Kaushik, R. K. "Pragati. Analysis and Case Study of Power Transmission and Distribution." J Adv Res Power Electro Power Sys 7.2 (2020): 1-3.
6. Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard business review, 95(1), 118-127.
7. Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain? In 2018 crypto valley conference on blockchain technology (CVCBT) (pp. 45-54). IEEE.
8. Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial Innovation, 5(1), 1-14.
9. Niforos, M., Ramachandran, V., & Rehermann, T. (2017). Block Chain.
10. Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of

applications, challenges, and opportunities. IEEE Access, 7, 117134- 117151.
11. Di Pierro, M. (2017). What is a blockchain? Computing in Science & Engineering, 19(5), 92-95.
12. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.
13. Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. SMART supply network, 21-46.
14. Bashir, I. (2017). Mastering blockchain. Packt Publishing Ltd.
15. Gao, W., Hatcher, W. G., & Yu, W. (2018, July). A survey of blockchain: Techniques, applications, and challenges. In 2018 27th international conference on computer communication and networks (ICCCN) (pp. 1-11). IEEE.
16. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In 2017 IEEE technology & engineering management conference (TEMSCON) (pp. 137-141). IEEE.
17. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview.
18. Sarmah, S. S. (2018). Understanding blockchain technology. Computer Science and Engineering,
19. Jain, M., Kaushik, M. and Kumar, G. (2015) "Reliability analysis for embedded system with two types of faults and common cause failure using Markov process," in Proceedings of the Sixth International Conference on Computer and Communication Technology 2015. New York, NY, USA: ACM.
20. Kaushik, M. et al. (2015) "Availability analysis for embedded system with N-version programming using fuzzy approach," International Journal of Software Engineering Technology and Applications, 1(1),
21. Sharma, R., Kaushik, M. and Kumar, G. (2015) "Reliability analysis of an embedded system with multiple vacations and standby", International Journal of Reliability and Applications,