ijaiem.com
ISSN: 2319-4847 /Dec 2023/ Volume 12/Issue 2/Article No-1/50-57

Blockchain Innovation: Transforming Industries through Distributed Ledger Technology

Dr. GANDHAVALLA RAO SAMBASIVARAO[1], Dr. FARHEEN SULTANA[2], Mrs. TAHERA ABID[3]
Department of Information technology
Nawab Shah Alam Khan College of Engineering and Technology (NSAKCET)

Article Info
Received: 27-11-2023 ***Revised: 10 -12-2023*** ***Accepted: 15-12-2023*** ***Published:25/12/2023***

Abstract
Blockchain is a new technology that allows financial data to be shared across a big peer-to-peer network. This way, people who don't trust each other can interact with each other without a third party, and the interactions can be checked. In this study, we look at what Blockchain is, how it works, and some of the most common uses for it. In addition to this new method, the safety, privacy, and consent features of this technology are also significant and cause for worry. This study also talks about the problems that come with Blockchain technology.

Keywords: *Blockchain; Consensus Mechanism; Distributed ledger; Security.*

1. Introduction

In standard deals, all of them rely on a single trusted party. This makes them expensive, inefficient, and unsafe in many ways. We need to bring up the idea of Blockchain technology to solve these problems and make interactions safer, faster, and more open.

The blockchain technology was created by Satoshi Nakamoto [1]. Bitcoin is an example of how Blockchain Technology can be used in the business world. Nothing more than a global record is what the blockchain is. All deals between people and businesses will be handled by it, so there is no need for a third party.

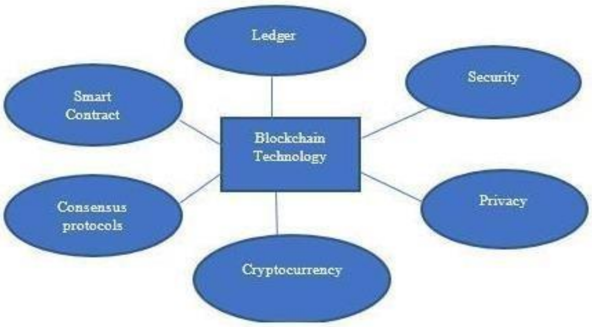


Fig. 1: General Architecture of Blockchain Technology.

The above figure shows the Architecture of the Blockchain Tech- nology. The elements of Blockchain Technology are:
Ledger: Blockchain is a distributed ledger technology, means the copy of the record is same who are participating in the network. There is neither central authority nor a trust- ed third party in the Blockchain

[1] Consensus Protocols: Transaction should be verified by all parties in a network. Creating a block and adding to its ledger is also a decentralized process. It is nothing but a mining process.

[2] Security: Blockchain uses the techniques of digital signa- tures and public key cryptography in order to verify the identity of the transactions in the network.

[3] Cryptocurrency (or cryptocurrency): it is designed as a digital asset works as an exchange of medium for providing secure trans-actions using cryptography.

[4] Privacy: All types of data can be stored in the blockchain. The privacy rules are applicable if sensitive data is pro- cessing-e.g. health data or citizen service

[5] Smart contract: These contracts are acts as agreements with a facility of self-execute and self-enforced. These contracts take the data from external source, so that data should not tamper with that a cryptographic proof must be attached.

2. Literature review

Satoshi Nakamoto [1] was defined as bitcoin is a chain of digital signatures. The chain of ownership can be verified using signa- tures.

The author [13] discussed in his paper was that Blockchain is a new technology and used in applications like artificial intelli- gence, human enhancement, and smart contract etc.

The author [14] explained the characteristics of Bitcoin, related concepts like proof of work and technical review on distributed currencies.

The author [15] proposed a model for exchange of Bitcoins using elliptic curve cryptography

The author [5] mainly focused on Byzantine agreement and con- cept of the ledger in a distributed environment.

The author [16] discussed in his paper that transactional privacy in a decentralized smart contract system

3. Blockchain technologies

A block is a part of the blockchain in which it records all the transactions and once it is completed enters into a permanent data- base in the blockchain. In Blockchain, the blocks are linked one after other like a linked list. Every block consists the hash of the previous block as shown in Figure 2. [2]

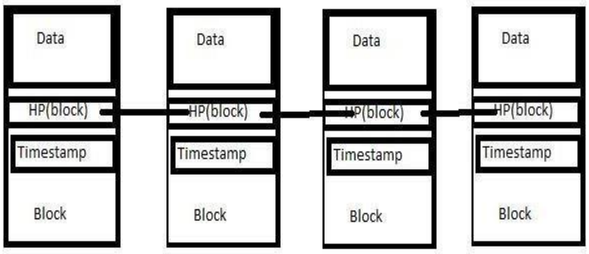


Fig. 2: Blockchain as A Linked List of Blocks Connected by Hash Point- ers.

Blockchain consists of a set of nodes formed like a peer to peer network. With the help of public/private keys, users can interact in the blockchain. The private key is used to sign their own transac- tion and is addressed in the network with the public key. It pro- vides authentication, integrity, and non-repudiation in the network. Each node in the blockchain makes sure that incoming transaction is valid before transmitting further. Invalid transactions are dis- carded. [3] Each Blockchain network should provide certain rules for each database transaction. These rules are programmed to each blockchain client, then verifying that incoming transaction is valid or not. [7]

3.1. Types of blockchain

Blockchains are classified into three types.
1) Public Blockchain,

2) Private Blockchain
3) Permission Blockchain. [11]

In Public Blockchain, everyone can contribute and no trust rela- tionships among the nodes. The transactions on the public block- chain can never be changed and cancelled. The Consensus algo- rithms used in this Blockchain are PoW, PoS and DPoS.
In Private Blockchain, only the owner of the Blockchain has the authority to modify the information and rest of nodes has limited access. PBFT consensus algorithm is used in the Private Block- chain.
In Permission Blockchain, Each participant selects its own con- sensus node based on specified rules. This one is suitable for the semi-closed network which is made by different enterprises.

3.2. Technologies involved in blockchain

Public Key Cryptography is one of the technologies used in Blockchain technology and it is used for encryption and decryp- tion of sensitive data and message authenticity.

3.2.1 Encryption and Decryption:

In asymmetric encryption, public and private key pairs will be used. The public key is used for encryption and the private key is used for decryption. Suppose there is a communication between Alice and Bob, Alice sends a message that is encrypted with Bob public key and then sends to bob. Bob decrypted the message with its own private key. To know the communication between Alice and Bob, the attacker must get both the private keys.

3.2.2. Digital signatures

PKC can be used for authentication also. The digital signature can be done by sender's private key and later it verified by the receiver using sender's public key.

3.2.3. Hash functions

It is nothing but a mathematical function that maps data of any arbitrary size to specific fixed length, called the hash. Hash func- tions are one-way functions that are of the hash value never get an original data.it is also deterministic; the same data always produce the same hash value.

3.2.4. Homomorphic encryption

Arithmetic operations can be carried on encrypted values. Plaintext1 with Encryption changed to Ciphertext1 Plaintext2 with Encryption changed to Ciphertext2 Ciphertext1 * Ciphertext2 = Ciphertext3

Ciphertext3 with decryption converted to Plaintext3 Plaintext1 * Plaintext2 = Plaintext3

4. Security issues involved in blockchain sys- tems

Blockchains mainly concentrating on three security concepts that are confidentiality, integrity, and availability. Basically, Block- chain is a distributed system, so it provides availability and all the nodes in the blockchain agreed based on a chain of transactions then the integrity of data is maintained. With the help of appropri- ate cryptographic keys confidentiality of transactions can be ad- dressed.
Holistic approach in Blockchain systems includes authentication and authorization of entities using the blockchain, transaction transparency, verification and communication infrastructure secu- rity, security from unauthorized insiders, compromised nodes or server failure.
Blockchain systems mainly to look at security in the following aspects. [1]

1) Ledger level security.

2) Network level security.
3) Transaction-level security.
4) Associated surround system security.
5) Smart contract security

4.1. Ledger level security

Authorized members can only participate in the blockchain. The transaction initiated by the members must be signed and valid participants create transactions in the network.

4.2. Network level security

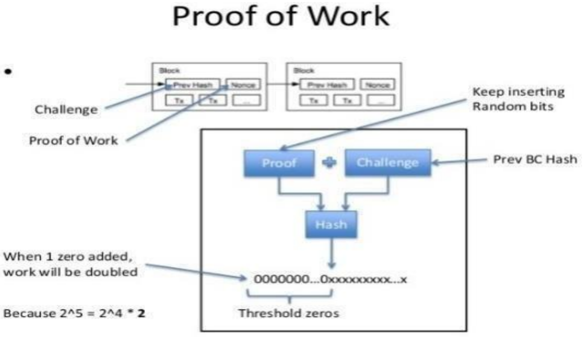
Communication between components of different nodes must be secure from a network point of view. It must be resistant from different external and internal attack vectors in the network. The ledger should possess the capability to withstand DoS attacks. **4.3. Transaction-level security**

Transactions must be encrypted with PKI concepts so that no one compromised with unintended parties. Identity and authorization of transaction creation must be guarded i.e. only particular name 'X' must be able to perform transactions using that name 'X’ only. No one can modify or alter the transaction information and the multisignature feature is available for sensitive transactions in the blockchain.

4.4. Associated surround system security

Associated surround system components such as shadow data- bases should be accessed by valid users. To achieve this imple ment authentication and authorization mechanisms. It also in- volves sharing of documents to prevent from viruses, worms, and malware.

4.5. Smart contract security



Blockchain contracts or digital contracts or self-executing con- tracts or smart contracts acts as agreements; it can be prepro- grammed with the ability to self-execute and self-enforced. Con- tracts loaded in the blockchain should follow the base rules given by the network. These contracts may require data from an external source that may be tampered data. To avoid this cryptographic proof must be attached; it came from the trusted source and not tampered.

5. Privacy issues in blockchain systems

The Bitcoin blockchain is one of the most well-known ones. With its permissionless blockchain record, everyone will be able to see every activity and check them.It looks like it breaks every user's privacy. There are two types of privacy that are used in blockchain systems: transactional privacy and unlinkability.

5.1. Transactional privacy

Only the transacting parties, any regulators, and auditors should be able to see the transaction details. Participating nodes have a tech- nique to validate the transactions considering the availability of funds, where the transaction is entirely encrypted.

5.2. Unlinkability

Arbitrary entities unable to know the details of transactions be- tween others. It may be possible to mine the data from several transactions so that information may be useful to get the infor- mation about the parties involved in the transactions. The idea of unlinkability is about avoiding such deductions from being made.

6. Consensus mechanisms in blockchain

Consensus mechanism provides a definite ordering of transactions and validating the block of transactions. In the blockchain applica- tions, two problems need to be solved 1) Double Spending Prob- lem 2) Byzantine Generals Problem. [11]

1) Double Spending problem: At a time reusing the curren- cy in two transactions.
2) Byzantine Generals problem: In the distributed system, the data is transferred between the nodes through peer to peer communication and there is a chance some nodes in the system may be attacked which leads to changes of commu- nication contents so we have to identify the nor-mal nodes. To solve these problems need to design powerful consensus algo- rithm.

6.1. PoW - Proof of Work

In this algorithm a node is called miner validates the new transac- tions (block) in the network. Miners choose a random number and apply the hashing algorithm for the combination of random num- ber and data in the block. The resulted hash value is within the prescribed range then that miner will get reward points and all other miners stop their work on that block as shown below.

6.2. Proof of stake (PoS)

This Algorithm is based on their share of coins on the network. Anode having more coins, then that node will get a chance to vali- date the block

6.3. Delegated proof of stake (DPoS)

It is the variation of Proof of Stake and concentrated on reputation and voting system. A node in the network selected as a delegated node if and only if the reputation is more and all other nodes vote for this node .when a user holds more coins, their vote will be more count for electing the delegate

6.4. Proof of Importance (PoI)

This algorithm assigns an important score to all the nodes in the network. The importance score depends on these factors such as the number of tokens held, network activity, reputa-tion and the no of transactions made to and from the particu-lar account.

6.5. Proof of activity (PoA)

PoA approach has combined the algorithms of Proof of Work and Proof of Stake. For initial mining Proof of work is used and Proof of stake for new blocks.

6.6. Proof of elapsed time (PoET)

The Proof of Elapsed Time consensus algorithm based on random leader election methodology. The leader may be any of the active nodes then the chosen leader finalizes the block. In this method, the system ensures that the leader is chosen without any manipula- tion and all nodes will verify the same.
6.7 PBFT (Practical Byzantine Fault Tolerance)
Byzantine Generals problem solved by the PBFT algorithm. It works on the concept of the replicated state machine. The replicas will vote for state changes. It also provides optimizations, such as signing and encryption of messages exchanged between replicas and clients, then it will reduce automatically the number of mes- sages exchanged and its size.It needs “3f+1” replicas in order to tolerate “f” no of failing nodes.

6.8. Stellar consensus

This algorithm is based on the concept of quorums and quorum slices. Some set of nodes needed for agreement, defined as a Quorum. A subset of a quorum is called quorum slice. A node can appear on multiple quorum slices. Quorum slices are introduced by Stellar, for the purpose to allow each individual node to select a set of nodes within its slice for allowing open participation.By intersecting the quorums can achieve the global consensus in the system.

6.9. Ripple consensus

In this algorithm, each node has a Unique Node List (UNL).It comprises of other Ripple nodes trusted by that node. The consen- sus is achieved by each node checking with other nodes in its UNL.
Consensus done by several rounds.Each node collects transactions and stored in a data structure called a candidate set. The candidate set receives more than 80% votes from all the nodes in the UNL, then-candidate set treated as a valid block and added to the chain.

7. Applications

7.1. Decentralized exchanges

In general, there is need of broker between buyer and seller. Using the concept of blockchain technology there is no third party. Users in a decentralized exchange create own digital assets and then be exchanged when they come to an agreement.

7.2. Distributed cloud storage

Now a day, centralized cloud storage service is available, must trust on a single storage provider. With the blockchain technology, it will be decentralized.

7.3. Digital identity

Passports, E-Residency, Birth certificates, wedding certificates, online account login are the following areas can apply blockchain technology for Identity applications.

7.4. Supply chain communications and proof of prove- nance

If a company could proactively provide digitally permanent, au- ditable records that show stakeholders the state of the product at each value.

7.5. Smart Contracts

The digitized contracts entered in blockchain are legally bound and smart because they are automated and selfexecute.

7.6. Digital voting

With the help of blockchain, a voter can verify and it was success- fully transmitted to the rest of the world.

8. Conclusions

Blockchains make peer-to-peer systems strong and widespread, and they let people talk to each other without trusting each other and in a way that can be checked. The government should make sure that the rules that guide this technology are uniform, and businesses are getting ready to use blockchain technologies. The consensus process is what Blockchain is all about. More work needs to be done on programs that use Blockchain technology's approval mechanisms to work in a variety of situations.

References

1. (https://bitcoin.org/bitcoin.pdf) is the source for the Electronic Cash System. The second source is the 2017 IDRBT white paper on blockchain technology's potential uses in India's banking and financial industries. the thirdFinancing using Blockchain Technology: A Methodical Approach (2016) Reports from Cognisant.
2. With contributions from Michael Devetsikiotis and Konstantinos Christidis (2016). The Internet of Things using Blockchain Technology and Smart Contracts [Online].Check it out: ieeeex-The file path is plore.ieee.org/iel7/6287639/6514899/07467408.pdf.
3. The Bitcoin Backbone Protocol: Analysis and Applications, edited by J. Garay, A. Kiayias, and N.
4. Leonardos, is available in print and digital form from Springer Berlin Heidelberg in 2015.
5. In their article titled "Is bitcoin a decentralised currency?", Gervais, Karame, Capkun, and Capkun cite the Following sources: Vol. 12, May 2014, pp. 54–60, IEEE Security and Privacy Journal.
6. "Blockchain contract: Securing a blockchain applied to smart contracts," in IEEE International Conference on Consumer Electronics (ICCE'16), pp. 467-468, Jan. 2016, by H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami.
7. H. G. Greenspan (2015). Staying Away from the Fruitless Blockchain Initiative. The Internet.At your disposal: Visit this website: http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain project/.
8. "Cryptocurrencies without proof of work," CoRR, vol. abs/1406.5694, 2014, by Bentov, A. Gabizon, and Mizrahi.
9. In their 2016 paper titled "On the security and performance of proof of work blockchains," A. Gervais, G. O. Karame, K. Wu¨st, V. Glykantzis, H. Ritzdorf, and S. Capkun presented their findings at the ACM SIGSAC Conference on Computer and Communications Security (CCS'16), along with other papers, in New York, NY, USA.
10. "Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake" (2012) by S. King and S. Nadal [11]. (ppcoin- paper_djvu.txt) may be found at this URL: https://archive.org/stream/PPCoinPaper.
11. IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2017, October 5-8, 2017, pp. 2567-2572, "A Review on Consensus Algo-rithm of Blockchain" (Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wnag Xianwei, Chen Qijun,2017).
12. Swan (2015) spoke at the 2015 Texas Bitcoin Conference on the topic of "Blockchain thinking: The brain as a DAC (decen-tralized autonomous organisation)" (pp. 27–29).
13. Florian Tschorsch and Björn Scheuermann] [14] Retrieved from: "Bitcoinand Beyond:A Technical Survey on Decentralised Digital Currencies" (2016, ieeeexplore.ieee.org/document/7423672).
14. The 2017 paper "Designated-Verifier Proof of Assets for BitcoinExchange Using Elliptic Curve Cryptography" was written by Huaqun Wang, Debiao He, and Yimu Ji.

15. "Hawk: The blockchain model of cryptography and privacy-preserving smartcontracts," Kosba, Miller, Shi, Wen, and Papamanthou presented the following: 839-858. The paper was published at the IEEE Symposium on Security and Privacy.