International Journal of Engineering & Technology, 7 (2.7) (2018) 418-421

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A study on blockchain technology

P. S. G. Aruna Sri [1, 2] *, D. Lalitha Bhaskari [3]

[1] *Research Scholar, Department of CS&SE, AUCE (A), Andhra University, Visakhapatnam, AP, India*
[2] *Associate Professor, Department of ECSE, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, AP, India*
[3] *Professor, Department of CS&SE, AUCE (A), Andhra University, Visakhapatnam, AP, India*

Abstract

Blockchain is a one of emerging technology for decentralized and sharing of transactional data across a large peer to peer network, where non-trusting members can interact with each other without an intermediary, in a verifiable manner. In this paper, we review the basics of Blockchain, its applications, types, and working of Blockchain. Behind this innovative technique, the security, privacy issues and Consensus mechanisms of this technology are also important and are a matter of concern. The problems associated with Blockchain technology are also discussed in this paper.

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

1. Introduction

All traditional transactions depend on the centralized trusted party, which gives many problems of transaction cost, efficiency, and security. To solve these problems and to achieve secure, faster and transparent transactions we need to introduce the concept of Blockchain technology.

Blockchain technology, which was introduced by Satoshi Nakamoto [1]. Bitcoin defines as one of the applications of Blockchain Technology in the financial field. The blockchain is nothing but a distributed ledger technology. It will process the transactions between the individuals and organizations without the need for third party involvement.

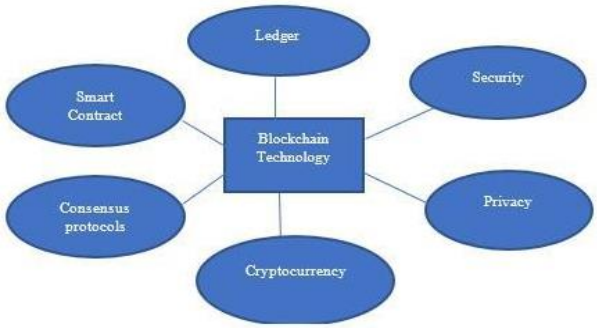


Fig. 1: General Architecture of Blockchain Technology.

The above figure shows the Architecture of the Blockchain Technology. The elements of Blockchain Technology are:

[1] 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 trusted third party in the Blockchain

[2] 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.

All the nodes in the network should agree on the transactions listed on the newly mined block [3]

[3] Security: Blockchain uses the techniques of digital signatures and public key cryptography in order to verify the identity of the transactions in the network.

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

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

[6] 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 signatures.

The author [13] discussed in his paper was that Blockchain is a new technology and used in applications like artificial intelligence, 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 concept of the ledger in a distributed environment.

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

Copyright © 2018 P. S. G. Aruna Sri, D. Lalitha Bhaskari. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 database 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]

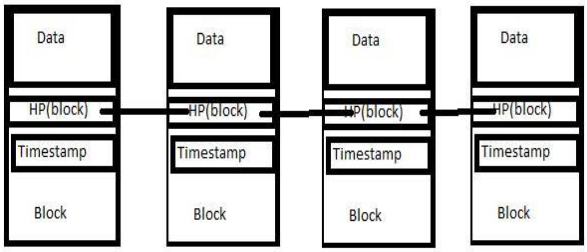


Fig. 2: Blockchain as A Linked List of Blocks Connected by Hash Pointers.

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 transaction and is addressed in the network with the public key. It provides 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 discarded. [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 relationships among the nodes. The transactions on the public blockchain can never be changed and cancelled. The Consensus algorithms 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 Blockchain.
In Permission Blockchain, Each participant selects its own consensus 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 decryption 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 functions 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 systems

Blockchains mainly concentrating on three security concepts that are confidentiality, integrity, and availability. Basically, Blockchain 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 appropriate cryptographic keys confidentiality of transactions can be addressed.
Holistic approach in Blockchain systems includes authentication and authorization of entities using the blockchain, transaction transparency, verification and communication infrastructure security, 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

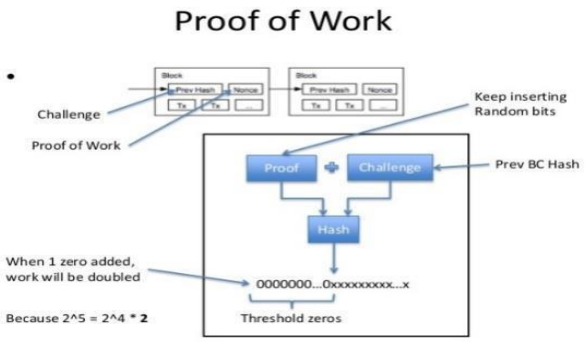
Transactions must be encrypted with PKI concepts so that no one compromised with unintended parties. Identity and authorization of transaction creation must be guarded i.e. only particular name 'X' must be able to perform transactions using that name 'X' only.
No one can modify or alter the transaction 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 databases should be accessed by valid users. To achieve this imple-

ment authentication and authorization mechanisms. It also involves sharing of documents to prevent from viruses, worms, and malware.

4.5. Smart contract security



Blockchain contracts or digital contracts or self-executing contracts or smart contracts acts as agreements; it can be preprogrammed with the ability to self-execute and self-enforced. Contracts 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

One of the well-known blockchains is Bitcoin cryptocurrency. It comes with permission less blockchain ledger, so each transaction will be visible to all and anyone can verify.it seems to violate the privacy of every user.
Transactional privacy and unlinkability are the two categories to provide privacy mechanism in blockchain systems.

5.1. Transactional privacy

Only the transacting parties, any regulators, and auditors should be able to see the transaction details. Participating nodes have a technique 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 between others. It may be possible to mine the data from several transactions so that information may be useful to get the information 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 applications, two problems need to be solved 1) Double Spending Problem 2) Byzantine Generals Problem. [11]

1) Double Spending problem: At a time reusing the currency 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 communication contents so we have to identify the nor-mal nodes.

To solve these problems need to design powerful consensus algorithm.

6.1. PoW - Proof of Work

In this algorithm a node is called miner validates the new transactions (block) in the network. Miners choose a random number and apply the hashing algorithm for the combination of random number 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 validate 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 manipulation 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 messages 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 consensus 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 provenance

If a company could proactively provide digitally permanent, auditable 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 self-execute.

7.6. Digital voting

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

8. Conclusions

Blockchains gives robust, distributed peer to peer systems and ability to interact with peers in a trustless and auditable manner. The government should provide consistent laws for this technology, and enterprise gets ready to hold blockchain technologies. Consensus mechanism is the core technology of Blockchain. In Future work, concentrate on algorithms based on consensus mechanisms of Blockchain technology for different scenarios.

References

[1] Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>

[2] White paper on Applications of Blockchain technology to Banking and Financial sector in India (2017)-IDRBT.

[3] Blockchain in Banking: A Measured Approach (2016) Cognizant Reports.

[4] Konstantinos Christidis and Michael Devetsikiotis (2016). Blockchains and Smart Contracts for the Internet of Things [Online]. Available: ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf.

[5] J. Garay, A. Kiayias, and N. Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[6] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?" IEEE Security Privacy, vol. 12, pp. 54–60, May 2014.

[7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in IEEE International Con-ference on Consumer Electronics (ICCE'16), pp. 467–468, Jan. 2016.

[8] G. Greenspan. (2015). Avoiding the Pointless Blockchain Pro-ject. [Online]. Available: ttp://www.multichain.com/blog/2015/11/avoiding- pointless-blockchain-project/

[9] Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies with-out proof of work," CoRR, vol. abs/1406.5694, 2014.

[10] A. Gervais, G. O. Karame, K. Wu¨st, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.

[11] S. King and S. Nadal, Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake, 2012. (https://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt)

[12] Du Mingxiao, Ma Xiaofeng,Zhang Zhe,WnagXianwei,ChenQijun, "A Review on Consensus Algo-rithm of Blockchain," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) pp.2567-2572, October, 5-8, 2017.

[13] Swan M. "Blockchain thinking: The brain as a DAC (decen-tralized autonomous organization)", Texas Bitcoin Conference. 2015: 27-29.

[14] Florian Tschorsch, Björn Scheuermann "Bitcoinand Beyond:A Technical Survey on Decentralized Digital Currencies" 2016 ieeexplore.ieee.org/document/7423672.

[15] Huaqun Wang, Debiao He, Yimu Ji "Designated-Verifier Proof of Assets for BitcoinExchange Using Elliptic Curve Cryp-tography" 2017.

[16] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. "Hawk: The blockchain model of cryptography and privacy-preserving smartcontracts", 2016 IEEE Symposium on Security and Privacy, 2016: 839-858.