BLOCKCHAIN DEVELOPMENT FOR CRYPTO-MINING

Abdallah Issaka, Umarani C.
Student, Professor & Guide,
MCA- Information Security Management Systems,
Jain University, Bangalore, India

Abstract: Block-chain technology is the new technology that uses cryptographic methods and decentralized peer-to-peer network to securely and transparently store and retrieve data. This technology seems to be the new tendency now a day and appears as the solution for the future in the data security domain but it is less known by many people. A good knowledge of this technology in the near future will be a very good add-on in once career in security field. Hence this paper explain about block-chain, its working, the domains related to it and how its combination with those domains for more data security.

I. INTRODUCTION

Block-chain is defined as an ever growing list of records (blocks) which are securely linked using cryptography. Block-chain can be define also as a leger which can store financial transactions or anything that is of value digitally and it is not related to a single person or an organization but will be transparent to all who are in the chain and can access it without revealing the identity of the user. In a block-chain, blocks are linked together backward by referencing hash from the previous block in the link. A hash is a unique digital signature that links the block together to create a chain and making it stronger.

The following are some of the important features of block-chain:

Immutable Ledger: data that are entered into the block-chain contain hash values and these hash values are what connect the blocks in a chain and each is linked to another using the previous hash value of the former. So, data cannot be altered later, why it is called immutable ledger.

Cryptographic hashes: Hashing is a one way encryption technique used in block chain to make sure the data in a block are authentic. Each block has its own hash value and the hash value of the previous block. So when a block is created a hash is assigned to it and this value will be used in the next block of the chain. If a hacker tries to change the content of the block even by a letter the hashing value will change, causing the rest of block to be unsynced sending alert to the rest of the nodes to replace the content of that block to the original.

Distributed P2P network: the main aim of distributed P2P network is the decentralization of the block-chain for better transparency. Also in distributed network all the nodes have the same chain and each user is identified using an identifier rather than their real identity. Even if one of the nodes is compromised the other nodes will communicate with the compromised node stating that the data is different and they will replace the data in the compromised node creating a trust in trustless environment.

Consensus Protocol: As a term, 'consensus' means that the nodes on the network agree on the same state of a block-chain, in a sense making it a self-auditing ecosystem. This is an absolutely crucial aspect of the technology, carrying out two key functions. Firstly, consensus protocols allow a block-chain to be updated, while ensuring that every block in the chain is true as well as keeping participants incentivized. Secondly, it prevents any single entity from controlling or derailing the whole block-chain system. The aim of consensus rules is to guarantee a single chain is used and followed

II. SIGNIFICANCE

A. Role of this project

The aim of project described by this article is mainly educative and informative. So this is to make understand block-chain in a simple but also clear way by using simple terms, explanations and implementation. As result of this paper we expect a detail explanation of how block-chain with a particular focus on security and transparency. More details are given in the description section.

A. Background

Now days, there are many cryptocurrencies we hear about (Bitcoin, Neo, Ethereum, Ripple, etc) which use block-chain, platforms like steemit also use block-chain and it is used in many private application, but I have never seen a good paper explaining block-chain development is a simpler way. Hence the article described in this paper does the same and invite the readers to be interested in this beautiful and feature oriented technology.

III. DESCRIPTION

This article aims to detail on development of a block-chain sample that can be used in a local network to show all the operations that can be done on a block-chain and how those operations are performed. Those operations are for example mining blocks, make the block-chain decentralized, make transactions, make divers changes etc. The different modules included in this project are described below in details:

A. Block-chain creation

In this module the block-chain concept is explain, the development of the block-chain with the mining method. Mining blocks in a chain is nothing more than adding new into it and growing the chain. Those blocks are linked together with current block and previous block hashes as explained in the introduction section.

A. Decentralization

In this module of decentralization, several nodes are created in the local network and interconnected. Then simulations of transactions are made to show the decentralization. So here nodes synchronization is done so that all nodes have the same data and everyone is the network sees the same data.

A. Block-chain explorer and postman

Postman is a powerful HTTP client for testing web services created by Abhinav Asthana, a programmer and designer, it makes it easy to test, develop and document APIs by allowing users to quickly put together both simple and complex HTTP requests. So it is the user friendly API that is used in this project to make the transaction and add them to the block-chain,

The block-chain explorer in the other hand is a small and simple web interface used to interact with the created chain. So using this interface, one can view the chain in a more comprehensive way, make searches based on block hashes, transaction ids, sender or receiver's address etc.

IV. WORKING

The working process of the system is as explain below:

- ✓ Firstly, all the nodes in the block-chain need to be running
- ✓ Then connect the nodes each other to create the decentralization. Connection of nodes is done using the postman application and the connect method of the chain.
- ✓ Then mine blocks in whichever of the nodes. Mining can be done either through the browser or the postman interface. As all nodes are connected in the previously, the newly mined blocks will appear in every one of the nodes.
- ✓ Make a transaction through the postman interface. A transaction four parts which are: sender's address, receiver's address, the amount of the transaction and the id of the transaction which is generated automatically.
- ✓ After making a transaction we need to mine a new block to incorporate that transaction because each transaction is include in the next block that is mined after it is made.
- ✓ Except the first two operations, the rest can be done as many as we want.
- ✓ At any time we can make use of the block-chain explore to explore it, either viewing it, making a search, etc.

So after making those operations on the block-chain, we easy understand the whole mechanism of the block-chain and decentralization.

V. SYSTEM ARCHITECTURE

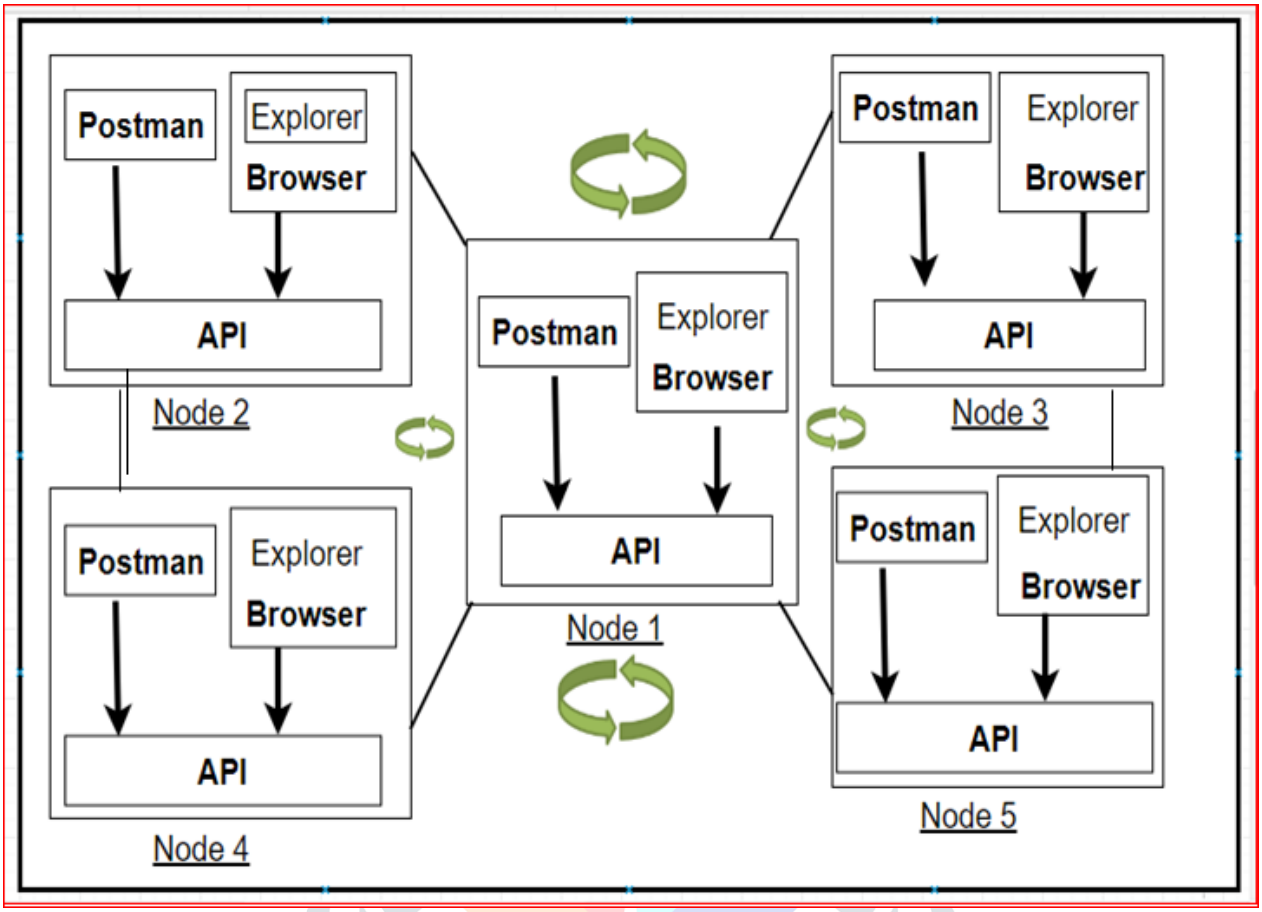

Figure-01: system architecture

A. System architecture explanation

The image in **Figure-01** is the systen architecture diagram of our block-chain. So the architecture comprises nodes which are connected to each other and synchronized to always have the accurate information. Each node has an API use to run the chain, a postman application running and a browser on which the block-chain explorer is used.

VI. FUTURE ENHANCEMENTS

Even though the project described in this article is successful in completing its duties there are some areas or parts where this can be improve. A few points to carry on for the future have been listed below.

1) There is no any wallet associated to this block-chain, so one can be added for more effectivity.
2) For now, this system works only a local network so we can improve to run on internet.
3) One can use this existing system to implement in a domain other than crypto-currency.

VII. CONCLUSION

In conclusion even though, this paper gives a simpler explanation of block-chain technology and decentralization, we can affirm that this is a very good point to start with one's block-chain learning journey. And at the end what I can assure is that this field is too exciting and it is surely the future destination for security, integrity, transparency even anonymity on the web and more.

VIII. REFERENCES

A. Research Papers

[1] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) 'An overview of blockchain technology: Architecture, consensus, and future trends', Proceedings of the 2017 IEEE BigData Congress, Honolulu, Hawaii, USA, pp.557–564
[2] Zyskind, G., Nathan, O. et al. (2015) 'Decentralizing privacy: Using blockchain to protect personal data', Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, pp.180–184.
[3] Michael Crosby (Google), Nachiappan (Yahoo), Pradan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America), Vignesh Kalyanaraman (Fairchild Semiconductor), BlockChain Technology: Beyond Bitcoin

[4] Atzori, Marcella, Blockchain Technology and Decentralized Governance: Is the State Still Necessary? (December 1, 2015).
[5] Wright, Aaron and De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015).

B. Web References

https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
https://www.anf.es//pdf/Haber_Stornetta.pdf
https://medium.freecodecamp.orgsmartcontracts-for-dummies-a1ba1e0b9575