TRANSACTION BASED BLOCK CHAIN CRYPTOCURRENCY

S. Aswin[1], T. Barathwaj[2], M. Mathiyazhagan[3], R. Mohan babu[4]

[1,2,3,4]*B.Tech, Dept of Information Technology, Valliammai Engineering College, Chennai, Tamil Nadu*

Abstract- *Blockchain technologies are gaining massive momentum in the last few years. Blockchains are distributed ledgers that enable parties who do not fully trust each other to maintain a set of global states. The parties agree on the existence, values, and histories of the states. While the current transaction is based on the centralized system. In which the miner uses the mechanism to mine the data and do the verification, which initially costs a large amount for the transaction. Once the node is breaking the data position is unknown. Even if the reversive transaction is enabled, we couldn't track the transaction. We cannot find the nonce in which amount is or where it is. So, we propose the Transaction based Block chain cryptocurrency. It is an initial PoC developed in Python. The main aim of this project is to build Transaction based Block chain architecture for discovering cryptocurrencies. This overcomes the mining transaction, which is decentralized and with that it can be used to have the nodes to store the ledger. So, the node to node transaction can be monitored. Basically, the transaction to going to happen between the accounts, this will be sent through a secure cryptographical channel, which is implemented with cryptographical algorithm. And wallet transaction will be verified and the traffic is captured and verification can be shown for the security purposes. This is a PoC that runs only on local networks and provides proper security. The code should only be used to get familiar with the building blocks for a cryptocurrency. Elliptical Curve Cryptographic / ECC public key compression/decompression is used for security feature. The entire validation is performed based on self-created wallet, crypto, validation, networking, mining etc. The entire project has been developed using python, Ethereum*

Keywords—component; formatting; style; styling; in

I. INTRODUCTION

Blockchain technologies, due to the success of Bitcoin, are taking the world by storm, largely. A blockchain, also called distributed ledger, which do not fully trust each other, is essentially an append-only data structure maintained by a set of nodes. Nodes in the blockchain, each containing multiple transactions, agree on an ordered set of blocks, thus the blockchain can be viewed as a log of ordered transactions. Blockchain can be viewed as a solution to distributed transaction management, in the database context where nodes keep replicas of the data and agree on an execution order of transactions. Blockchain systems in such environments are called private (or permissioned), as opposed to the early systems operating in public environments (or permission less) where anyone can join and leave.

Applications such as security trading and settlement, asset and finance management, banking and insurance are being built and evaluated. Oracle and MySQL, These applications are currently supported by enterprise-grade database systems but blockchain has the potential to disrupt this status quo because it incurs lower infrastructure and human costs.

In particular, blockchain's immutability and transparency help reduce human errors and the need for manual intervention due to conflicting data. In the original design, Bitcoin's blockchain stores coins as the system states Bitcoin nodes implement a simple replicated state machine model, for this application, which moves coins from one address to another. Since then, blockchain has grown beyond crypto-currencies to support user defined states and Turing complete state machine models.

For example, Ethereum enables any decentralized, replicated applications known as smart contracts. Interest from the industry has started to drive development of new blockchain platforms, settings, where participants are authenticated, designed for private.

II. SCOPE OF THE PROJECT

This concept to developed to have the transaction of the amount without uninterrupted by maintaining the node level transaction ledger. This project over comes the mining transaction, which is decentralized and that can be used to have the nodes to store the ledger. So that the node to node transaction can be monitored. Basically, the transaction to going to happen between the accounts, this will be sent through a secure cryptographical channel, which is implemented with cryptographical algorithm. And wallet transaction will be verified and the traffic is captured and verification can be shown for the security purposes.

They have the transaction data that is to be transferred to the other account will be sent through a secured cryptographical channel. Because these accounts will be having a private and a public key separately. And to avoid the Middle Man attack. The data is sent through the secured channel. For that we are using Elliptical curve cryptographic system. Each node will be created with the public and private keys uniquely for that having the address separately. So, the transaction will be from one account to the other is done by transferring the amount. This sent as a encrypted hashed value through the nodes. The miners verify the data with the mechanism and the data transaction proceeds. Even the miners fail, the process is not disturbed, as the ledger is maintained the proceeds.

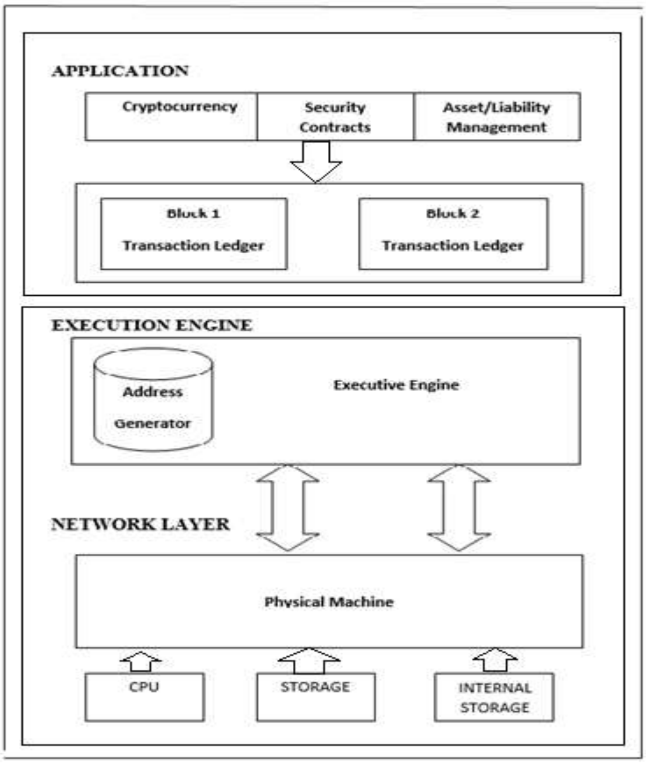
III. PROPOSED SYSTEM

This concept is developed to have the transaction of the amount without an interruption by maintaining the node level transaction ledger. This project over comes the mining transaction, which is decentralized and that can be used to have the nodes to store the ledger. So that the node to node transaction can be monitored. Basically, the transaction to going to happen between the accounts, this will be sent through a secure cryptographical channel, which is implemented with cryptographical algorithm. And wallet transaction will be verified and the traffic is captured and verification can be shown for the security purposes.

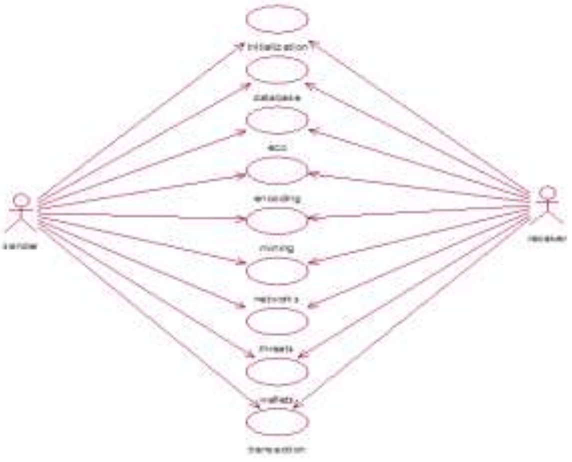
The have the transaction data that is to be transferred to the other account will be sent through a secured cryptographical channel. Because these accounts will be having a private and a public key separately. And to avoid the Middle Man attack. The data is sent through the secured channel. For that we are using Elliptical curve cryptographic system. Each node will be created with the public and private keys uniquely for that having the address separately. So, the transaction will be from one account to the other is done by transferring the amount. This sent as a encrypted hashed value through the nodes. The miners verify the data with the mechanism and the data transaction proceeds. Even the miners fail, the process is not disturbed, as the ledger is maintained it proceeds. And wallet transaction will be verified and the traffic is captured and verification can be shown for the security purposes.

This is a PoC that runs only on local networks and provides proper security. The code should only be used to get familiar with the building blocks for a cryptocurrency. Elliptical Curve Cryptographic / ECC public key compression/decompression is used for security feature. The entire validation is performed based on self-created wallet, crypto, validation, networking, mining etc. The entire project has been developed using python, Ethereum.

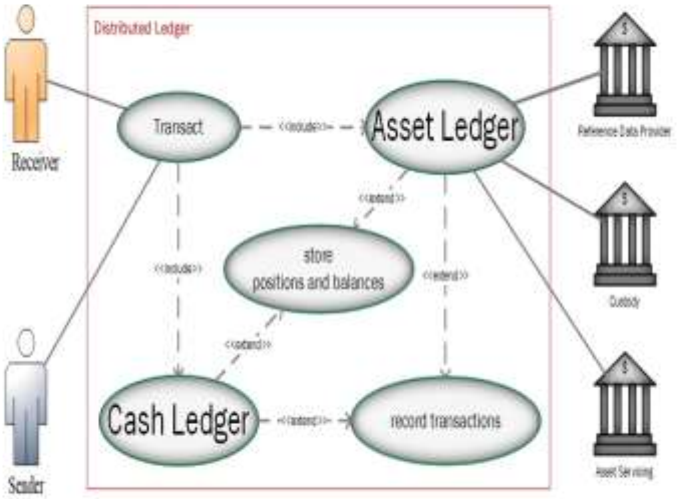
IV. ARCHITECHTURE DIAGRAM



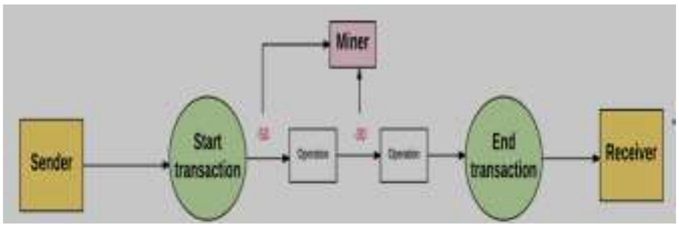
V. USE CASE DIAGRAM



VI. ACTIVITY DIAGRAM



VII. FLOW DIAGRAM



VIII. METHODOLOGY

The content of the ledger reflects historical and current states maintained by the blockchain. Being replicated, updates to the ledger must be agreed on by all parties. In other words, multiple parties must come to a consensus. Note that this is not the case in many real-world applications such as fiat currency, in which one entity (e.g., the bank or the government) decides the updates. One key property of a blockchain system is that the nodes do not trust each other, meaning that some may behave in Byzantine manners. The consensus protocol must therefore tolerate Byzantine failures. The research literature on distributed consensus is vast, and there are many variants of previously proposed protocols being developed for blockchains. They can be largely classified along a spectrum. One extreme consists of purely computation-based protocols that use proof of computation to randomly select a node which single-handedly decides the next operation.

Bitcoin's proof-of-work (PoW) is an example. The other extreme is purely communication-based protocols in which nodes have equal votes and go through multiple rounds of communication to reach consensus. These protocols, PBFT being the prime example, are used in private settings because they assume authenticated nodes.

IX. MODULE DESCRIPTION

A. CRYPTOGRAPHIC MODULE

Cryptographic module is primarily used for securing the identity off the sender transaction. That it uses the ECC for the cryptographical transaction. That makes sure that the everyone in the network will be having the copy of the data bring transferred. The public distributed ledger id maintained. It can be viewed by everyone in the network. That is sent as an encrypted value as a hashed value. The proof of work is done and maintained, and the mining is done by the miners.

B. ENCODING MODULE

Blockchain eliminates unauthorized access by using cryptographic algorithm to ensure the blocks are kept secure. Each user in the blockchain will have their own keys. Private and public key. The sender sends the data, as the transaction. The data will be hashed and the hashed value is passed through the algorithm. Now the transaction data and the public are transmitted to the receiver. The transaction is passed through the hash function to get the hash value. And it is compared with the hash value obtained of the transaction.

C. MINING

Proof of work is the method to validate the transaction in blockchain network by solving a complex mathematical puzzle(mining). Finding the nonce value is the mathematical puzzle that users or miners need to solve in the network. The puzzle is solved by determining a nonce that generates a hash value and gives an output lesser than an a given output. miners verify transaction within the blockchain and adds the block to the blockchain when confirmed. With proof of work the miners compete against each other to solve the mathematical puzzle. The miner who solves the puzzle is rewarded.

D. TRANSANCTION

The transaction module maintains the overall transactional data. That is each node in the blockchain is made to a separate address and a unique key. These are made have been stored in the database on its itself. The node of the blockchain are made to have the header and along with it the block verification number and the hashed value of the previous block. And the nonce value is also kept in here. And the target value is set, that id is predefined.

E. WALLET MODULE

The wallet is created to have the amount for the transaction. That is each node in the blockchain will have the private key and public key and the address associated with it. If the sender wants to send the amount. The amount will be deducted from the wallet and the transactions made to view by everyone. And the data is made to send for authentication. Once authenticated the data will be added to the ledger. And the receiver gets the amount credited.

X. REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, http://bitcoin.org/bitcoin.pdf, Last accessed: 2017.

[2] Q. Lin, P. Chang, G. Chen, B. C. Ooi, K. Tan, and Z. Wang, "Towards a non-2PC transaction management in distributed database systems," in Proc. ACM Int. Conf. Manag. Data, 2016, pp. 1659–1674.

[3] A. Thomson, T. Diamond, S. Weng, K. Ren, P. Shao, and D. J. Abadi, "Calvin: Fast distributed transactions for partitioned data- base systems," in Proc. ACM Int. Conf. Manag. Data, 2012, pp. 1–12.

[4] P. Bailis, A. Fekete, M. J. Franklin, A. Ghodsi, J. M. Hellerstein, and I. Stoica, "Coordination avoidance in database systems," Proc. VLDB Endowment, vol. 8, no. 3, pp. 185–196, 2014.

[5] Ethereum blockchain app platform. (2017). [Online]. Available: https://www.ethereum.org/

[6] Konstantinos Christidis, and Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things" 2016

[7] Nir Kshetri, University of North Carolina at Greensboro, "Can Blockchai Strengthen the Internet of Thing" 2017

[8] Keke Gai, Liehuang Zhu,” Block chain-Enabled Reengineering of Cloud Data enters” 2018

[9] Zhaofeng Ma, School of Cyberspace Security, “A master slave blockchain paradigm and Application in Digital rights management” 2018

[10] Qingsu He, Yu Xu, Yong Yan,JunshegWang,QingzhiHan, and Lili Li, “A Consensus and Incentive Program for Charging Piles Based on Consortium Blockchain” 2018