Development of System for Cryptocurrencies Using Blockchain Technologies

Sahana Bisalapur[1], Bhagyashree Patil[2], Meghana Neelannavar[3], Nalini Karagi[4], Prajna Nayak[5]

Assistant Professor S.G. Balekundri Institute of Technology Belagavi[1], India Student of Computer Science Engineering Belagavi[2345], India sahanabisalapur@gmail.com[1], shilpapatil9063@gmail.com[2], meghun06@gmail.com[3], nalinikaragi9@gmail.com[4], prajnanayak311 @gmail.com[5]

Abstract: Peer to Peer money transfer in Android App with blockchain architecture is a very novel and holistic approach to transfer money within a small group of peers who lend, borrow and transfer money from one person to another in e-wallets. Money transfer in blockchain is inevitable in the near future as it entails non-repudiation, security, transparency, preserves anonymous of users with homomorphism encryption and the internet tamper-proof nature of the distributed ledger of the blockchain makes it more resilient and robust. The transactions of all the peers are recorded in the distributed ledger stored in the cloud.

Keywords: Android mobile phone.

I. INTRODUCTION

In the traditional centralized financial system, many problems are encountered such as, Firstly, banking business can be done only during bank's working hour, though all banks have opened a few transaction services over pervasive Internet with some limitations. Second, the transnational remittance will also encounter the review in international wire transfer. For example, if sending a sum of money from the local bank of United States to a bank in China, not only needs to wait for the office hours in these two different national banks, but also payee needs to wait three working days even after the wire transfer to China and the submission of declaration document to

prove the source of this money. Third, the customer finally needs to pay a fee of up to NT$ 750. Among these many problems mentioned above in conventional money transactions the emerging blockchain technology has become the best solution to solve the time difference problem of transnational remittance. Based on the peer-to-peer (i.e. P2P) architecture and anonymity in blockchain technology, so customers do not need to go to the bank to declare the source of funds, do not need to pay a high amount of cross-border wire transfer fee.

Bitcoin is a P2P electronic cash system, compared to traditional centralized financial institutions. Decentralized design can bring more advantages, such as reducing the risk of cyber-attacks, because the storage of blockchain is distributed across the Internet computers running full node [1] via P2P network technology [2]. Nowadays Bitcoinblockchain size has reached more than 100GB. All the data in Bitcoin transaction is permanently stored in blockchain since 2009. The computers running the Bitcoin system in the world are up to more than six thousand network nodes according to the statistics. It means that the blockchain information has been copied over six thousand times. Such a large number of network nodes for blockchain backup can ensure the stability of Bitcoin network. The failure of a host does not affect the normal operation of Bitcoin network. Besides, the decentralized system applied in Bitcoin network, people do not need to operate, manage and maintain manually at any time. So, Bitcoin system can run continuously without disruption in fair stability, very different from the traditional centralized financial organizations.

The traditional financial transaction system is composed of many traditional financial organizations. Users have to trust the closed payment flow to use these organizations' financial services. However, the centralized financial transaction system has some problems that need to be overcome. For example, since all transaction information is managed centrally, customers are not authorized to freely access their transaction information. These transactions are not publicly reviewed and customers are forced to trust their financial companies in the safety of funds, including the flow of funds.

If these traditional central financial institutions apply blockchain technology in their financial flow system. The blockchain technology will be inherited to indicate that the transaction records will be transparent to all the customers to review. So, there will be no unknown cash flow problems. It not only preserves money flow transparent, but also ensures that consumers' transaction records won't be

changed and deleted. That's to say; the seller can believe that the algorithm's correctness by using blockchain technology to trust the transaction and further grasp all the transaction details clearly, or even the company's business status can be provided easily. Then, the human resources can be reduced to efficiently generate financial statement and statistics reports. Finally, the government can easily review and believe the correctness of all the business transaction information. For the tax collection, it also can have a standardized, trusted and fully automated operating procedure. It can reduce not only the labor cost, but also the errors in government taxation procedure.

Therefore, in this project, we propose a Blockchain-based Payment Collection Supervision System, which is abbreviated as BPCSS, for transactions between customers and merchandise stores who use the pervasive Bit coin digital wallet. All transaction details can be cost-effectively saved on the cloud database right after customers use their NFC-enabled [3] Android Smartphone App to purchase RFID-tagged goods in merchandise store. The customers and merchants can review these transaction details without troubles mentioned before in traditional financial system.

This project is organized as follows. In Section II, the blockchain technologies related to pervasive digital wallet are introduced. In Section III, the subsystems and their functions in proposed BPCSS system are described in details to provide blockchain-based payment collection supervision using Bitcoin digital wallet. In Section IV, preliminary digital currency transaction experiments on the implemented subsystems of BPCSS prototype are conducted via BitcoinTestnet [4] and performance analysis is concluded. The last section summarizes the proposed solution and provides future work.

II. LITERATURESURVEY

[1] Sebastian Feld, Micro Schonfeld, and Martin Werner."Analyzing the Deployment of Bitcoin's P2P Network under an ASlevel Perspective."Procedia Computer Science 32 (2014): 1121- 1126.

Sebastian Feld et al [5] discusses the deployment of Bit coin's P2P network in distinct autonomous systems. The parameters considered are bitcoin peers, autonomous systems with routable peers, peer list of all connected peers in the autonomous systems, routable peers, non-routable peers and unreachable peers. The traversal of Bitcoin P2P peers in distinct autonomous systems and their statistics is exploited in this paper.

[2] Dennis, Richard, Gareth Owenson, and Benjamin Aziz."A temporal blockchain: a formal analysis."2016 International Conference on Collaboration Technologies and Systems (CTS). IEEE, 2016

Richard Dennis et al [6] discusses the scalability of blockchains and he emphasizes a time period during which the data from the blockchain is read and verified. Any transaction data before that time period is omitted. The time period data for 30 days is checked for availability, consistency and Integrity. The data gets updated and at the older time, the block gets deleted. The availability, consistency, and Integrity measures are considered against the traditional blockchain. The author has presented a paper on B-language and Z-language.

[3] Suankaewmanee, Kongrath, et al. "Performance analysis and application of mobile blockchain."2018 international conference on computing, networking and communications (ICNC).IEEE, 2018.

Kongrath, Suankaewmanee, et al [7] discusses about an android app that deploys the message passing process regarding transactions from one mobile user to all mobile users that are connected to a gateway. The miners take the unconfirmed transactions from a pool of transactions present in backlog and mine them and add it to the blockchain. The ID of the new block, previous block ID, timestamp, transaction, miner's, signature and public key are the quintessential features in a block.

[4] Kano, Yuki, and Tatsuo Nakajima. "An alternative approach to blockchainmining work for making blockchain technologies fit to ubiquitous and mobile computing environments." 2017 Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2017

Yuki Kano, Tatsuo Nakajima et al [10] discusses about the Blockchain mining work for making Blockchain technologies fit the ubiquitous, mobile computing environment. In this paper, a new solution to solve the mining problem by using a simple virtual currency service that allows a user to operate the service by giving the user a new incentive based on gamification. Mining work based on gamification of services consists of following elements such as Currency Unit, Communication protocol, Account, Transaction, Block and Mining Work. These technologies can be implemented by Graphic User Interface (GUI) of functions such as Account Registration and Login, Menu, Transaction, Publication, List Up account and Mining Work.

[5] Manzoor, Ahsan, et al. "A Delay-Tolerant Payment Scheme on the EthereumBlockchain."2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(Wow Mom).IEEE, 2018.

AhsanManzoor et al [11] discusses the delay tolerant payment scheme on the ethereumBlockchain. Cash-less payment scheme for remote villages based on block chains that allow maintaining a record of verifiable transactions in a distributed manner. The bank joins as a peer and monitors node behaviors, rewards miners and processes currency exchanges whenever the connectivity is available. These groups of peers can be a conglomerate of three network nodes that consists of miners, full nodes and light nodes. The feasibility of the system design with a prototype implementation containing a private Ethereum block chain with an intermittently connected bank node is implemented

[6] He Zhu, Changcheng Huang, and Jiayu Zhou. "Edge Chain: blockchain-based multi-vendor mobile edge application placement."2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft).IEEE, 2018.

He Zhu et al [12] discusses the blockchain-based architecture to make mobile edge application placement decisions for multiple service providers, based on a stochastic programming problem minimizing the placement cost for mobile edge application placement scenarios. All placement transactions are stored on the block chain and are traceable by every mobile edge service provider and application vendor who consumes resources at the mobile edge. The potential security problems including service overlay, security, trusted classification policy, and secure encapsulation can be prevented. This can be implemented by using the edge chain algorithm.

III. EXISTING SYSTEM

Block chain is a tremendous approach for daily Life Operation, which helps us to maintain distributed storage system. In day to day life, user come across certain operations where, the user has to maintain the data in ledger, which is centralized at one place and any physical damage occurs, there is a possibility of losing a data and also remote access is not achieved. In such situation the one who holds the ledger might attempt to tamper the data. In order to overcome these problems and issues block chain technology approach is used.

Examples: Currency and Transaction Support,

Supply Chains and Item Histories, Voting, Government Operations, Intellectual Property, Marijuana Industry's Banking and Logistics Issues, Cloud Storage, Charity.

In the above mentioned sectors operation is performed with blockchain technology without any effect of data tamper and secure operation is achieved.

IV. PROPOSEDSYSTEM

The objective of the proposed sytem is to have a secured, tamper proof transaction. The system can perform 50,000 transactions per second. The anonymity of the payer and payee is maintained in the transaction.

The proposed system implements a Crypto currency buying and paying mechanism by maintaining blockchain for the transactions on multiple mining nodes

The proposed system will be implemented in multiple modules, like:

User Module:

The module will be developed as a mobile app catering to numerous mobile users.

This module should provide all the user interfaces to the user like Account Registration, Payment options, Buying options, Checking balance etc.This module will work like a currency wallet, for buying and spending crypto currency.

Central Server Module:

The system should be developed as a combination of Distributed and Central Blockchain ledger.This module should maintain the blockchain and also the distributed peers (Mining Nodes).Each peer module (Mining nodes) should also have the recent blockchain.

Peer Node (Mining Node):

This module should verify the transaction, by validating the payer and receiver and also checking double spending.This module is also responsible for updating the blockchain on the Central server.This module should pickup transaction from the pending transactions pool.

V. IMPLEMENTATION

The user wallet app, i.e the user android module provides interface for user interaction. It provides login, registration, Account creation, Buying Ecoins, Paying Ecoins, and Balance check can be done in this module. This app is used to login to user’s wallet and spend the Ecoins. This app can be accessed only by the user.

The admin central module i.e the mining node module runs in mining node continuously validating and verifying transactions and creating blocks.The task is done by the trusted third party.

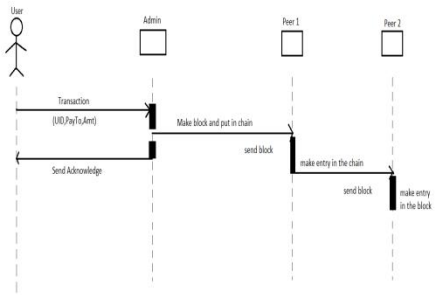

Fig 5.1 System sequence diagram

The Peer node module i.e the central server module provides interface for system monitoring. It views accounts, transactions, mining nodes, Blockchain etc. It is done by the peer node.

Real time database is created with the cloud. The implementation is done in cloud server and in Android system. The data is displayed, synchronized across all its clients, web clients or mobile clients. The user of this app has to sign in and register their details like name, mobile number and password. The login phase needs the user to login the details of mobile number and pin number and login to the mobile application. The blocks of each user, the number of users and the transactions of the user are stored in the Google cloud server, a real time database; this cloud database has details of the group of users who wants to do their transactions in this Mobile-chain with the other registered users. The database has user details like his name, his phone number and pin number. The user details are validated and entered or else the users are asked to enter proper values.

The sender node signs the transaction and broadcasts it to other users. The receiver node will sign with his private key to get the transaction details and also broadcast it to other users. Proof of work consensus mechanism is used which requires all the nodes to participate in block generation and verification process. The Mobile Wallet application, the user can Login, Buy e-coins, Pay e-coins, check the wallet balance and can logout.

The block of each user has the hash value of the block, merkle root, the nonce, hash value of the previous block. If a new user downloads the blockchain and if the transactions are broken during the download phase, the user can utilize the merkle tree for downloading the transactions. The block chain architecture has a pool of transactions, where the first invalidated transaction is taken from the pool and validated by miners. Here all the users are considered as miners.Thenumber of transactions of each user, from whom they have got money and with whom they have transacted money are also shown in encrypted form. Thus the anonymity of the payer and the payee are maintained by the app. The user validity of the chain is checked and shown in Log cat and the transaction details of a

successful transaction, the public key of the user.

The data that is stored in cloud storage by the users can be stored using homomorphic encryption that yields for security and privacy preserving features.

RESULT

Blockchainprotects the assets and transactions based on decentralized distribution of data. Since every bit of information can be replicated across large number of computers, destroying or modifying the information on one or more computers simultaneously will not impact the integrity of the Blockchain.The systemis more accurate, consistent and transparent .Hence the transaction done using blockchain is completely secured.

CONCLUSION

In this system, secured transaction is possible. Decentralization makes the storage of information on blockchain much safer compared to centralized storage system. There is increase in efficiency and speed in this system when compared with traditional system. By streamlining and automating various processes with blockchain, transactions can be completed faster and more efficiently. There is transparency in the system.Transaction histories are more transparent through the use of Blockchain technology. Remote access can be achieved i.e. easily accessible from anywhere.Blockchain is a technology that allows individuals and companies to make instantaneous transactions on the network without any middlemen (like banks). Transaction made on blockchain are completely secured, by function of Blockchain technology, are kept as record of what happened. Strong computer codes ensure that, no record of transaction on Blockchain can be altered.

REFERENCES

[1] Sebastian Feld, MircoSchonfeld, and Martin Werner."Analyzing the Deployment of Bitcoin's P2P Network under an AS level Perspective." Procedia Computer Science 32 (2014): 1121- 1126

[2] Dennis, Richard, Gareth Owenson, and Benjamin Aziz. "A temporal blockchain: a formal analysis."2016 International Conference on Collaboration Technologies and Systems (CTS).IEEE, 2016.

[3] Suankaewmanee, Kongrath, et al. "Performance analysis and application of mobile blockchain."2018 international conference on computing, networking and communications (ICNC).IEEE, 2018.

[4]Kano, Yuki, and Tatsuo Nakajima. "An

alternative approach to blockchain mining work for making blockchain technologies fit to ubiquitous and mobile computing environments." 2017 Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2017

[5]Manzoor, Ahsan, et al. "A Delay-Tolerant Payment Scheme on the EthereumBlockchain."2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(Wow Mom).IEEE, 2018.

[6] He Zhu, Changcheng Huang, and Jiayu Zhou. "Edge Chain: blockchain-based multi-vendor mobile edge application placement."2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft).IEEE, 2018.