Digital Cash: Tracking of Users in Bitcoin Transactions

Gunasundari B
Assistant Professor at Prathyusha Engineering College, Department of Computer Science and Engineering, Tiruvallur,
Nithyassree V
Final year student at Prathyusha Engineering College, Department of Computer Science and Engineering, Tiruvallur, India
Prithikca Lakshmi SP,
Final year student at Prathyusha Engineering College,Department of Computer Science and Engineering, iruvallur,India.

ABSTRACT

Digital cash is a type of cash available in digital form. It exhibits the properties similar to physical currencies, but can allow for instantaneous transactions and borderless transfer-of-ownership. In today's world, amount transfer is happening through normal banking process. The bank finds an easy and convenient option for most people, but they charge excessive fees. To overcome this, we introduce a Digital cash transfer that will happen through cryptocurrency called Bitcoin. The process of cryptocurrency transactions will be implemented by blockchain technology. The admin creates a group to add the members. Group members can add other people as a group member, only after getting consent from the admin and the other group members. The new member has permission to add the other people. The mandatory prerequisite imposed to the group members is to link their Aadhar number. Bank transaction details are extracted through their Aadhar number. If any person needs fund they have to give a request to the group members for bitcoin transaction. Anyone can give the response to that requested member. Their transaction gets proceeded through an authentication like username, password. Group Admin monitors the entire activity of the group. All the Transactions are tracked by the main Server.

Keywords - **Bitcoin, blockchain, cryptocurrency, digital cash, peer-to-peer computing.**

I. INTRODUCTION

Money transfers are widely preferred to be made on the Internet for a long time, especially in the last decade, as with many other things in this digital age. This preference comes from the speed, which is provided by the digitalization and needed in busy daily life, as well as increasing global connectivity with the rise of digital businesses and social networks. Commerce on the Internet is done assured that financial institutions and banks serve as trusted authorities. This model can be called trust-based; buyers and merchants may not trust each other. However, they trust well-known banks and banks act as trust entities managing transactions and keeping records. However, there are some disadvantages to this trust-based model. First, financial institutions act as mediators between merchants and buyers, and there exists a cost for mediation. This limits the minimum transaction size. Second, there is a possibility of reversal of transactions. Transactions can be reversed by banks if there is a dispute between the trading parties, e.g., the buyer transfers the money, but the seller does not send goods or provide services to the buyer. Merchants get information about their customers. Merchants do not have to get extra information about their customers like billing address,name,etc.When transactions are irreversible. Inaddition, irreversibletransactions protect merchants from chargeback fraud, i.e., a dishonest buyer says that he did not make the purchase. If dishonest merchants are considered, using security services may be a method for protecting buyers in the case of irreversible transactions.

The blockchain is a decentralized, distributed and a public ledger that can record transactions between two parties. It is an open source technology and a list of records called blocks. Each block contains cryptographic hash functions of the previous block. The blockchain is typically managed by a peer to peer network for communication and validating new blocks. It was invented by a person named Satoshi Nakamoto in 2008.This invention has been made in order to solve the double-spending problem without the need of trusted third party. The benefits include greater transparency, enhanced security, improved traceability, increased efficiency and speed of transactions.

Bitcoin is an open source peer to peer(P2P) network. It is the decentralized digital currency that can be sent from user to user on the peer-to-peer network without the need for intermediaries and Satoshi is the smallest unit of currency. Bitcoin uses public key cryptography. Bitcoins are the transparent payment network, since all the transactions are public.

In today's world, the internet has security problems that are familiar to everyone. So we all rely on the username/password system to protect our personal identity. Blockchain security methods use encryption technology. The basis for this called public and private "keys". A "public key" is used as an address of the user in the blockchain. A "private key" is used as a password that gives its owner can access their bitcoins for transactions. The users can pass the bitcoins to another user by digitally signing the hash of the previous transaction by using their private key. Transactions are verified by the network nodes through cryptographyand recorded in a blockchain. Data can be stored on the blockchain is incorruptible.

II. Related Work

The literature related to bitcoin anonymity and privacy, the studies that gives a brief survey by Schaffner,which is included in resources of a lecture, mentioned previous work on Bitcoin security and anonymity; however, the content and the number of studies is very limited.

ShenTu and Yu compiled research on anonymization and deanonymization in the Bitcoin system. They grouped deanonymization methods, like linking Bitcoin addresses expected to belong to the same user by blockchain analysis or network analysis, and countermeasure methods. They mentioned studies including these methods; however, there still are missing studies in this work.

Herrera-Joancomartí examined studies on Bitcoin anonymity and grouped them into three classes; (□) blockchain analysis, (□□) traffic analysis and (□□□) mixing techniques for anonymity. However, the number of the included studies is very small, and there is no further classification, or there are not any proposed properties for analyzing the studies.

A very detailed examination of Bitcoin and similar cryptocurrencies from many perspectives were provided by J. Bonneau. However, the discussion has a broader perspective compared to this study. Stability, client-side security, and alternative modification methods to the protocol are some included topics. Although anonymity and privacy issues are also included in a separate chapter analyzing the studies related to deanonymization and proposals for improving anonymity, it is kept brief, and a very limited number of studies are examined.

Narayanan published a book providing introductory information on Bitcoin and cryptocurrency technologies that includes a section on Bitcoin and anonymity.

An extensive technical survey by T schorsch and Scheuermann provided a more in-depth overview by including more studies.Nevertheless, it is not focused on anonymity and privacy, as well. Issues on security and network are discussed, and detailed investigation on Proof-of-X (PoX) schemes are done.

III. Existing System

In the Existing system, cryptocoin is commonly known as a cryptocurrency, but then still now we may know cryptocoin based money transfer is legal or illegal because there is no tracking mechanism is implemented so far in this system. All the records are destroyed after the amount transfer, so there is no authenticated system to track the money transfer which is implemented in real time.

3.1 Drawbacks

- The transaction cannot be made, in case, the bank's server is down.
- Mediator fees are charged by Banks.
- There is no tracking system to monitor the coin exchange.

IV. Proposed System

We propose a blockchain technology processed by cryptocurrency called bitcoins.The admin creates a group to add the members. The group creation is made to transfer an amount between the group members. The fund transfer is made by bitcoins. Group members are should link their Aadhar number.Admin gives permission to the group members can add other people as a group member. But the group member can add the other people to get consent from the admin and the other group members. Both provide consent then we can add other people to this group. The new member has permission to add the other people. Extract bank transaction details are made through their Aadhar number. If any person needs fund , they have to give request the group members as bitcoin. Anyone can give the response to that requested member. Their transaction proceeded through an authentication system and the whole activity is monitored and maintained by admin and the server.

4.1 Advantages

- Requires lower transaction fee.
- Fraud-proof and identity theft can be easily sorted out.
- Instant Settlements can be made.
- Aadhar number is linked , so it is easy to track the transaction made by the user.

V. System Requirements

5.1 Hardware Requirements

- Processor: Core i3/i5/i7
- RAM : 2-4GB
- HDD : 500 GB

5.2 SOFTWARE REQUIREMENTS

- Platform : Windows Xp/7/8
- Front End : Java,Java Script,Node.js
- Back End : Json / MYSQL
- Tools :Geth,Solidity,Ethereum.mist,remix

VI. Methodology Used

The proposed system consists of five modules.

In NETWORK FORMATION, Group construction is formed and members are registered in the network. Group Admin is assigned to monitor the entire activity of the group. Bitcoin based money transformation is processed through this group.

In GROUP LEADER & MEMBER GOVERNANCE, Group leader holds the complete control of the group. New member addition or Removal of an existing member will be processed by the Group admin only after the approval from all the group members. The new user can be added by any member, and the request is processed by the admin and finally, that member is added after getting approval from all the members. If group admin wants to exit from the group then the admin has to assign another member as Group admin and then that Group Admin is allowed to exit from the group.

In BANKING REGISTRATION, all the members register their Bank details for banking purpose. All these recorded are stored in the network database securely. None of the users can view the banking details of the other users.

In BITCOIN TRANSFER, one member contacts another member for bitcoin based money transfer. If the request is accepted by that member then bitcoin based money would happen in the network. All the transactions are secretly maintained in the network and also updated to the main server called RBI.

In TRACKING SYSTEM, the banking system is completely tracked through the centralized main server called RBI. This server holds complete control of the banks of all the users in that network. This module is a main advantage of the existing system of Bitcoin because there is no tracking mechanism is implemented in the bitcoin. Complete money based bitcoin transaction is tracked through this module.

VII. SYSTEM ARCHITECTURE

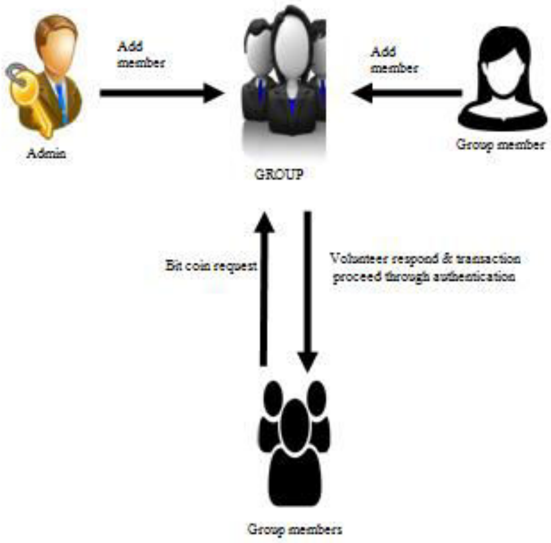
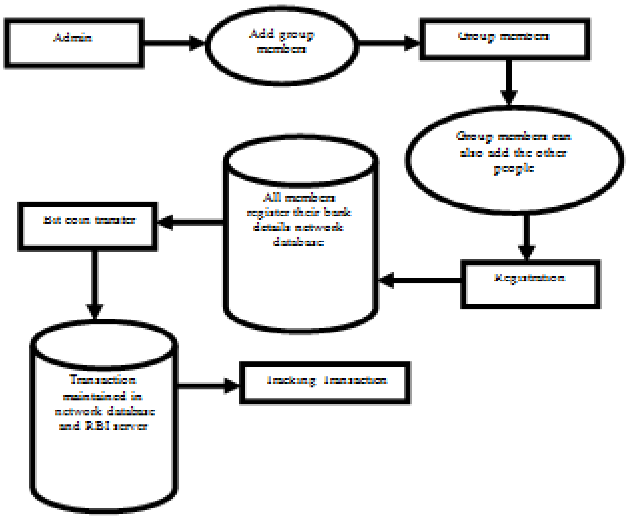


Fig:1

VIII. DATA FLOW DIAGRAM


Admin
Add group members
Group members
Group members can also add the other people
All members register their bank details network database
Bit coin transfer
Registration
Transaction maintained in network database and RBI server
Tracking Transaction

IX. CONCLUSION

Our analysis demonstrates that blockchain analysis covers the majority of the studies in this category and there are few studies on network analysis. The most used methods in blockchain analysis are multi-input and change address heuristics, which are used to link Bitcoin addresses that are expected to belong to the same user. Numerous studies exist that include proposals for improving anonymity and privacy in Bitcoin-like digital cash systems.We include aadhar as a main link for the transaction. This infers that in the existing system tracking bitcoin transaction is a challenging one. So, we use blockchain technology to secure the transaction details.

REFERENCES

[1] Herrera-Joancomartí, C. Pérez-Solà, “Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions,” Modeling Decisions for Artificial Intelligence, Lecture Notes in Computer Science, vol. 9880, pp. 26-44, 2016.

[2] Schaffner,“BitcoinAnonymityandSecurity”,2014.[Online].Available:http://www.cs.tufts.edu/comp/116/archive/fall2014/tschaffner.Pdf.Accessed: 9-Jan-2017.

[3] Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, 2016.

[4] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with accountable mixes," Financial Cryptography and Data Security, Lecture Notes in Computer Science, Springer, vol. 8437, pp. 486–504, 2014.

[5] Q.ShenTu,andJ.Yu,“TransactionRemoteRelease(TRR):ANewAnonymizationTechnologyforBitcoin,”arXiv:1509.06160,2015.