Bitcoin Service Transaction

Shilpa M, Jaritha M, Jayalakshmi G, Bhuvana B, Meghana C G
Department of Computer Science
Sapthagiri College of Engineering, Bengaluru

Abstract:- Bitcoin is the first decentralized digital encrypted currency and worldwide payment system. The system works without a central bank or single administrator. It has a peer-to-peer network. The transactions take place between users directly, and no intermediary necessary. The verification of transactions takes place with the help of network nodes by means of cryptography. Blockchain is the public distributed ledger used to read transactions. The smart coins with associated non uniformed funds for smart transactions are created. These transactions are with secured online OTP gateways with user friendly selection with volume of transactions. Fully service oriented architecture has to be online with asynchronous transactions facility and automated with selective transactions with email security gateway (OTP). This way transactions will carry on with fully non distributive model with a new framework (in this work we created a new framework called CST). So transactions with funds framed from coin's funds is reduced and visually appears to the user.

Keywords:- *Cryptocurrency, blockchain, gateway, OTP.*

I. INTRODUCTION

Bitcoin is a digital currency system proposed by Satoshi Nakamoto and then gained popularity due to its invisibility and decentralized design characteristics. One core technique of Bitcoin is called Blockchain, which is a peer-to-peer ledger system keeping track of all bitcoin transactions and the order of the transactions. The set of bitcoin transactions are recorded in blocks. Owners of bitcoins can generate new transactions by broadcasting blocks of the transactions to the Bitcoin network. Then, a process called mining confirms the transactions and includes the transactions to the Blockchain. Essentially, mining is a randomized distributed agreement of component that confirms pending transactions by including them in the Blockchain.

To process electronic payments, the financial institutions serve as trusted third parties, where the online commerce relies on it. Even though the system works fine for most of the transactions, trust based model is its major weakness. It is not possible to perform completely non-reversible transactions, since financial institutions cannot give up on mediating disputes. The transaction costs are raised due to the raised median cost and also limiting the minimum practical transaction size and lowering the possibility for small casual transactions, and there is a greater cost in the loss of ability to make non-reversible payments for non-reversible services. As the possibility of reversal is needed, the need for trust becomes essential. Vendors must be careful about their customers, not giving out more information than they would otherwise need. A certain percentage of fraud is accepted as unescapably. There is no existing mechanism to make payments without the trusted party, expect for the transactions with physical currencies. Cryptographic electronic payments are the major alternative for trusted third party system. The main objective of work is, in the existing scenario bitcoins mechanism was selective and equally distributed and the transactions were also equally distributed. But by using randomly distributed artificial intelligence mechanism, the transactions are user independent for the chosen coin frequency, as the procedure is offline hackers cannot easily intrude into the transactions, or obtain the amount details. This is unstable and unstructured flow. Transactions are limited in the existing scenario, which is enhanced.

II. RELATED WORK

A. Social media networks Fraud

Everybody is tending to use the e-wallet in the current situation of currency demonetization. Among the e-wallets, simpler and useful for making money is the Bitcoin wallet. A trusted confirmation is required for bitcoin transactions. Anju et al [1] proposed a framework; bitcoin trading including the social media which is new method was introduced. A trusted confirmation can be got from friends in a friend circle of a social media. But still by using the information of real users some fraud identities can create fake news about bitcoin trading. The system blocks the fake posts and reports about fake identities in such situations.

B. Use of digital signatures to prevent double spending

Online payments would be allowed to be sent directly from one party to another without going through a financial institution by a purely peer-to-peer version of electronic cash. The main part of the solution can be digital signatures, but in order to prevent double spending trusted third party is still required where its benefits are lost. Satoshi Nakamoto [2] proposed a solution using a peer-to-peer network for the double-spending problem. When forming a record that cannot be changed without redoing the proof-of-work, the transactions are time stamped by network by hashing them into an ongoing chain of hash-based proof-of-work. The proof of the sequence of events witnessed and the proof that it came from the largest pool of CPU power is the longest chain. They'll generate the longest chain and outpace attackers as long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network. A minimal structure is required by the network. On a best effort basis messages are broadcasted, and nodes can leave and rejoin the network, accepting the longest proof-of-work chain as proof of what happened while they were gone.

C. Bloom Filter Implementation

Kota et al [3] have proposed a privacy-preserving Bloom filter design for Bitcoins' SPV (Simplified Payment Verification) client based on ϒ-Deniability. Although it has been said that introducing Bloom filter improves the privacy

level of an SPV client, none of the specific privacy metric is specified.

D. SMS system to access bitcoin wallet

Kishor Krishnan et al [4] presented a method to acquire a Bitcoin wallet and access it using a low-end mobile phone, just by sending an SMS. This system was developed as a proof of concept and to demonstrate its feasibility, but it still requires other functionalities for it to be a fully functional system that can be made available to people.

E. Study of security flaws in bitcoin to affecting currency value

John et al [5] investigated whether the security flaws surrounding Bitcoin have affected the value of the currency. The results gathered in the resulting investigation suggest that security flaws and security breaches in Bitcoin services have been the greatest factor contributing to the drop in value of Bitcoin. The underlying Bitcoin protocol has only once caused a drop in value and has never succumbed to a targeted cyber-attack. The conclusion drawn from these results is that the Bitcoin technology is strong enough to gain mainstream popularity and could rival traditional technologies. The high volatility of the value of Bitcoin is not as a result of the underlying technology but instead as a result of Bitcoin services not being strong enough and being compromised by various parties.

III. SYSTEM ARCHITECTURE

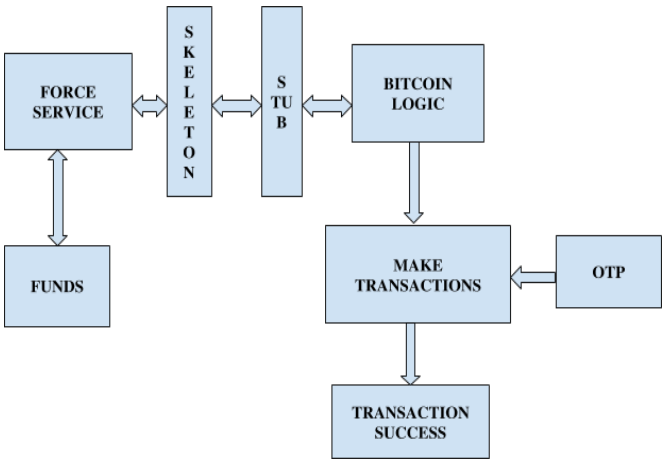

Fig 1:- Bitcoin service system architecture

A. Force service

The service lies on the main server, client can access this service by using bitcoin algorithm explained below, the service has to be activated before the coin generation and transaction. The service checks if the client is in the blocklist if so, he will be not allowed to perform transaction. This service will assist in collection of amount from various banks and coin generation.

B. Stub

To present the simple invocation mechanism to the caller, the network-level communication and serialization of parameters is hidden. This task is accomplished by stub.

C. Skeleton

The call to the actual remote object implementation is dispatched by skeleton. Every remote object will be having a corresponding skeleton, in case of remote JVM but the Java 2 platform-only environment doesn't require any skeleton.

D. Bitcoin logic

Here the randomly distributed artificial intelligence is used to distribute the amount to each coin and again distribution at each transaction using same mechanism takes place.

E. One Time Password

The disadvantages of traditional password-based authentication were overcome by OTPs. Two factor authentication is incorporated by number of implementations ensuring that it require access to something a person has such as a small key. The reversal of the function used to create otp is difficult and hence the attacker cannot obtain the data that was used.

IV. THE PROPOSED ALGORITHM

➢ *Algorithm for service*

Step 1: The individual funds is updated to a variable Up, which is integrated and stored in Bk, where Bk is the total funds from various banks.

$$Bk = \int_0^{n-1} Up$$

Step 2: The recent user's bank details and the information about the funds is stored in cache which is indicated as Fs. c1 refers to customer one and CACHE is a storage area for the funds.

Fs (c1) = CACHE (Bk)

Step 3: GET is used to obtain the total money from the fetched details of each user, Tm is a variable where the total money is stored.

Tm = GET (Fs (c1))

➢ *Algorithm for bitcoin logic*

Step 1: Initialize the value of λc, where λc is the total number of coins.

Step 2: Store the total money in a variable Tm.

Step 3: The amount in first amount is divided equally and assigned to next coins.

Tm [1,2] = Tm/2

Step 4: The funds from the above generated coins will be randomly divided to further coins.

temp1 = Tm [1,RAND]
temp2 = Tm [2,RAND]

Step 5: Calculate Tm[3], which is the value of the third coin. This process is repeated for any number of coins specified in the input.

Tm[3] = temp1 + temp2

Step 6: The value Tn is initialized i.e, the number of transactions. In each transaction the division of the amount to coins is performed as in step 3 and step 4.

V. IMPLEMENTATION

First the service has to be started, Service will be created on SOAP architecture with SOA model. At service side solid skeleton has to be generated for DOM or SAX parsers to parse the broad casting XML envelopes. Normally SOAP transmission will take in the form of XML only and these XML envelopes will be parsed by skeleton at service side and stub at client side. User registers into the system presenting his unique username and password which will be stored along with his various bank account details like the amount he wants to transact through bitcoin wallet. Once the user wants to perform the transactions of the amount in his bitcoin wallet, user logs into the system using his credentials. Now the system validates his login credentials with the existing accounts. If the user holds the account in the bitcoin wallet the total amount from various banks is calculated. The user decides on the number of coins necessary for the transaction. The distribution of the amount to each coin is displayed where the coin distribution happen using randomly distributed artificial intelligence. Next the frequency of transaction has to be given by the user. In order to select the transaction secondary verification process like OTP generation is initiated, OTP will be generated with 4-roll algorithm and with capital letter with numeric ceiling with proper security and will be sent as mail for further transactions. The email is implemented in gateway model and OTP will be sent using ROTA algorithm for encryption and decryption. If the verification is not satisfied the transaction fails. On the successful verification, user selects the number of transactions. The amount is distributed from each coin to various transactions using randomly distributed artificial intelligence. The final outcome is displayed in the graphical format, which indicates the distribution of amount to various coins in each transaction.

VI. RESULTS

It is the choice of the user to decide on the number of coins to which the money in the account has to be distributed and the number of transactions that has to be performed from the coins.

The figures show the distribution graph when the user chooses three coins and three transactions. In every transaction graph the amount that is remaining after the distribution is depicted and hence in the last transaction graph the amount remaining a null since the transactions is completed. The distribution of funds is user independent, the user himself is unaware about the transaction fund details and hence it is protected from the third party interference. As the system works offline, the intruders through online details cannot obtain the transaction information and hence the system is secure.

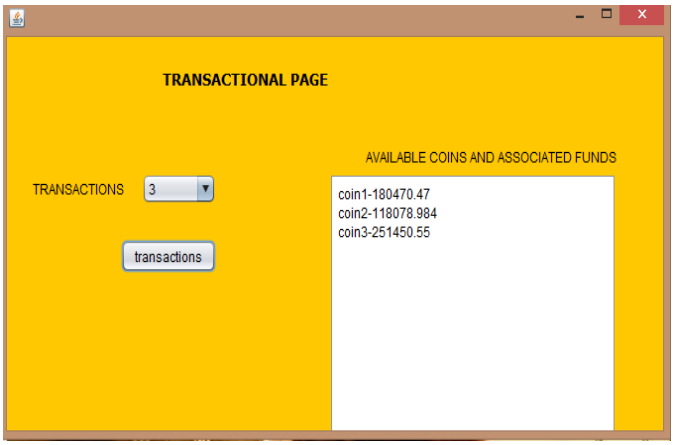

Fig 2:- Coin value and frequency of transaction

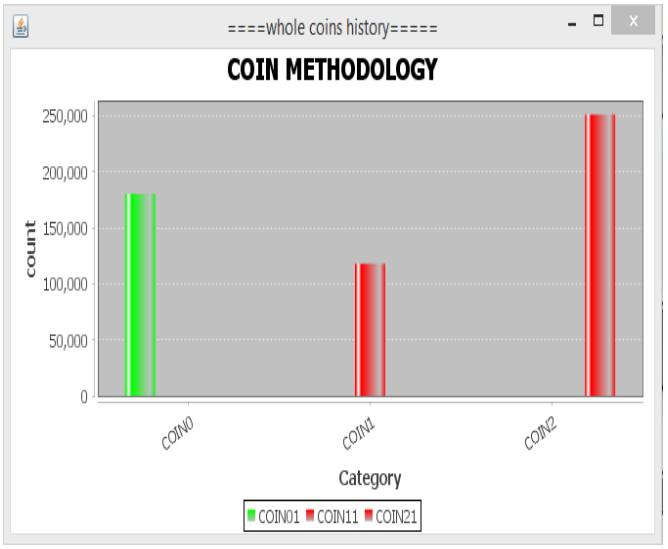

Fig 3:- Whole coins history

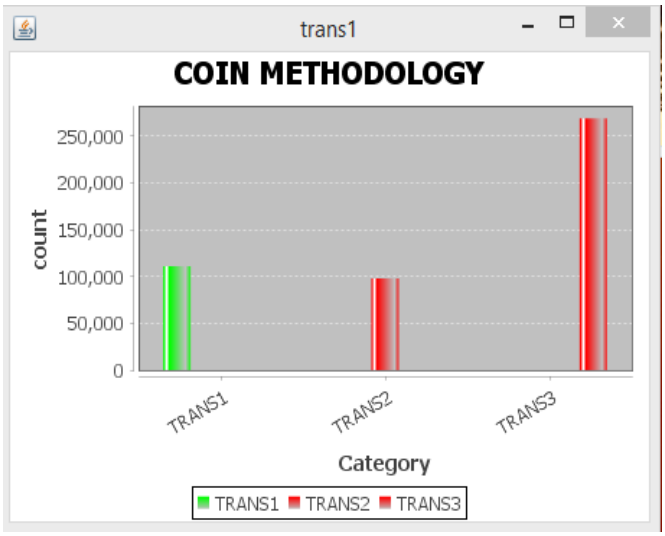

Fig 4:- Initial transaction graph

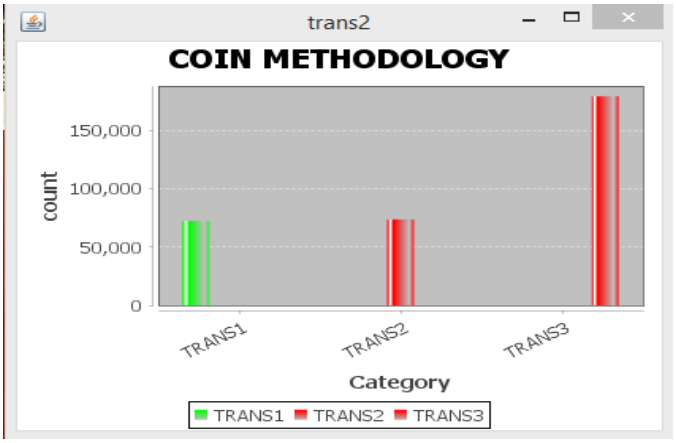

Fig 5:- Transaction 2 graph

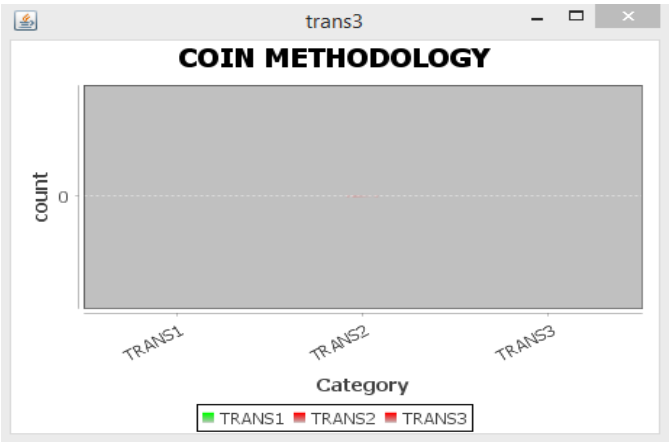

Fig 6:- Final transaction value when the user chooses three coins and three transactions

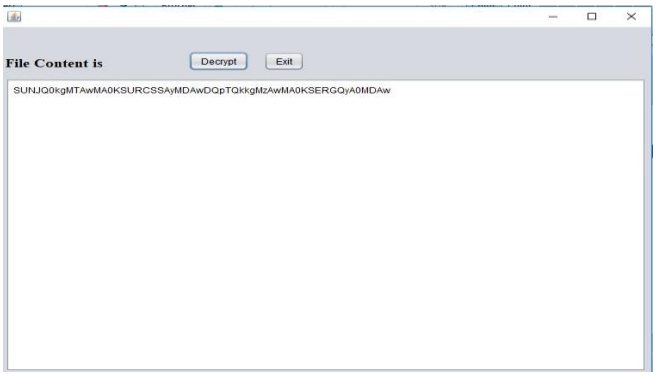

Fig 7:- The encrypted bank details

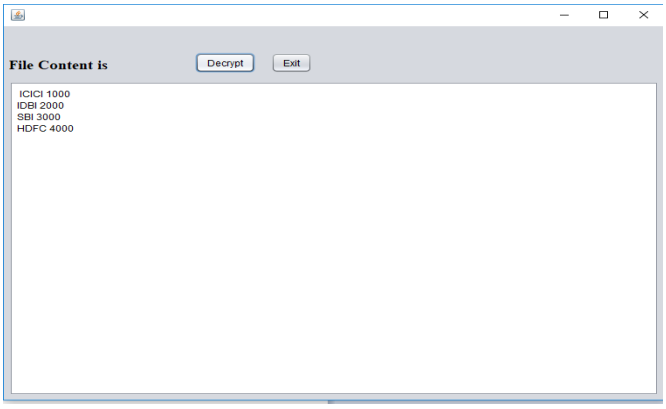

Fig 8:- The decrypted bank details

VII. CONCLUSION AND FUTURE WORK

We have described how our solution provides a higher security level without any trust worthiness assumption over the devices involved in the payment protocol. Limiting data access in a physical device is extremely difficult problem. The possible outcome is, by using the Randomly distributed AI model of forward and reverse engineering the transaction can be done in the form of bitcoins. With respect to the choice of coins and transactions required by the user, the distribution of amount is user independent. As the system runs offline, it can protect the transactions from cybercrime or third party interference through online data. Usage of OTP (One Time Password) is an enhanced second level security for the system. The financial intermediates like the government or banks cannot interrupt the transactions of the user, which is the major benefit of the bitcoin account. We are working on an enhanced version that will allow digital credit to be spent in multiple offline transactions while maintaining the same level of security and usability.

REFERENCES

[1]. **“**An Efficient Bitcoin Fraud Detection In Social Media Networks **”** , Anju Viswam , Gopu Darsan , 2017
[2]. “Bitcoin: A Peer-to-Peer Electronic Cash System” , Satoshi Nakamoto
[3]. “Design of Privacy-preserving Mobile Bitcoin Client Based on ϒ-Deniability Enabled Bloom Filter”, Kota Kanemura, Kentaroh Toyoda, Tomoaki Ohtsuki, 2017
[4]. “Development of an SMS System Used to Access Bitcoin Wallets”, Nelisiwe Peaceness Dlamini, Mfundo Shakes Scott, Kishor Krishnan Nair, 2017
[5]. “Have the Security Flaws Surrounding Bitcoin Affected the Currency's Value?”, John Gregor Fraser and Ahmed Bouridane, 2017
[6]. ”Introduction to bitcoins: a pseudo-anonymous electronic currency system.” Martins, S. and Yang, Y. (2011).
[7]. ”Fully Off-line secuRe CrEdits for Mobile Micro Payments”, Vanesa Daza, Roberto Di Pietro, Flavio Lombardi and Matteo Signorini, 2014.
[8]. ”An improved off-line electronic cash scheme”, Wang, C., Sun, H., Zhang, H., and Jin, Z, 2013.