APPLICATION OF BITCOIN AND CRYPTO-CURRENCY

[1]*Nikhil L. Deore,* [2]*Ganesh B.Bagul ,*[3] *Ashwini N. Kannade,* [4]*Surabhi M. Landge,*[5] *Prof. Satish T. Pokharkar*
[1,2,3,4] *Students, Department of Computer Engineering, Savitribai Phule Pune University, Pune*
[5]*Professor, Department of Computer Engineering, Savitribai Phule Pune University, Pune*

ABSTRACT: *This project presents an application based on crypto currency called Bit-coin to carry the safety online transaction using Bit-coin wallets. Bit-coin is one type of digital currency. It becomes very necessary to provide high level security for this online-transaction so that we can make it reliable for any type of user. In this system, we are providing three way securities. We are using 3-D security algorithm, PKI infrastructure, and threshold signatures algorithm. To provide high level security to Bit-coin wallets & online transactions. We are giving each user a unique 3-D image & he has to choose 4 specific points in that image in proper sequence for 3-D security. PKI is utilized for encryption. Threshold signature is new technique for providing secure authorization by user.*

KEY WORDS: *Digital currency, PKI, 3-D security, Threshold signatures, SHA-256*

I. INTRODUCTION

Bit-coin is a digital cash and payment system invented by Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009. The system is peer-to-peer users can exchange directly without needing an intermediary. Transactions are affirmed formally by network nodes and accumulated in a public distributed register called the block chain. The register uses its own unit of account, also called Bit-coin. The system works without a central depository or single administrator, which has led the US Treasury to categorize it as a decentralized virtual currency. Bit-coin is often called the first crypto-currency, although prior systems existed. Bit-coin is more correctly depicted as the first decentralized digital currency .It is the giant of its kind in terms of total market value.

Bit-coin as a form of payment for products and services has grown, and merchants have a reward to accept it because fees are lower than the 2 to 3 percent typically imposed by credit card processors. Unlike credit cards, any fees are discharged by the purchaser, not the vendor. The European Banking Authority and other sources have cautioned that Bit-coin users are not protected by refund rights or charge backs. Trotz a big increase in the number of merchants accepting Bit-coin, the crypto-currency doesn't have much impetus in retail transactions. A crypto-currency is a medium of exchange using cryptography to secure the transactions and to be wield the creation of new units. Crypto-currencies are a subset of alternative currencies, or distinctively of digital currencies. Bit-coin became the first dispensed crypto-currency in 2009.Since then, numerous crypto-currencies have been created. These are frequently called Alt-coins, as a blend of Bit-coin alternative. Crypto-currencies use dispensed control as opposed to centralized electronic money/centralized banking systems. The dispensed control is related to the use of Bit-coin's block chain transaction database in the role of a distributed ledger.

II. LITERATURE SURVEY

- ***Bit-coin:*** A peer-to-peer Electonic cash system & Satoshi Nakamato& 2008-10-31/Paper & Basic theme of Bit-coin. Its merits and demerits discussed.

An analysis of anonymity in the Bit-coin system & Fergal Reid, Martin Harrigan& 2011-07-22/Paper & Anonymity is analyzed and measures suggested removing anonymity.

- ***Bit-coin:*** An innovative alternative digital currency & Reuben Grinberg& 2011-12-09/Paper & First use as a digital currency.

Secure multiparty Bit-coin anonymization & Edward z. Yang & 2011/Article & Security is improved.

- ***Commit-coin***: Carbon dating commitments with Bit-coin & Jeremy Clerk & Alexander Essex & 2012/Paper & Conceptualization with carbon dating commitments.

III. PROPOSED SYSTEM

A) User module

In this module users are there. For each and every transaction there must be some user or human who are interested in online transactions. User may be a valid user or an invalid user or it may be an attacker. For this we must give a condition to check whether this user is a valid user or an invalid user or an attacker. After that we can get a use this module. User is one of the entity required for our project. It is acclaimed by 'U'.

B) Bit-coin converter module

In this module we are converting the actual currencies in a virtual currency called as Bit-coin. Bit-coin is a payment system invented by Satoshi Nakamoto who published the invention in 2008 and released it as open source software in 2009. There is no utilization of a central repository / single administrator, which has led the USA Treasury to categorize it as a decentralized virtual currency. Bit-coins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into

public ledger. This activity is called mining and miners are rewarded with transaction fees and newly created Bit-coins. Besides mining, Bit-coins can be obtained in exchange of different currencies, products, and services. Users can send and receive Bit-coins for an optional transaction fee.

Bit-coin is commonly referred to with terms like: digital paper money, digital cash, virtual paper money, electronic currency or crypto-currency. The price of Bit-coin has gone through various cycles of appreciation and depreciation referred to by some as bubbles and busts. in 2011, the value of one Bit-coin rapidly rose from 0.30$ to 32$ earlier returning rear to 2$. In the latter half of 2012 and during the 2012-2013 Cypriot Financial Crisis, the Bit-coin price began to rise, reaching a high of $266 on 10 April 2013, before crashing to around $50. On 29 November 2013,the cost of one Bit-coin rose to all-time peak of $1242. In 2014 the price fell sharply, and as of April remained depressed at little more than half 2013 prices. As of August 2014 it was under $600. In January 2015, noting that the Bit-coin price had fallen to its lowest level since spring 2013 – around $224.

C) Transaction module

In this module we are dealing with the on-line transactions. Transaction is a process, in which we can transfer the money, or we can buy any product, or we can have some deals on shares in stock market. Each n every single process can be counted as a transaction, butt herein we need to take care that no any transaction can be get duplicated for that we have another module known as a key generation module. Transaction is also one of the entities. It can be denoted as 'T'.

D) Attacker module

In this module we are dealing with an attacker. Attacker is such a user which is not a valid user as well as it is not an invalid user but it is a user which having some harmful motives like attacking on a transaction or carry out some fake transaction, etc. For each and every attacker our system will generate an alert. Attacker is an entity required for our project and it is denoted as 'A'.

E) Alert generation module

In this module we are going to generate alert. For each user which is an attacker system can generate an alert. Which is simple alert message shown in dialogue box/pop up window? Alert is an entity which is denoted by 'X'.

F) 3-D security module

In 3-D security module for each and every user we give 3-D security for his all transaction by giving him an unique 3-D image. He has to choose the points in that image by simply clicking on those points. But these points should be selected in the order. If false points are selected by the user then that transaction will not be authorized by system. Also if points are not selected in the same order then also the transaction will be cancelled and user is treated as invalid user.

Key generation module

In this module we are going to generate keys. Each user having 'n' number of transactions then how system can identify n distinguishes between them. For this purpose we are going to generate an unique keys for each transaction. Each user has 'n' number of transactions, and for each transaction there will be a key which is unique. So if there are 'z' numbers of total transactions then system can generate same number of keys. Key is an entity which is denoted by 'K'.

G) Threshold signatures module

A threshold signature is the new and innovative approach we have introduced in the proposed system. In this module we have break the key in two similar threshold signatures. From which only one threshold signature is given to the user. And the other signature is stored in the system database. When any user wants to do some transaction then these two keys are matched after that the whole key is verified if it matches then and then only the transaction is successful otherwise it is all the way discarded or cancelled.

H) Payment get-way module

In this module we are going to select an payment gateway for a transaction. There are many numbers of payment gateways, system have to select a suitable payment gateway for each and every transaction. Payment gateway is an entity which is denoted by 'P'.

I) Logs module

In this module we are dealing with the logs maintained by a system. Or it can be called as consensus. For each and every user there are 'n' numbers of transactions. All these transactions are stored in logs. So that if any user wanted his statement over an specific time period then system can be able to give his statement by using particular logs. Each user has its separate log so if there are 'n' numbers of users then there will be same numbers of logs in system. Log is an entity which is denoted by an 'L'.

In this way we divided the whole project into these seven modules so that we can easily make project, n that too with very great accuracy and precision. Typically each project has some different modules in it so that developer can easily build up software which can be comfortable. Also if we use divide and conquer strategy then it will assist the testing too. Literally we can say that the project work can be made comfortable and easy by using divide and conquer strategy.

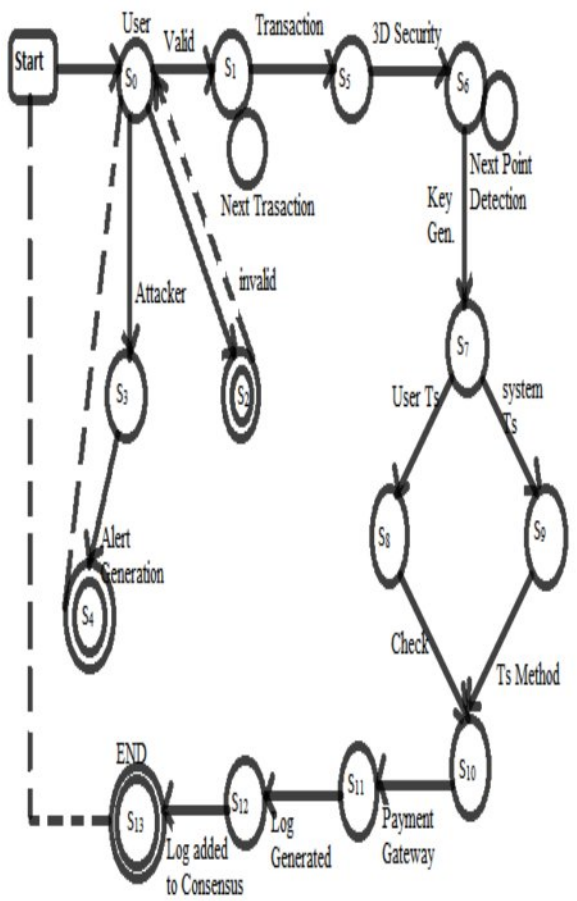

Figure 1: Proposed System Flow

IV. CONCLUSION

So after removal of all the flaws in the existing system, proposed system becomes superior over the existing system. Also the 2-layer security of the proposed system made it most reliable. So the wide user range is available to the proposed system. Also we have used very new and innovative security option known as threshold signatures.

We have reduced the updation time interval to 5 minutes i.e. 12 time period in 1 hr. So these all advantages made it as the best system over the existing system.

REFERENCES

[1] G. Andresen. March 2013 Chain Fork Post-Mortem. BIP 50.

[2] A. Back et al. Hashcash-a denial of service counter-measure, 2002.

[3] A. Biryukov and I. Pustogarov. Bitcoin over Tor isn't a good idea. In IEE Symposium on Security and Privacy, 2015.

[4] D. Chaum. Blind signatures for untraceable payments.In CRYPTO 1982.

[5] M. Corallo. High-speed Bitcoin Relay Network, November 2013.

[6] G. Andresen. Pay to Script Hash.BIP 16, 1, 2012.

[7] R. Grinberg. Bitcoin: An Innovative Alternative Digital Currency, November 2011.

[8] M. Hearn. Dan Kaminsky's thoughts on scalability.bitcointalk.org, 2011.

[9] M. Hearn. Merge-Avoidance: a note on privacy-enhancing tech- niques in the Bitcoin protocol. medium.com, 2013.

[10] M. Hearn. Rapidly-adjusted (micro)payments to a pre-determined party. bitcointalk.org, 2013.

[11] J. Herrera-Joancomart. Research and Challenges on Bitcoin Anonymity. Keynote Talk: 9th International Workshop on Data Privacy Management, 2014.

[12] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko. Botcoin: monetizing stolen cycles. In NDSS, 2014.

[13] jav.Instawallet introduces new approach to instant payment: Green address technique. bitcointalk.org, July 2011.

[14] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In Workshop on Bitcoin Research, 2014.

[15] Bit coin magazine