Centralized Bank Digital Currencies (Ethereum)

[1]Triveni Yadaw and [2]Sumit Sharma
[1]Master of Computer Science, [2]Head of Computer Science Department
[1, 2,] Computer Science
[1, 2]Vaishnavi Institute of Technology & Science, Bhopal, India

Abstract: The digital word has change efficiencies of our world, daily invention in technology and in ideas changes the global relationship, as the discovery of mobile, internet and social media share a platform of freedom- gives better opportunity for better decision. To shot out the Chios of financial model the overture of cryptocurrency into existence. A blockchain is revolutionizing the digital world by introducing to new prospective such as efficiency, security and resilience. In today's world Bitcoin is more popularized where asblockchain is a foundation for cryptocurrency. It approaches to secure way of trade such as services or transaction. The rapid growth in trusted partnership among industries inhabits expansion in rate of fraud, regulation and cybercrime. The use agile value of blockchain like quicker integration, close customer relationship and faster innovation in product with integrated approach with IoT and Cloud technology can give attention to on these challenges. Furthermore it provides solution with trusted contract with removing third party interference at low budget cost without any direct value addition. To posses inherent, robust security features can be facilitates with agreement, contracts and engagements. In my thesis an effort to show case study to demonstrate, the use cryptocurrency in multiple industrial and banking applications under Blockchain.

Keywords: Bitcoin, Ethereum and cryptocurrency

I. INTRODUCTION

The application of mobile phone, internet and digital card has change the mode of payment from hard cash to digital cash. These create an innovative money payment in today's digital world. The alternative mode of digital payment such as PayPal, Payatm, M-Pesa, Airtel Money, Moven, Bhim and Google Wallet has been encouraging people for direct transaction rather building trust on any another third party.

For faster, more flexible and more innovative payment method for financing goods and services- A growth in use of digital currency is more likely acceptable beyond fiat currency. To have outstanding currency with more trust is only one that is Bitcoins in our digital world [1]. To be specific, it is a cryptocurrency which is a small part (subset) known to the current world in universe of digital currency.For instance the Bitcoin is one which is widely acceptable to the world in country like Japan [2]. To create a Bitcoin it uses the highest computational power of internet and huge amount of electricity to mine a single coin for process of transaction.

*JaysingBhosale and SushilMavale*in his paper explains increasing use of virtual currency and its volatility, cryptocurrencies are being adopted across world for various transactions- legal and illegal. The return received behalf of investment in cryptocurrency has raised the question on its credibility and existence in future with same returns. It is secured by cryptograph for securing virtual currency. In many cryptocurrency only Bitcoin is ahead of all of its kind and resulted in a number of companies to promotion alternative cryptocurrencies as new currency. Our main focus is on three major type digital currency- Bitcoins, Ethereum and Litecoin according to their stability and vulnerability in recent time [3].

Andrew Miller and Arvind Narayan focus their research into cryptocurrencies for a decades-long pedigree in academic world, but decentralized cryptocurrencies (starting with Bitcoin in 2009) have drive the world by tempest. The payment mechanism that is "indigenous to internet" underlying blockchain developed technology, touted a way for transaction and store information like property record or receipt for everyone [4]. To a great extent of this improvement happen in the broader hobbyist and capitalist communities (with growing interest from recognized industry players); Bitcoin itself came from outside college circles. The gusto attitude of researcher has shown valid contribution insights.

II. BITCOIN AND CRYPTOCURRENCY

The first bankrupt of public money in USA focused to research in ways of transaction to secure money in both end of parties by elimination of third party as server. This was first proposed by Rivest, Shamir, Adleman. They choose two large different prime number *p, q* and calculate

$$n = p*q$$

They name the other unknown variable as Ø, which is calculate

$$Ø = lcm(p - 1, q - 1) \text{ \{LCM=Least Common Factor\}}$$

Now we calculate gross Cumulative distribution as 1 and we have to assume a value of e such a ways that it remains it outcome as unity in defined function

$$gcd(e,Ø) = 1$$

We required to calculate *d (Alice's secret key)* such that

$$d = e^{-1} mod Ø \rightarrow e \times d = 1 \text{ } mod \text{ } Ø$$

This gives Idea to for the function represented as

$$m^{e\times d} = m^{e^{d}} = m \text{ } modulo \text{ } n$$

To encrypt the code we have to write in such a way that it always approaches its maximum value encryption:

$$c = m^{e} \text{ } mod \text{ } n$$

To know or to decode the code we need decryption of encrypted code:

$$p = c^{d} \text{ } mod \text{ } n$$

The foremost aim is to convince everybody that Alice have signed the document and nobody should be capable to forge the document by straightforward pasting a copy of signature should not work. The idea to secure, we have to use RSA. For document m Alice uses s = m^{d} as her digital signature. To authenticate and verifier calculates s^e and if $m = s^e$ mod n, signature is genuine. Therefore d is called Alice's secret key and e is called Alice's Public key.

Is the Scheme secure? The answer is No. Because it is given as (n, e) for confidential (private) key of Alice which cannot be calculated due to the given document m, $s = m^d$ could not be guessed.

The difficulty is that forging of given m_1, m_2 as two documents, and s_1, s_2 as their digital signature, one can find the valid signature of $m_1.m_2$ as $s_1.s_2$ and also the size of document is proportional to its length of signature and slow computational. So how it can be resolved?

To resolution this function we have to use SHA (Secure Hash Function)

An idyllic Hash function is one which has following properties

1. given f (x) it is impossible to guess x
2. given x_1 it is impossible to find x_2 such that $f(x_1) = f(x_2)$
3. it is impossible to find x_1, x_2, such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$

III. MERKLEDEMGRAD CONSTRUCTION

Need of padding message m? And achieved by

Where m is prefix of PAD (m) then following condition is formed

$$\textit{if } |m_1| = |m_2| \textit{ then } |PAD(m1)| = |PAD(m2)|$$

$$\textit{if } |m_1| \neq |m_2| \textit{ then the last block of } PAD(m_1) \neq PAD(m_2).$$

IV. BITCOINS

4.1 CRYPTOCURRENCY

4.1.1 The character of cryptocurrency

An original cryptocurrency has peer-to peer cash transfer through electronic cash. It make online payment directly from one party to another party without approaching to any another financial institute like our banks. The cryptographic is used as trust building (as proof of work) as the time-stamps at the time of transaction. It follows the protocol by basically by contest of decoding and accessing to rewards as incentive those who take part in it [5]. For first participant with crack code will be rewarded with newly developed coins. This hunt forms a record of a transaction and cannot interfere without redoing the proof of work.

Cryptocurrency is a small part of digital currency. As respective country currency can be used in their respective country only and face problem as it cannot be used globally, for example Indian Rupee can only be used in India rather than any country, and the person has to make exchange the currency with paying some amount of money-where as it not needed in cryptocurrency.

4.1.2 The establishment of E-Cash

Commercially, it all began with DigiCash, Inc.'s eCash system in 1990, based on two papers by its founder (Chaum, 1983; Chaum et al., 1992). They tested their system by transferring online and offline payment using crypto graphical method to avoid double spending. Its protocol is also made in such a way that it uses blind signatures to protect user. The first cryptocurrency was used by various banks of United States and Finland for electronic cash transfer via bank and card was made successful. In last 26 years it was developed by various software developers to bring it into current state.

4.1.3 The rise of Bitcoin

A model of a cryptocurrency is bitcoins. Satoshi Nakamoto in year 208 published a paper on the Web for a peer-to-peer electronic cash system and it become viral and all focus after financial crises in USA also help people to again move around clock to find new financial model Satoshi come into picture. Despite many efforts to find the identity of Satoshi remains, it remains unknown to the public as it is a person or group of person [1].

Satoshi Nakamoto invented the cryptocurrency and named it bitcoins, which is open-source software. It means it can be downloaded by anyone from anywhere. And every node of computer terminal is connected to one another and functions on a decentralized peer-to-peer network. For authoritative record every node is allowed to connect and leave at their will and can have longest proof of work (Blockchain). Hence longest blockchain is a proof of events happened while nodes are absent. There are few reasons due to which cryptocurrency is called mysterious and misunderstood.

First, no one knows behind the system of cryptocurrency who exist. As it was designed in such a way that there is no need of third party and any legal entity as it is open-source software.

Second, many have without being serious remarked that Bitcoin sounded like "big con" particularly after the collapse of Mt. Gox. But it is significant to note that Mt. Gox was simply a financial mediator, being just one of numerous unregulated interactions that trade in Bitcoins. Mt. Gox does not have any part in system of Bitcoin. It is a multifarious currency system to the men in the street and therein lays dilemma of confusion.

The person who solve cryptography problem first gets the rewards of mining. The cryptocurrency is so cleverthat it solve the problem of double spending, so it can be used once only. In addition to financial technology the governance of regulation becomes difficult even for professionals working on it as it was mystery that who developed and how. This is the reasons to attract researcher, investor and regulatory and always hitting headlines in prompting future. The general point of view for a successful circulated cryptocurrency is as follows [6]:

1. Open-source software: It is essential to verify the code for possible changes for adoption required a core and trusted group of developers to maintain the network.
2. Decentralized: Although it is not fully distributed, to keep it secure it is essential that it is controlled by a group of person or entity.
3. Peer-to-peer: the major responsibility is to remove the third party as trust.
4. Global: The currency can be accepted globally and this will provide financial integration with or without legal contracts among the geographical area or parties.
5. Fast: The speed of transaction can be faster and confirmation time can be shortened.
6. Reliability: The advantage is that it eliminates settlement risk and another aspect is that it saves a large settlement cost invested on financial recovery team for financial activities.

7. Secure: Privacy architecture can be better designed incorporating proof of identity with encryption. If that is done, the issues nearby to Know Your Customer/Client (KYC) and anti-money laundering and terrorist financing (AML/TF) will be resolved.
8. Sophisticated and flexible: The system will be able to cater to and support all types of assets, financial instruments, and markets.
9. Automated: For payment and contract algorithm can be executed easily.
10. Scalable: The millions of users can use this system at a time.
11. Platform for integration: It can be considered to integrate digital finance and digital law with ecology to sustain elegant contracts with financial transactions.

The potential applications will be across-the-board and include worldwide payment and transfer of funds systems, decentralized exchanges, commercial solutions, online gaming, and digital astringent systems. Every cryptocurrency is an immense and an attention-grabbing experiment.

Though it smart accounting or smart contract, it will change the way business is being done by thinning the role of the middleman and directly connect user and seller. It will also put new mile stone in financial model in raising money or lending it. Basically, it is done by crowd offering at initial level or crowd lending at the same stage all by using peer-to-peer network for removal of third party (middleman).

However, there is dark side or potential risk of cryptocurrency too as it depends upon mining and once the incentive mining disappears-no one is able to know. To overcome such issue there should be legislation required for it, for this instance of reasons RBI (Bank regulatory body of India) did not considering it. Till to date there are 400 cryptocurrency in approx and number increasing daily basis, but still may are in graveyard and needed to be mined [7].

4.2 A Decentralized Ledger

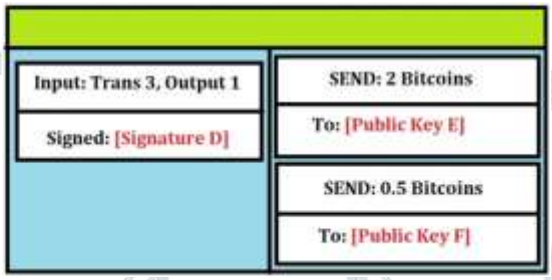

Figure 1: Decentralized Ledger for Transfer

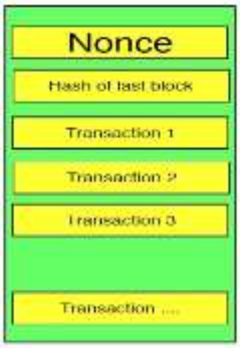

Figure 10: Decentralized Ledger for Transaction

Bitcoin has advantages of Security, transparency, no counterpart risk, decentralized, Privacy and low transaction cost. The Bitcoing (the processes of mining bit coins) is Awesome! But Block creation time is very high 10 mins/block and Block confirmation time is very high 60 mins/block can only do one function. Cryptocurrency uses too much of energy-by 2020 electricity equivalent to entire Denmark.

4.3 Ethereum

A planetary scale computer builds on blockchain technology which is permission-less by turning complete language. It begins the era of Decentralized app: Program that can run without failure, without any downtime, censorship, fraud or third party inference.

4.3.1 EVM: Ethereum Virtual Machine

EthereumBlockchain is Blockchain with built in programming language decentralized massive database, where the recent state of every account is stored EVM handles internal state and computation. Computation is paid in Ether, per computation step each account object have: Its own internal state has 32 byte key/value called storage that can call or send messages to supplementary node [8].

4.3.2 Basics of Ethereum

Ether: the underlying cryptocurrency of Ethereum
Gas: Gas is a basic unit of computation
Smart contract: Pre-written logic (code) that can be stored and computer-generated on blockchain by self executing by running the code along with update of blockchain. It can do transfer of assets and run code to make payment

4.3.3 Account types

There are two type of account in Ethereum

[1]. Externally Owned Accounts
[2]. Contract Accounts

4.3.4 Externally Owned Accounts

Has ether Balance which can send transactions (Ether transfer or trigger Contract code). It is controlled by personal keys and does not have associated code.

4.3.5 Contract Accounts

Has associated Ether balance and associated code. In such account the code implementation is triggered by transaction or messages received from other accounts. It can execute code of arbitrary complexity (Turing Completeness) and manipulate data in blockchain

4.3.6 Transaction

Transaction Contains receipt of the message and signature for Value amount of wei to be transferred from sender to recipient. It has optional data field which contains message to be send to recipient. Start gas value represent the maximum number of computational steps in the transaction execution is allowed to take

4.3.7 Mist: Introduction

Mist Ethereum wallet is a Desktop hybrid application which is both Ethereum node and client.
Aim: To install mist and run a Faucet account

Ethereum node needs to sync, please wait...

Looking for peers...

Figure 11: Ethereum Application

4.4What is need of alternative currencies?

An assortment of social and economical aspects of forces that raise the demand for alternative currencies [9]:
(a) Localism: By promoting group of people to commerce or "save high street," localism retains using up within a group of sovereign retailers or within a geographic area for job and enhanced business conditions for development.
(b) Technology: Such technology has become to a large extent for easier use with better software and near to the ground entry barriers causative to network effects.
(c) Political economy: There is cynicism about the high salary of CEOs and bankers, the notion of traditional banks being too gigantic to fail. With high liability and quantitative easing, there is great embarrassment with the economic ambiguity.
(d) Environmentalism: There are ecology concerns that ether we have reached to last extraction points such as petroleum resources and need to find new type of currency.
(e) Inefficiencies: Present financial governance failed due to overpriced and system is too expensive to bear.
(f) Financial freedom: Cryptocurrency have transferring advantage in digital currency along through weak internet connection. Such developed digital currency gives freedom to user to bypass capital controls and approaches to safe and secure harbor at a time of fiat economical crisis.
(g) Speculation: The wider acceptance of cryptocurrency by digital buyer appreciates it due to anticipating price. It has wide possibility in future as it easy to develop and without any cost till today [1]. However most of these original creations will come to an end of circulation within a relatively short time. Among many cryptocurrency in the race of establishment but only one can be accepted globally by the people.

V. RESULTS AND DISCUSSION

Many people see similarities between the expansion of the Internet and the development of cryptocurrency and postulate that cryptocurrencyisgoing to view similar rocketed growth as internet. However, from the business perspective, the growth of the Internet has more to do with e-commerce and less to do with finance. On the other hand, with cryptocurrency, for once in the history of mankind, technology is playing a leading role in finance. In future, one should expect a bank to be a digital or technologically savvy bank. The disruptive force has now arrived at the door step of finance and the blockchain technology is one of the solutions.
There are also similarities between hedge funds and cryptocurrency at the industry level. When the hedge fund industry was in its infant stage, it was perceived to be disruptive to the currency system because hedge fund managers were perceived as the bad guys who took big bets. They were seen to be the mavericks that attacked the currency system and caused the stock markets to collapse. Some banks did not want to pact with them as it did not make business sense with the high compliance costs. The most of emerging start-ups fail as consequence of same financial barrier in cryptocurrency.
In conclusion, Bitcoin is a novel invention, which is a breakthrough in terms of the payments and decentralized networks we know today. The various risk and benefits comes along with cognizant and conversant users wish need to deal within bitcoins. This thesis is a case study of Ethereum which is one of subset of cryptocurrency are likely similar to Bitcoins which aid to have educated us for clear window of understanding other different cryptocurrency. It is beginning of foundation of new era with smart technology connecting globe that is fullest potential without fear.

Acknowledgment

This work is outcome of the Research project- “A Case Study on Ethereum” at Vaishnavi Institute of Technology & Science affiliated to Rajiv Gandhi Technological University of MP, INDIA. The work is done under the Guidance of Mr. Sumit Sharma, Head of Department of Computer Science at Vaishnavi Institute of Technology & Science affiliated to Rajiv Gandhi Technical University respectively

REFERENCES

[1]Satoshi in Japanese means “wise” and someone has suggested that the name might be a portmanteau of four technology companies: SAmsung, TOSHIba, NAKAmichi, and MOTOrola. Others have noted that it could be a team from the National Security Agency (NSA) or an e-commerce firm (Wallace, 2011).

[2] Lam Pak Nian, David LEE KuoChuen- Introduction to Bitcoin-SimKee Boon Institute for Financial Economics, Singapore Management University, Singapore

[3] JaysingBhosaleand SushilMavale“Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin”Symbiosis Centre for Management Studies, Symbiosis International (Deemed University), Pune

[4] Arvind Narayan and Andrew Miller “Cryotocurrencies, Blockchain and Smart contracts” Expert-Curatedd Guides to the best CS research

[5] Sachchidanand Singh and Nirmala Singh “Blockchain: Future of Financial and Cyber Security” Tech Mahindra Pune, India - 411 057

[6] Jonathan Chiu and Thorsten Koeppl “The Economics of Cryptocurrencies- Bitcoin and Beyond” Bank of Canada Victoria University of Wellington and Queen's University

[7]Jesse Yli-Huumo, DeokyoonKo, Sujin Choi, Sooyong Park, Kari Smolander “Where Is Current Research on Blockchain Technology?-A Systematic Review” PLoS ONE 11(10): e0163477. doi:10.1371/journal.pone.0163477

[8] Rajshri Suresh, Rahul Batra, SeemaGhosh “Bitcoin – The Currency of the Future” IOSR Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668 PP 05-09

[9] A.Seetharaman, A.S.Saravanan, NitinPatwa&Jigar Mehta “Impact of Bitcoin as a World Currency” https://doi.org/10.5430/afr.v6n2p230