ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Integration of Cryptocurrency in Sovereign Economies

Ayush Kanth
Computer Science and Engineering
SRM University
Ramapuram, Chennai-600089
Email: akaran619@gmail.com

M.Madhusai
Computer Science and Engineering
SRM University
Ramapuram, Chennai-600089
Email: mmadhusai@gmail.com

Raghavendra Singh Dasila
Computer Science and Engineering
SRM University
Chennai, Tamil Nadu - 600089
email:raghavdasila@outlook.com

G.Kalpana
Computer Science and Engineering
Asst. Professor
SRM University Chennai
Email: g.gkalpana@gmail.com

Abstract—Introduction of cryptocurrency has revolutionised the way we perform transactions, providing a secure and anonymous method of payment .Out of the 710 cryptocurrencies existing today bitcoin has been the most dominant. Bitcoin works on the blockchain system.Till now we have seen cryptocurrency been used at a global level.In recent times , mos of the european economies have begun their testing phases with cryptocurrency and its allied tech. The driving force of the recent boom in cryptocurrency is the fact that most of the tech stack facilitating the transactions is open source meaning it is more than posible to edit and understand the essentialities.

Keywords—Cryptocurrency, Wallets, Block, Blockchains,Mining

I. INTRODUCTION

Cryptocurrency is the system of exchange of money which is transferred in a peer to peer manner and verified by solving mathematical problems.This system works on the principles of cryptography and encryption.The role of cryptography comes in ensuring the safety of transaction.The whole system is made possible through the blockchain technology.Cryptocurrency has revolutionized the online money transfer since its peer to peer system of transfer eliminates the role of a third party and is a better way for untrusted transfer. Over the past few years there have been introduction of many cryptocureencies. With Digitalizations booming in today's time, Some of the Cryptocurrencies such as bitcoin, XMR Monero , Litecoins to name a few and some others have been able to make an impact on the global level.In total there exists 710 cryptocur-rency mostly inspired by the bitcoin model. Implementing Cryptocurrency Globally has made things simple in terms of trading as going by the exchange rates of currency it iss easy to send a large amount of money in a single go.but there have been some problem as well.Like the heavy exchange rates of bitcoin have made it easy for drug peddler[3] to make money exchanges from any part of this world, same can be applied for terrorists.This can be brought into control if the usage of a cryptocurrency is limited within boundary of a nation. Integration of the cryptocurrency into national national economy will allow only allow the people who have the citizenship of a nation to use this form of money within the boundary of the nation. This will keep intact the advantages of the cryptocurrency by removing certain flaws from it. Free and Open Source Software (FOSS) has made it easier to get the codes of existing system and modify it as per the requirement of the neeeded System.Certainly Most of the cryptocurrencies which exist today are making use of the open sorce code provided by the open source currency like bitcoins.

II. RELATED WORK

A. e-CFA

Senegal a nation in Western Africa is bringing in its own cryptocurrency based on the blockchain model into System in 2017.The currency is proposed to be used in the parts of Africa like Cote dIvoire, Benin, Burkina Faso, Mali, Niger, Togo and Lusophone Guinea Bissau.it is designed to operate alongside the CFA.The eCFA will be issued by the regional bank.eCFAs development stems from a partnership between regional bank Banque Rgionale de Marchs (BRM) and eCurrency Mint Limited.The eCFA is a high-security digital instrument that can be held in all mobile money and e-money wallets. It will secure universal liquidity, enable interoperability, and provide transparency to the entire digital ecosystem in WAEMU

B. Cryptocentavo

Cryptocentavo is another national-cryptocurrency integration.This is proposed by a South-American nation Ecuador.This proposition was made after banning the use on bitcoin in that nation.The nation plans to start a Cryptocurrency on the centralized model which removes the double spend-ing model.In bitcoin this was solved using the timestamped blockchain.Banning bitcoin has also been an issue since they cannot use opensource bitcoin software.

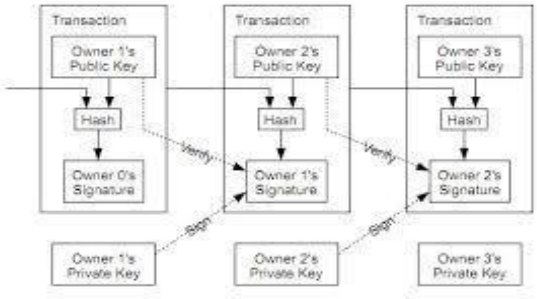
III. EXISTING SYSTEM

A. BlockChain

The blockchain provides a mathematically verifiable way of making a transaction.Blockchain also provides solution to byzantine general's problem. The merkle tree is a kind of bottom up tree where a pair of blocks are hashed together to form a node of merkle tree following the other nodes forming pairs and hashed together in order to have a final root node.Each node consists of a block header.The block header consists of three address of the previous block.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017



B. Wallets

Wallets are used to permit the use of sending or receiving the cryptocurrency.The transaction to be made requires two types of keys, The private Key and the public Key the private key comes into play when money is to be sent by a user. When money is sent private key is used for approving transaction from the wallet.The public key of a user is open and miners use it for the verification of the user.

C. Mining

Mining is an activity done to increase the number of blocks in the block chains. It also includes new blocks in the block chain.Mining results in rewards for the miners. Mining can be performed in two ways either as solo or in pool.

Solo Mining- In this mining an individual himself tries to generate new blocks and earn reward for himself.

Pooled Mining- In pooled Mining the reward is shared by a pool of miners and is more efficient way of mining.

IV. PROPOSED SYSTEM

A. Centralized System

The integration of Cryptocurrency with national econ-omy will automatically bring in the cryptocurrency under the scanner of the government.Government can play a role in monitoring the transactions taking place. aBut to keep it independent, government should not interfere with the pro-cessing of the cryptocurrrency.This way the goverment track and record the flow of currency among buyers and sellers.This can be made possible by not giving any body power to control the transactions.

B. Unique Id

A valid citizenship proof of the nation is required.The Wal-let software will only be issued to a person based on his Unique Id which will be generated from his citizenship proof F or a valid citizenship proof identity proofs like passports or for example, India's Aadharcard card can be used. This will enable the issuing of wallet to a citizen.Nations Indonesia can use Indonesean identity card.The National Identity document which is held by mass Population of the country can be used.

V. ECONOMIC MODEL

A. Integration with Economy

The proposed is independent of existing administrative institutions,however the income tax department and the central government is allowed access to monitor and query all trans-actions. This action will enable the government to prevent cor-ruption and fraud thereby preventing setbacks to the economy caused. A developing country, India suffered an economic loss of 36,400 crore INR (55.6 million USD) due to corruption[1].

B. Exchange Rates

The initial exchange rare should be set keeping in mind the nation's Internet using population.If only a limited amount of people are using Internet. The number of people using Internet determines the number of miner strength as well as number people capable of adopting this system. This can be seen as more number of people using internet there is a great potential for number of miners at the same potential people to use the system are more.The problem is miners need reward which will be in the form of cryptocurrency. The rate of cryptocurrency for a sovereign economy has to be determined keeping in mind that miners are benefited in order to take up the work.

C. Exchanges

Currency exchanges allow users to trade cryptocurrency for traditional currencies or other virtual currencies. Most operate double auctions with bids and asks much like traditional financial markets, and charge a commission ranging from 0.2 to2 percent. Some exchanges offer more advanced trading tools, such as limit or stop orders. To date, derivatives markets and short-selling remain rare. [7] discussed about a system, In this proposal, a neural network approach is proposed for energy conservation routing in a wireless sensor network. Our designed neural network system has been successfully applied to our scheme of energy conservation. Neural network is applied to predict Most Significant Node and selecting the Group Head amongst the association of sensor nodes in the network. After having a precise prediction about Most Significant Node, we would like to expand our approach in future to different WSN power management techniques and observe the results. In this proposal, we used arbitrary data for our experiment purpose; it is also expected to generate a real time data for the experiment in future and also by using adhoc networks the energy level of the node can be maximized.

VI. ARCHITECTURE

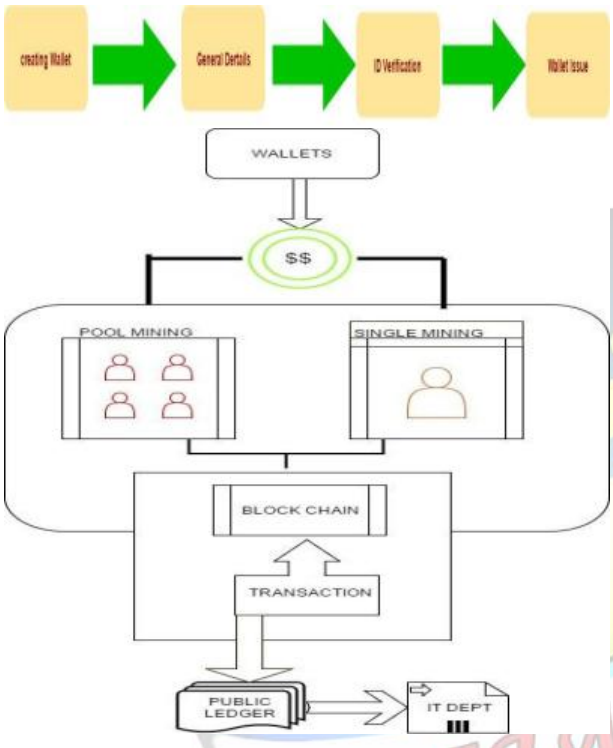
A. Change in Wallet Specification

Wallets will be an application which will have to be iden-tified by the known nation tax identity.For instance pancard in India.This will serve the purpose of giving the government track of user identity.Also the usage of tax identification for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

the verification brings the user dirctly under scanner of the tax department of that nation.Hence for the issues of wallet a form consisting of general wallet will have to be filled in followed by the verification using the income tax identity details.Following which wallet will be issued.



VII. ARCHITECTURE WORKFLOW

A. Wallet

The wallet will be an desktop or mobile based application which is tax identity verified.It will be used for making or receiving payments.The payment can be made using a special private key 256 bit of and public key of 65 bytes.The private key acts as digital signature for a payment for checking the authenticity of of the payment the there is a public key the public key is used to verify the payment is coming from an authorized user.

B. Mining

Mining requires different types of processors depending upon the complexity of the problem.The speed of processor required directly depends upon complexity of the algorithm used.Some of the cryptocurrencies existing today use the SHA-256 algorithm for encryption.While the others use Scrypt.The SHA-256 based System requires System producing very high hash rates, in the range of giga hash per second.Other Algo-rithm used is Scrypt, this algorithm needs a hardware which requires a hash rate in the range of kilo hash per seconds. Scrypt algorithm based system donot need a special proceesor or harware it can be done using a general computer system.The use of HSA 256 hardware requires special hardware to produce high hash rates. It can be done in a pool system or in as a solo.

C. Blockchain

Blockchain is the entity which ensures the Successful transaction.It will work on the same principles on the lines of merkle tree. each node of a merkle tree will consist of a combination of two block hashes. The final node will be the root node.The transaction once entered in a blockchain is a confirmed transaction and will contain all the transaction which has taken place in the system.The workflow of blockchain works in the following way first digital transaction is initialised then transaction is sent to miner for verification followed by broadcast of transaction to all the connected nodes.Network accepts the transaction if the data is valid receiver will get the transaction.

D. Transaction

Transaction will be timestamped i.e. whenever the transaction takes place the date and time will be mentioned in the block in order to solve the problem of double spending.Transaction once takes place that it is confirmed in the blockchain. A notification message will be sent to the sender and the receiver confirming the transaction.Also the details will go to a special ledger created known as the public ledger which will be directly under the Income tax department of the nation.

E. public ledger

The public ledger here is the central database which consists the detailed description of the all the transactions made. The original cryptocurrency system doesnot have the idea of a central database. In other currencies the blockchain itself acts as a public ledger.The public ledger will be open to the Income tax deparment of the country.

F. IT Deparment

IT department will play the role of bringing the whole system under the government.It is the link between the center and the system. The existing system currently works as decentralized. This system is proposed to be decentralized under the monitorship of center.Unlike the banks where a transaction is completely dependent on the banking system the system will work independently.This linking of the system with the Income tax department ensure that there is account for all the transfer taking place.

REFERENCES

[1] http://timesofindia.indiatimes.com/business/india-business/India-suffered-Rs-36400-cr-loss-due-to-corruption-Report/articleshow/21252592.cms

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

[2] http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213

[3] https://silkroaddrugs.org

[4] https://bitcoin.org/en/developer-guide

[5] Quoc Khanh Nguyen,"Blockchain A Financial Technology For Future Sustainable Development",2016 3rd International Conference on Green Technology and Sustainable Development(references).

[6] Rainer Bhme, Nicolas Christin,Benjamin Edelman, and Tyler Moore,"Bitcoin: Economics, Technology, and Governance",Journal of Economic Perspectives

[7] Christo Ananth, A.Nasrin Banu, M.Manju, S.Nilofer, S.Mageshwari, A.Peratchi Selvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015,pp:16-19

[8] http://enetium.com/resources/Bitcoin.pdf

[9] https://www.weusecoins.com/

[10] https://www.happycoins.com/en/info/links