IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct. 2018 E-ISSN: 2347-2693

CRITICAL ANALYSIS ON CRYPTOCURRENCY

R. Sujeetha A.P.[1*], Sarthak Haldar[2], Bijoy Krishna Saha[3], Pranjal Katyayan[4]

[1,2,3,4] Dept. of Computer Science, SRM Institute of Science and Technology, Chennai, India

[*]*Corresponding Author: sujeethasrm@gmail.com, Tel.: +91-94861-96279*

Available online at: www.ijcseonline.org

Accepted: 8/Oct/2018, Published: 31/Oct/2018

Abstract— A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. The anonymous nature of cryptocurrency transactions makes them well-suited for a host of nefarious activities, such as money laundering and tax evasion.

The first cryptocurrency to capture the public imagination was Bitcoin, which was launched in 2009 by an individual or group known under the pseudonym Satoshi Nakamoto. As of September 2015, there were over 14.6 million bitcoins in circulation with a total market value of $3.4 billion. Bitcoin's success has spawned a number of competing cryptocurrencies, such as Litecoin Namecoin and PPCoin.

Keywords—cryptocurrency,bitcoin,litecoin

I. INTRODUCTION

Digital forms of money have gotten extensive consideration as of late by purchasers and shippers as a practical type of cash for the installment of merchandise and enterprises on the web. For quite a while, a scope of Internet based installment frameworks have given elective intends to executing buys. Anyway those frameworks have generally been founded on customary types of installment instruments, for example, credit cards, bank account transfers, and third party accounts. These types of money related exchanges are basically fixing back to national bank issued physical monetary standards. On the other hand, the present cryptographic money notes and coins are not issued by banks. Or maybe, they are made by peer administrators in a system of electronic cash mining activities. The outcome is the formation of virtual electronic money, and its trustworthiness is supported by an arrangement of cryptographic natives making it unmanageable to fashion and in the meantime the digital money endeavors to save the properties of genuine money as a transferrable electronic type of cash that can't be followed (i.e. mysterious). The emanant frameworks picking up selection depend on distributed electronically produced coins. Subsequently, it might be foreseen that a halfway bank issued electronic cash (Fiat digital currency) influence take to attach sooner or later to contend or maybe control in some mold the circulation and utilization of cryptographic money.

As such, we outline in this paper an IT solution framework to support a central bank issued electronic currency by complementing the existing peer-to-peer systems, which have gained favor with merchants and customers.

In this paper, we provide some background to the genesis of electronic currencies and how these have transformed to the more recent peer-to-peer based cryptocurrencies in circulation today. We discuss some of the motivations for adopting both the peer-to-peer and a central bank issue Fiat Cryptocurrency. Based upon the needs for supporting the issuance of both forms of cryptocurrency we propose a reference architecture for supporting two forms of electronic currency. The frameworks may be used as a building block for central and retail banks that may elect to support cryptocurrencies as the need arises.

In the next section, the related work to electronic forms of cash is reviewed and discussed. Following in next Section , we discuss the various forms of cash and currency systems that have evolved over time. Next, we identify the key properties that need to be supported in a payment system based upon electronic cash. This is then followed in later Section with the proposed IT solution framework for supporting a Fiat cryptocurrency issued by a central bank. We then demonstrate how this framework can be used in practice as we examine the interactions of each IT component in more detail. We conclude our paper in next Section with a discussion of the observations in this paper and discuss the potential areas of further work.

II. THE BITCOIN PROTOCOL

A cryptocurrency is a computerized resource intended to function as a medium of trade that utilizations solid cryptography to anchor budgetary exchanges, control the production of extra units, and confirm the exchange of advantages. Virtual money is a subset of Cryptocurrency. Cryptographic forms of money utilize decentralized control instead of incorporated advanced digital cash and central banking frameworks. The decentralized control of every cryptographic money works through a technology called distributed ledger, usually a blockchain, that fills in as an open monetary exchange database.

Bitcoin, first discharged as open-source software in 2009, is for the most part thought about the first primary decentralized digital money. Since the arrival of Bitcoin, more than 4,000 altcoins (elective variations of Bitcoin, or different digital currencies) have been made.

Amid the 1990s two electronic money conspires that experienced noteworthy preliminaries were Mondex and Digicash. Mondex was brought about by Tim Jones and Graham Higgins in 1991 and included the utilization of an electronic wallet conveyed to a smartcard tolerating electronic money . Notwithstanding early selection and support by the managing an account and retail businesses amid the preliminary, the plan did not continue. Digicash was presented by David Chaum and upheld computerized money that was mysterious, transferrable, and separable. In addition, the early work by David Chaum on the utilization of a visually impaired computerized signature procedure to sign an exchange is recognized to be the primary work identifying with a genuine shape electronic of money and henceforth a cryptocurrency.

Resulting to the spearheading work of David Chaum on electronic money, which depended on various associations with the bank (called cut-and-choose), some of extra electronic money frameworks were distributed that expanded or proposed elective conventions . In Okamoto and Ohta recommended the principal conspire with the capacity to pull back one electronic money sum (in view of cut-and-choose) that could be later sub-partitioned and afterward utilized in a few resulting littler installment exchanges. Afterward, Brands sketched out a more effective plan with a money withdrawal convention that just required one association trade with the bank, while freely Ferguson additionally proposed an elective plan to accomplish a comparative single collaboration exchange to pull back money; the two methodologies swearing off the requirement for various connections of the cut-and-choose technique. Elective money conventions have likewise been proposed utilizing particular cryptographic strategies. For example, Traore plots a money conspire that applies the utilization of gathering digital signatures . There is likewise chip away at the utilization of bunch cryptography to make the measured exponentiation activities for advanced marking and confirmation more proficient using increase and hash tree techniques that join various coin groups amid the mark and check periods of money withdrawal and installment . Despite the fact that there is noteworthy work on the security conventions and cryptographic instruments in electronic money, there is less work on the functional use of the ICT systems supporting these rising money plans, and henceforth, we treat this subject in this paper.

III. CURRENCY AND CASH SYSTEMS

Prior to the presence of any type of broadly acknowledged installment component, early trades of products and ventures were done straightforwardly as a dealing framework. The trades can likewise be considered as an early type of a distributed framework that did not require the nearness of a focal expert to back the exchanges. It was not until considerably later that a money in view of coins ended up accessible, and these were at first in light of some valuable metal. This advanced further when the valuable metal was substituted for a stamped type of paper cash. Anyway the cash issued by the overseeing expert was initially supported by some type of benefit or commodity, most normally gold (standard), and were alluded to as ware cash. All the more as of late, the highest quality level was surrendered in 1971 and thus the support for money originated from the national bank supported by the administering expert for the land. This type of cash is alluded to as Fiat cash, with no unmistakable resource supporting the money other than the guarantee of reclamation by the overseeing expert. The expulsion of a ware backing has implied that the roof for the production of cash was expelled. This has enabled cash to be produced as regarded fundamental by the administering body, and its creation is directed to adjust the state of mind of the economy in lieu of the predominant financial conditions affecting neighborhood and worldwide markets (i.e. inflationary, retreats, blast).

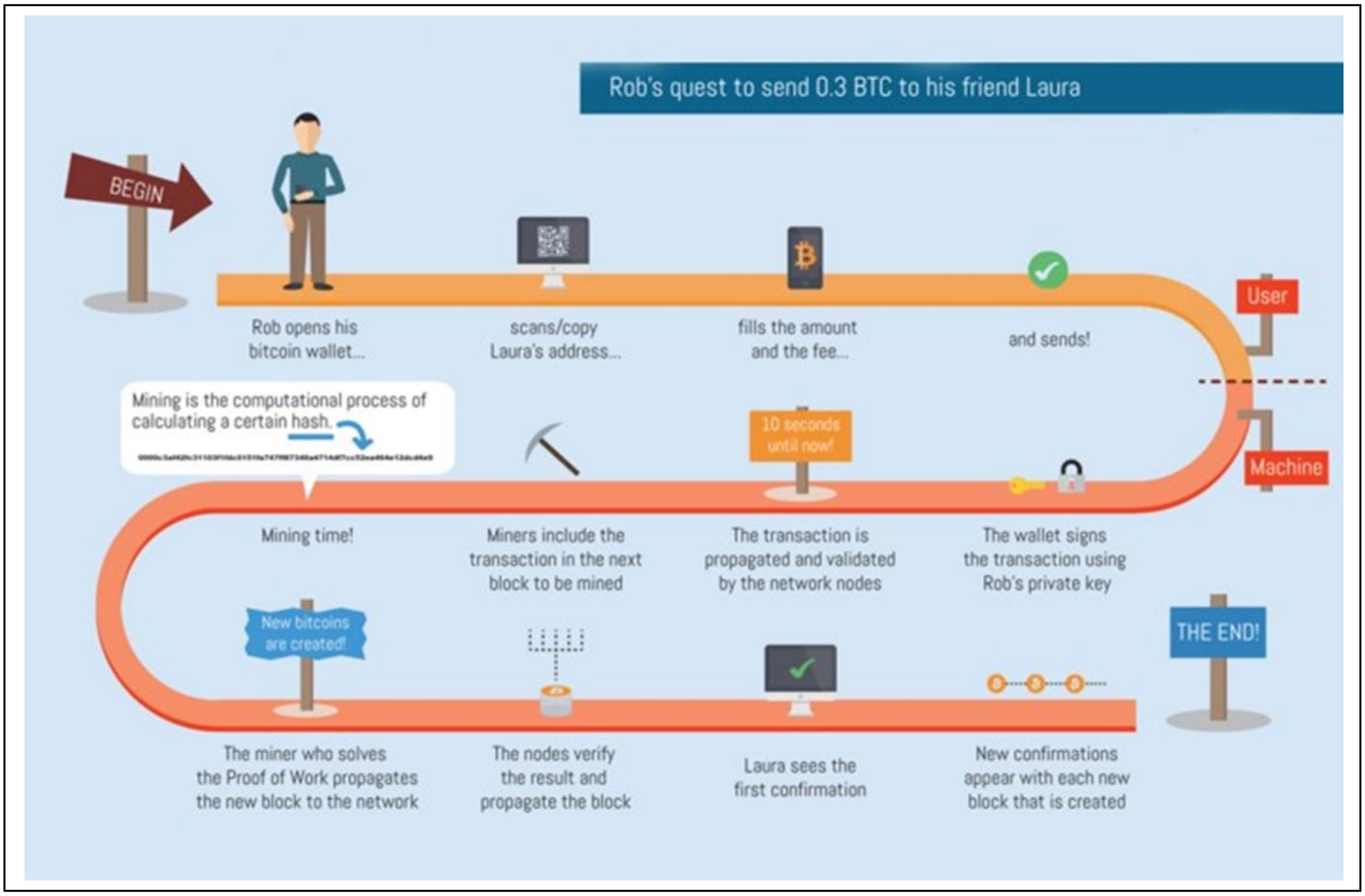
Rob's quest to send 0.3 BTC to his friend Laura
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
Mining time!
Miners include the transaction in the next block to be mined
10 seconds until now!
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created

FIG. 1

IV. PROPERTIES OF CRYPTOCURRENCY

Electronic money (both shared and Fiat based) in its basic frame expects to reproduce similar properties and highlights displayed by physical money. Be that as it may, because of the idea of its virtual presence, a few extra attributes must be watched. We quickly clarify a few of these highlights, which incorporate counteractive action and location of twofold spending, convention proficiency, and disconnected transferability.

Numerous electronic money/digital currency conventions have a general helplessness where the same electronic coin might be spent more than once. Since it is anything but difficult to duplicate the paired arrangement that speaks to the cryptographic money, there must be an instrument set up to both distinguish the replay of an utilized electronic coin and keep this from happening. In that capacity, all obvious electronic money frameworks have some type of cryptographic convention that gives an ability to recognize and counteract twofold spending. The effectiveness of the convention is an essential element to see the same number of cryptographic tasks are computationally costly, and when handled by a trader, may overpower the portal server preparing capacity. Consequently the capacity to have a productive convention is an extremely alluring component. At long last, physical trade can be exchanged out a disconnected way between parties, with no middle of the road party included. Consequently digital money is planned likewise to reproduce this component. Given the pervasiveness of being dependably on-line for clients, this trademark is maybe not as noteworthy currently contrasted with when electronic money was conceived amid the 90s.

V. FIAT CRYPTOCURRENCY ARCHITECTURE

A. Mining:

The digital money stamping, mining, and trade frameworks are the key segments that give guide support to the virtual business. At this system layer, there exist two digital money vaults: one to store distributed coins and a second to store focal expert created electronic coins. These vaults are designed to be very accessible and blame tolerant, with visit reinforcement capacity; since any loss of information in these vaults implies an immediate loss of crude cash. In spite of the fact that the mining activities empower the bank to take an interest in creating new distributed electronic cash, maybe the key inspiration is investment in the common general record as a confided in substance for hazard and consistence administration. The stamping production line is, obviously, the segment that enables the bank to fabricate new Fiat electronic money.

Despite the fact that the national bank may make cryptographic money, customary saving money allows the bank to make extra digital currency in view of partial save managing an account. To take part in currency advertises that range both the conventional money frameworks and electronic money, the digital money trade intermediary is required.

B. Payment:

The digital money stamping, mining, and trade frameworks are the key segments that give guide support to the virtual business. At this system layer, there exist two digital money vaults: one to store distributed coins and a second to store focal expert created electronic coins. These vaults are designed to be very accessible and blame tolerant, with visit reinforcement capacity; since any loss of information in these vaults implies an immediate loss of crude cash. In spite of the fact that the mining activities empower the bank to take an interest in creating new distributed electronic cash, maybe the key inspiration is investment in the common general record as a confided in substance for hazard and consistence administration. The stamping production line is, obviously, the segment that enables the bank to fabricate new Fiat electronic money. Despite the fact that the national bank may make cryptographic money, customary saving money allows the bank to make extra digital currency in view of partial save managing an account. To take part in currency advertises that range both the conventional money frameworks and electronic money, the digital money trade intermediary is required.

VI. SYSTEM INTERACTION

Amid the installment exchange, the client has cryptographic money (consistently) coins put away inside their eWallet on a cell phone and uses this to pay for products at a shipper shop. It is expected that the shipper terminal is appropriately furnished with an eWallet to get the exchanged assets and has experienced an enlistment and enlistment process with the bank to build up itself as a partaking digital currency vendor. Note additionally that the trader would require numerous enrollments, and will have various eWallets, one for each unique sort of digital money bolstered. The graph at Figure 2 outlines the groupings of communications when the client conducts installment with a dealer. The vendor begins by entering the buy sum into the business terminal . The terminal at that point produces a QR Code and shows this for examining by the clients' installment gadget . The client may (for instance) utilize the camera to check the QR code and convert this into the installment sum while starting the exchange of assets from the eWallet to the trader .

The client gadget accordingly transmits the installment to the shipper terminal (this might be accomplished by close field remote). The trader terminal gets the installment exchange and advances this onto the bank for confirmation to check for twofold spending . Now, for little sum the shipper may choose to acknowledge the hazard and not sit tight for the aftereffect of the misrepresentation check by the bank and endorse the exchange quickly. An endorsement is shown on the vendor terminal and the coins focused on the eWallet. On the other hand, for bigger sums the trader may choose to sit tight for the misrepresentation check to be finished before showing the endorsement result and afterward submit the coins to the vendor eWallet.

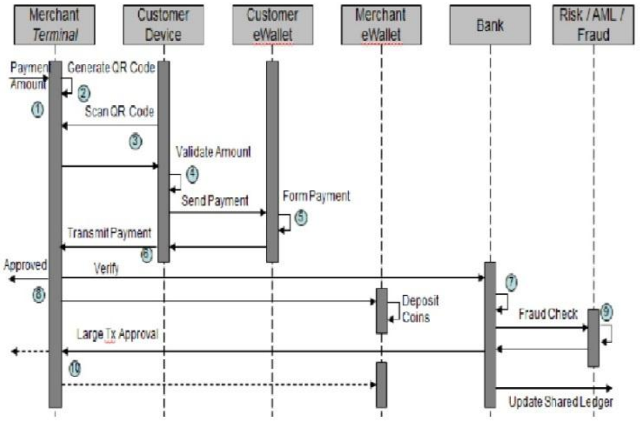

FIG.2

VII. SUMMARY

In this paper, the thought of a Fiat based cryptographic money as an integral answer for the ongoing development of associate based digital money is inspected. The properties of physical money that are probably going to be the safeguarded attributes of any digital currency are likewise examined. A Fiat based national bank issued digital money may well be positively gotten by dealers and clients as the ongoing patterns in associate based cryptographic money frameworks shows that the more extensive network is maybe prepared to embrace these more up to date electronic style money advances. In light of this, a reference design for keeping money is introduced that shows the key specialized parts and security controls required to help both a Fiat and shared based digital money condition. Since these advancements are still generally new, there is impressive further work in seeing how business exchanging frameworks and currency markets will develop and be affected by these new monetary advances.

REFERENCES

[1]. Sonali singh , Arfiha Khatoon , Sarvesh Kumar , Harshita Chawala "An Analysis of cryptocurrency",IEEE Confrence,2018

[2]. Prasanta Kumar Dey "Cryptocurrency":-few words on digital money", IJTSRD, May-June 2018.

[3]. Mahendra Kumar Shrivas, Thomas Yeboah, "A Crictal Review of Cryptocurrency Systems", Texila International Journal of Academic Research

[4]. Volume 4, Issue 2, Dec 2017.

[5]. Lewis Tseng, "Bitcoin's Consistency Property", 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing.

[6]. Florian Tschorsch and Bj¨orn Scheuermann , "Bitcoin and Beyond: A Technical Survey onDecentralized Digital Currencies", IEEE COMMUNICATION SURVEYS & TUTORIALS,2015.

[7]. Christopher J. Pavlovski, "Reference Architecture for Cryptocurrency in Banking", IT in Industry, vol. 3, no. 3, 2015.

Authors Profile

Ms.R.Sujeetha pursed Masters in Engineering from PSG College of Technology, Anna University, Coimbatore. She is currently working as Assistant Professor in Department of Computational Sciences, SRM Institute of Science and Technology, Chennai. She has published many research papers in reputed international journals. Her main research work focuses on Software Engineering and Object Oriented Analysis and Design. She has many years of teaching experience and Research Experience.

Mr Sarthak Haldar is currently pursuing Bachelor of Technology from SRM Institute of Science and Technology, India. He is currently working on AI with Phython with help of Machine Learning and Deep Learning. He has published one research paper in a reputed international journal. His main research work focuses on Cryptography Algorithms, Blockchain , AI , Machine Learning and IoT. He has 3 years of Programming experience.

Mr. Bijoy Krishna Saha is currently pursuing Bachelor of Science from SRM Institute of Science and Technology, Chennai,India. He is currently working on web development and android applications and published paper on a reputed journal . His main research focusses on machine learning, Internet Of Things, Android, Artificial Intelligence and cryptocurrency.

Mr Pranjal Katyayan is persuing Bachlor of Technology from SRM Institute, Ramapuram campus (Chennai) in computer science stream . His main intrest lies in maching learning, artificial intelligence and iot. He has published one research paper in a reputed international journal. He has 3 years on programming expercience on C and C++.