Analysis of Cryptocurrency

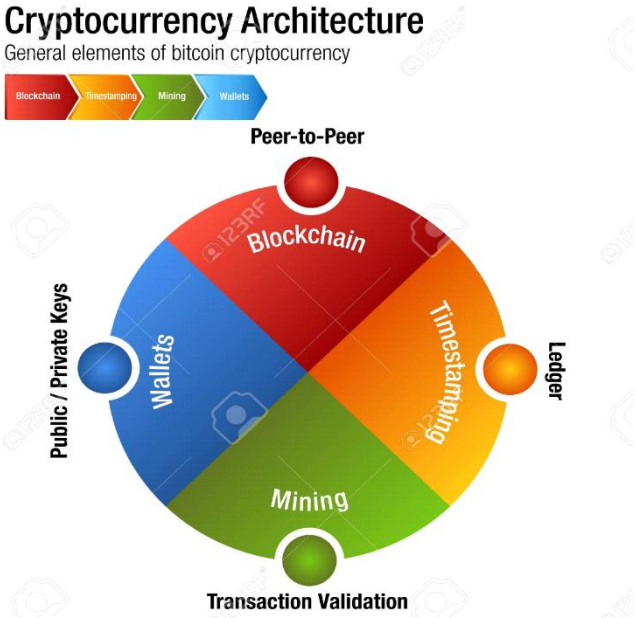
Monica Uttamchandani[1] Prakash Kene[2]
[1]PG Student [2]Assistant Professor
[1,2]Department of MCA
[1,2]P.E.S.'s Modern College of Engineering, Pune, Maharashtra, India

Abstract— This paper identifiedthe understanding of cryptocurrencies including bitcoin and the blockchain. This paper provides a primer on the basics of Bitcoin and discusses the existent narratives about the technology's potential to facilitate remittances, financial inclusion, cooperative structures and even micro-insurance systems. Due to the fast developments in bitcoins it needed to understand the factors that influence its value formation. At present the value of bitcoin is $7 million of notional value and more than $ 60 million value changes every day. The current active wallets of cryptocurrency are estimated around 6-11 million. The currency exists in 2009 and was accepted as a legal instrument for making payment by various countries. In june 2011 WikiLeaks accept bitcoins for donations. Later it became popular after master card, visa, PayPal.

Key words: Cryptocurrency, Bitcoin, Bitpay, Exchange Rates, OraSaifu

I. INTRODUCTION

Cryptocurrency is a digital asset designed to work as a medium of exchangethat uses cryptography to send its transactions . In the currenDigital era, cryptocurrency is moving fast led by Bitcoin which was created in 2009 was the first decentralised crypto currency.Bitcoin is follwed by Ether, Litcoinetc are all taking the financial storm and influencing the public to invest and buy these currencies.Government of various countries are much concerned about crypto currencysuch as Bitcoin. The significancant feature of these currencies are payments can be made without the involment of banks.customers can transfer the huge sum of money through the digital wallets.Central bank of various countries like Bank of England and Bank of isreal are trying to launch their own digital currencies.this will helpnpeople using the official system which has the benefit of both tradiional and crypto currencies.The traditional system for electronic payments and transfers and security checks on each transaction by banks consumes much time and cost. Whereas the crypto currencies help to process these transactions much faster and the transactions would be recorded instantly and need not be cleared by Banksinstead technology known as Block chain is used.



II. TECHNOLOGY USED FOR CRYPTOCURRENCY

A. *Blockchain?*

1. Defining blockchain: a technology with many faces Blockchain is a particular type or subset of so-called distributed ledger technology ("DLT"). DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes. Blockchain is a mechanism that employs an encryption method known as cryptography and uses (a set of) specific mathematical algorithms to create and verify a continuously growing data structure – to which data can only be added and from which existing data cannot be removed – that takes the form of a chain of "transaction blocks"11, which functions as a distributed ledger. In practice, blockchain is a technology with many "faces". It can exhibit different features and covers a wide array of systems that range from being fully open and permissionless, to permissioned[13]:

On an open, permissionless blockchain, a person can join or leave the network at will, without having to be (pre-) approved by any (central) entity. All that is needed to join the network and add transactions to the ledger is a computer on which the relevant software has been installed.

There is no central owner of the network and software, and identical copies of the ledger are distributed to all the nodes in the network. The vast majority of cryptocurrencies currently in circulation is based on permissionless blockchains (e.g. Bitcoin, Bitcoin Cash, Litecoin,).

On a permissioned blockchain, transaction validators (i.e. nodes) have to be pre-selected by a network administrator (who sets the rules for the ledger) to be able to join the network.This allows, amongst others, to easily verify the identity of the network participants. However, at the same time it also requires network participants to put trust in a central coordinating entity to select reliable network nodes. In general, permissioned blockchains can be further divided into two subcategories. On the one hand, there are open or public permissioned blockchains, which can be accessed and viewed by anyone, but where only authorised network participants can generate transactions and/or update the state of the ledger. On the other hand, there are closed or "enterprise" permissioned blockchains, where access is restricted and where only the network administrator can generate transactions and update the state of the ledger.What is important to note is that just like on an open permissionless blockchain, transactions on an open permissioned blockchain can be validated and executed without the intermediation of a trusted third-party. Some cryptocurrencies, like Ripple and NEO utilise public permissioned blockchains.

III. How Blockchain Works:

a. The blockchain is a distributed database In simple terms, the blockchain can be thought of as a distributed database. Additions to this database are initiated by one of the members (i.e. the network nodes), who creates a new "block" of data, which can contain all sorts of information. This new block is then broadcasted to every party in the network in an encrypted form (utilising cryptography) so that the transaction details are not made public.Those in the network (i.e. the other network nodes) collectively determine the block's validity in accordance with a pre-defined algorithmic validation method, commonly referred to as a "consensus mechanism". Once validated, the new "block" is added to the blockchain, which essentially results in an update of the transaction ledger that is distributed across the network. In principle, this mechanism can be used for any kind of value transaction and can be applied to any asset that can be represented in a digital form. We illustrate this in Figure 1 below.

Transaction "blocks" are signed with a digital signature using a private key Every user on a blockchain network has a set of two keys. A private key, which is used to create a digital signature for a transaction, and a public key, which is known to everyone on the network. A public key has two uses:

1)it serves as an address on the blockchain network; and

2) it is used to verify a digital signature / validate the identity of the sender. On the Bitcoin blockchain, this translates into the following example. Suppose that Anna wants to send 100 Bitcoins to Jeff, then first of all she will have to digitally sign this transaction using her private key (which is only known to her). She will have to address the transaction to Jeff's public key, which is Jeff's address on the Bitcoin network. Next, the transaction, which will be collated into a "transaction block", will have to be verified by the nodes within the Bitcoin network. Here, Anna's public key will be used to verify her signature. If Anna's signature is valid, the network will process the transaction, add the block to the chain and transfer 100 Bitcoins from Anna to Jeff. A user's public and private keys are kept in a digital wallet or e-wallet. Such wallet can be stored or saved online (online storage is often referred to as "hot storage") and/or offline (offline storage is commonly referred to as "cold storage").

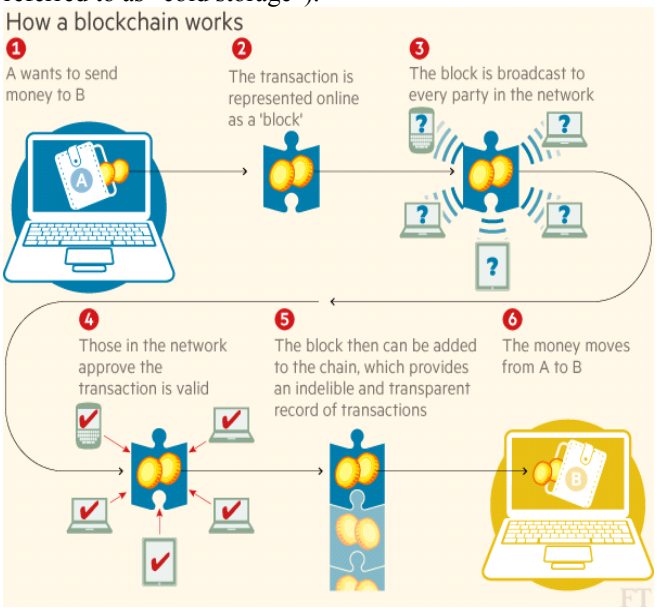


Fig.1:

Bye-bye middleman? One of the key advantages of blockchain technology is that it allows to simplify the execution of a wide array of transactions that would normally require the intermediation of a third party (e.g. a custodian, a bank, a securities settlement system, broker-dealers, a trade repository, …). In essence, blockchain is all about decentralizing trust and enabling decentralized authentication of transactions.Simply put, it allows to cut out the "middleman". In many cases this will likely lead to efficiency gains. However, it is important to underscore that it may also expose interacting parties to certain risks that were previously managed by these intermediaries. For instance, the Bank for International Settlements ("BIS") recently warned in a report of 2017 titled Distributed ledger technology in payment, clearing and settlement, that the adoption of blockchain technology could introduce new liquidity risks. More in general it seems that when an intermediary functions as a buffer against important risks, such as systemic risk, he cannot simply be replaced by blockchain technology.[1]

IV. Great Examples of Cyptocurrency

A. Bitcoin

Bitcoin, the world"s most common and well known cryptocurrency, has been increasing in popularity. It has the same basic structure as it did when created in 2008, but repeat instances of the world market changing has created a new demand for cryptocurrencies much greater than its initial showing. By using a cryptocurrency, users are able to exchange value digitally without third party oversight. Cryptocurrency works on the theory of solving encryption algorithms to create unique hashes that are finite in number. Combined with a network of computers verifying transactions, users are able to exchange hashes as if exchanging physical currency. There is a finite number of

bitcoin that will ever be generated, preventing an overabundance and ensuring its rarity. Water, despite its requirement as a life giving material, is generally accepted as being free or of little cost because it is so abundant. If water was rare, it would be more valuable than diamonds. Value exists for bitcoin because its users have trust that if they accept it as payment, they would could use it elsewhere to purchase something they want or need (Kelly, 2014). As long as the users maintain this faith, the valued object can be anything. Bitcoin‟s value exists in its ecosystem much in the same way that wampum, a seashell, was the currency of the land for Native Americans (Kelly, 2014). Bitcoin does not have intrinsic value like gold in that it cannot be used to make physical objects like jewelry that have value. Nevertheless, value continues to exist due to trust and acceptance.

Current legal and financial structures are not designed with a technology like this in mind. Financial institutions are built off of much older forms of currency. In some ways, it is comparative to the computing industry. The baseline of computing still relies on transmitting and processing 1‟s and 0‟s, providing only two dimensions of input. Yet all of our current technology uses this technologically archaic system due to adoption, cultivation, and lack of need for newer systems. If cryptocurrencies became the global norm for transactions, long standing systems for trade would need to be completely reformed to deal with this type of competition. For this reason, cryptocurrencies could possibly be the single most disruptive technology to global financial and economic systems.

BitPay, the largest bitcoin processor in the world, has recently seen transaction rate grow 110% in the past 12 months (Team, 2016).

Transaction increase is an indicator of user acceptance growing. The conditions for Bitcoin‟s widespread adoption could be described as a “fire triangle”. Where fire needs fuel, oxygen, and heat to exist; Bitcoin needs user acceptance, vendor acceptance, and innovation to ignite. Without all three aspects, bitcoin may not truly become a legitimized mainstream currency. Bitcoin is currently experiencing an increase in user acceptance and use, which is driving the other two aspects of the “fire triangle”.

Cryptocurrency‟s adoption will be an important subject to watch in the future, as it could be a truly transformative technology that alters the way money is exchanged worldwide. Bitcoin‟s increased adoption has been integrally tied to global market shifts. The current Internetfueled global market is very much entangled. If one regional market begins to plummet, it can easily drag the others with it. Bitcoin, like the Euro, can freely move across many national borders, creating an environment that promotes global trade, mutual prosperity, and even peace.

V. A PRIMER ON CRYPTOCURRENCY

To understand the Bitcoin system, it is useful to sketch out the similarities and differences with the normal bank-run electronic payments system. In the normal system:

1) A person has an account number at a bank.
2) They have a way of proving that they control that account number—for example, a PIN code.
3) The bank, in turn, has a data record of how much money is attributable to that account number, thereby keeping score of the person’s money on a private internal database or ledger.
4) The person can then use an electronic communications system to identify themselves to their bank as the authentic account holder, and can request for the money associated with their account number be transferred to someone else’s account at a different bank.
5) This then spurs the bank to edit their ledger of accounts—changing the person’s score—and to tell the recipient’s bank to do the same. The process is a little more complex than this, but in effect the money moves via a series of private databases being edited. The normal bank payments system thus works by a limited set of private intermediaries editing private databases that they control, and then informing the account holders that the transactions have occurred (e.g. “Your new balance, recorded in our datacentres, is £1,240”). The Bitcoin system—like the normal bank payments system—is intended to move monetary tokens between people through the changing of account entries on databases, but it has two immediate differences. First, the database that is used to record payments between people is public, rather than the privately held account databases of the normal banking system. Second, the intermediaries that change that database are a decentralized network of people (“miners”) running special Bitcoin software, rather than banks running their own private software systems.1Thus, the Bitcoin system, at its most simple, consists of a widely distributed, and highly visible, public ledger (or database)—colloquially referred to as the blockchain—that people can use to record transactions of digital tokens between themselves. Thedatabase thus keeps score of their tokens on the system in a highly public and transparent2 way.

VI. IN THE BITCOIN SYSTEM:

1) A person wishing to make a payment has a public address (akin to an account number).
2) They have a way of controlling that public address through the use of a private key (roughly akin to a PIN number)
3) They then use an electronic communications system (the internet) to identify themselves to the Bitcoin network, and request that digital tokens—associated with their public address—be moved to someone else’s public address.
4) This then occurs by a change made to the blockchain ledger by a set of participants colloquially known as miners.3 It is beyond the scope of this paper to describe the exact means by which this happens, but the process involves the miners using their computing power to validate the transactions.
5) The two parties who control the public addresses can then see these changes, proving that the tokens have moved from one address to the other.

VII. THE NATURE, STABILITY AND SECURITY OF BITCOIN TOKENS

Note that all the Bitcoin system actually does is enable digital tokens to be moved between participants, with the help of miners who volunteer their computer power to move the tokens around. Whether such digital tokens are perceived to have value or not is a separate, and more complex, issue. Some of the first questions that have been asked about bitcoins are:

- What is the nature of these tokens? Are they money? Where does their value come from?
- Is this perceived value stable, or prone to volatility?
- Is the system safe, or prone to hacks and fraud?

VIII. IS BITCOIN MONEY?

When addressing the first question, it is important to note that our normal money is also just tokens—whether in a digital form or in a symbolic paper or metal form—which people move around either by editing databases (electronic money) or by literally handing over the symbolic physical representation (cash). The construction of the perceived value of the euro or the yen is a historical process involving deep cultural and political dynamics. The value of a US dollar is underpinned by enormous network effects, the fact that hundreds of millions of people implicitly agree that the tokens represent value and the fact that the tokens are deeply anchored in a vast real economy. The fact that so many people are interdependently locked into usage of such tokens makes it incredibly difficult for anyone to deny their perceived value, and if they do so they will tend to find themselves excluded from economic life. To get such tokens into such a central economic position does not come easily—it involves deep interplays between state power, central banks, commercial banks, institutions that protect property title, and the redeemability of legal tender to pay taxes and other debts—but once a monetary standard is established it is very difficult to dislodge.

Bitcoin, by ontrast to a token like the South African rand, has no geographically and politically discreet real economy in which it is dominant. It thus does not tend to be aprimary unit of pricing in any economy—very few vendors explicitly price their goods in terms of Bitcoin as a unit of account—and it is also not widely perceived as a means of exchange. Thus, while it has the potential to be a currency unit, in practice few people actually use, or perceive, Bitcoin as money in a traditional sense.

This has led some national authorities to characterize it as a digital asset rather than a currency. In this sense it bears some resemblance to gold, which similarly has ambiguity as to whether it should be perceived as an asset or as a form of money. For now, though, it suffices to say that

1) Bitcoin is a digital token that can be moved between parties, and
2) the token has market value in terms of major national currencies (the token can be exchanged for dollars, pounds and other currencies) and
3) it is sporadically used—albeit often in small amounts—in exchange for real world goods and services. Perceived risks: Volatility and safetyThe question of what underpins Bitcoin tokens' perceived value—and the related question of its price in terms of fiat currencies—is beyond the scope of this paper.

It suffices to say for now that when Bitcoin first started it was seen by many as a mischievous, subversive, and slightly mysterious, experiment, rather than a serious commercial instrument. The digital tokens went through a fetishization process in which they began to get imbued with imagined value by a small, dedicated group of evangelists, who in turn paved the way for speculators to get involved, and for media outlets to run stories (Glaser et al. 2014). This in turn opened up the tokens' usage to more ordinary people, business owners and entrepreneurs. Today, perhaps the most we can say is that the digital tokens have a perceived value contingent upon theirspecialized usage among specialized communities, and that the construction of thisperceived value is an ongoing process that develops as more players get involved. One key element of this, though, is that—in contrast to locked-in state currency systems—the perceived value (as measured in terms of other currencies) has fluctuated greatly over time. This volatility creates a chicken-and-egg scenario: if more people got involved, the value of the tokens would stabilize, because the larger the user base, the less influence any one user would have in influencing the price.

But many people shy away from using Bitcoin because of the volatility.Another perceived risk that keeps people away is the fact that the Bitcoin system has been subjected to various security breaches, mostly involving third-party services—like exchanges where you can buy bitcoins in exchange for fiat currencies—but also involving hacks of private computers where people have Bitcoin "wallets", the software they use to interact with the system. It is important to note, however, that as the community around Bitcoin has matured and expanded, the security standards havesteadily increased.

Many new markets are initially subject to cowboy or rogue operators who gradually get pushed out by more formal actors over time.

IX. ORASAIFU TOUCHSCREEN SMART WALLET

Cryptocurrency wallet with industry leading security set to launch in mid-July 2018

OraSaifu, a technology company based in Japan with offices in Beijing, New York and Hong Kong, has announced its first revolutionary payment product: OraSaifu smart wallet, a hardware crypto currency wallet that will enter the global payment market in mid-July 2018.

"OraSaifu Wallet will impress the blockchain world with its security technology and the premium digital card screen display performance," commented Leon Liu, OraSaifu Global Market Executive and MIT alumnus.[5].

According to a real-time data tracking by Blockchain.com, the number of active users of blockchain wallet users has exceed 26 million, and Bitcoin wallet holders have grown to over 10 million in 2018. With a daily trading volume rises to $3 billion for the top ten crypto currencies, smart wallets are becoming an unprecedented business opportunity.[7]

There are three Bitcoin wallet types on the current market: hardware, software and paper. Hardware wallets are physical wallets with your private keys encrypted in them, software wallets are programs that live either on your computer or on the Internet, and paper wallets are physical documents with private keys. The OraSaifu hardware wallet enhances all the safety advantages of the current USB wallets such as Trezor and Ledger, and also turned the traditional bank cards payment life into a mobile payment method. OraSaifu wallet is a perfect choice for an all in one solution for all your financial assets storage, transaction and recovery. Features of the smart wallet include the ability to :

- Unlimited storage - OraSaifu is designed to provide a one-stop solution for managing all your crypto currencies, by offering easy and worry-free offline storage, and two step authentication transaction.
- Enhanced security – OraSaifu wallet is 100% isolation from the internet (the USB port doesn't even have a data transfer capability).
- Anti-loss function and easy recovery: with TEE & SEE encrypted chip built-in, OraSaifu Wallet enjoys the world's top anti-theft solution. It will wipe the whole wallet if you fail the authentication more than 5 times.

OraSaifu supports the following digital currencies – Bitcoin (BTC), BCH, BTG, BCD, LTC, GOGE, ETH, ETC, ERC20, EOS, ADA,XRP,XLM, IOTA, NEO, XMR, NEM, QTUM and etc.

OraSaifu's solution offers a mobile payment substitute that allows users to pay anywhere. It allows you to safely store all your credit cards, crypto currencies, even the membership cards in one place, meaning that everything important is accessible at your fingertips. OraSaifu is the first hardware using both (TEE) and (SE) technology in one secure chip to ensure 100% security over your assets and NFC payments. OraSaifu also provides the Cold Wallet mode, compare to traditional hardware wallet using USB port for data transferring. OraSaifu uses NFC and Offline QR code reading technology that is totally isolated from the internet world, meaning you will have full control of your crypto currencies.

Leon Liu concluded "We're delighted to launch the most secure digital wallet on the market today. We hope that our technology will allow more people than ever before to use crypto currencies in a practical way, helping the technology become truly mainstream."[8].

X. Conclusion

The cryptocurrencies are a hot topic in the global financial system. There is great volatility of cryptocurrencies exchange rates. With this, there is a high risk of trading these cryptocurrencies. Their growth has been able to gain the attention of many speculators.

They are easily portable. It is only after the required trust in the cryptocurrencies after which they will be used on a wider scale. If the cryptocurrencies fail to gain that trust, then their boom might decline. They are still in their infancy, and it is not sure as to when they will be maturely traded in the markets globally. Many different cryptocurrencies have gained the required attention. Some nations have started to issue national cryptocurrencies (Hofman, 2014). It is quite possible that shortly, the bitcoins might have a way for cryptocurrencies to flourish. Despite the flaws, bitcoins are still considered tour-de-force in the digital currency. It has provided an alternative currency for the less developed countries and has opened the doors of economic transformation. In this way, it gives the individuals more choices to manage their finances. Without regard to bitcoins accomplishing the lofty transformations, the cryptocurrencies are seen to be entering the financial stage and changing the global financial landscape forever.

References

[1] P. WITZIG and V. SALOMON, “Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry”, Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel,
[2] Bearman, J. (2015, May). The Untold Story of Silk Road, Pt.1. RetrievedfromWired.com
[3] Bitcoin: A New Global Economy. (2015, August 4). Retrieved July 2016, from BitPay, Inc.
[4] Another example of distributed ledger technology is “directed acyclic graph”, the underlying technology of the IOTA-platform (see below). See also: M. VAN DE LOOVERBOSCH, “Crypto-effecten: tussen droom en daad”, TRV-RPS 2018, 193, footnote 2.
[5] See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), “Distributed Ledger Technology (DLT) and blockchain”, 2017, FinTech note, no. 1. Washington, D.C.
[6] www.Google.com
[7] Newspaper:Economic Times
[8] By Bitcoin Exchange Guide News Team -July 21, 2018

