

Cryptocurrency and Blockchain

*Apoorva Jishtu, Grusha Pahwa, Manasa S, Priyanka
Binnani, Shivya Singh*

Introduction

Crypto currency is a digital asset that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. What makes crypto-currency unique is its ability to be decentralized and the fact that it eliminates the necessity of present banking system. Once released in the market, crypto-currency has the ability to facilitate trade and create additional units of the currency with each transaction, leaving no space for a third party to act as the liaison officer.

Block-chain Technology:

Block-chain is a method of securely storing digital information, distributed through a network of participating computers that creates a verifiable record of events. The distributed record of events is called 'distributed ledger technology (DLT)'.

Block-chain is an undeniably ingenious innovation, which allows digital information to be distributed but not copied. A block-chain can be seen as a spreadsheet that is duplicated across all computers in the network, totally public and easily verifiable. Block-chain is said to leave no room for missed transactions, human or machine errors or any transaction taking place without the consent of both the parties.

Using Block-chain, in any form, is like a peer to peer transaction where the need for mutual trust is replaced by cryptography. It is the technology behind Bitcoin and other digital currencies which have exploded in growth in recent years. It has more applications, which be explored later, in form of application in existing systems of voting, transactions and contracts.

Objective

The paper elaborates the working of crypto-currency and block-chain. Though, existing since 2009, crypto-currency is, till date, not regulated nor completely accepted by the world and the financial system. Its working needs to be understood and evaluated before any conclusion can be drawn. Though the working might seem technical, the paper attempts to explain the technicalities in the simplest way possible while elaborating the economic aspect and effect of block-chain and crypto-currency.

As countries and organisations are looking into crypto-currency and block-chain technology, the question still remains, how does it work and can a decentralised currency debase the existing governance and financial institutions? Is crypto-currency just a ponzi-scheme or can it evolve into an asset? We will try to understand the

feasibility of crypto as a means of payment. We look into the possibility of making crypto-currency state owned.

Cryptocurrency and Blockchain

Working of Crypto-currency Transactions

1. Each transaction is broadcasted into the network of the crypto-currency. This broadcast contains the details such as wallet address of the sender and receiver and the amount crypto-currency transferred.
2. Every miner which is active in the network then updates this transaction in their block. This update involves verification of the digital signature and other details. Adding the transaction to a block does not make it valid. Each block needs proof of work to validate it.
3. If the miner is able to add his block to the chain, a special transaction gets added to the top of this block, which gives a certain amount of crypto-currency to the said miner for the work that he has done. This is what we call the reward. This reward increases the total number of crypto-currency in the economy.
4. The transaction looks very similar to any online transaction from a user's point of view. The difference lies in the working of confirming the transaction. Traditionally this verification was done by a bank, creating a need for a third party acting as a middle man, but in crypto-currency it's a peer to peer transaction, confirmed by miners which makes it decentralised.
5. Crypto-currency wallets are very similar to online banking. It has a digital address which is often called the public key which is similar to a bank account number.

Anyone who knows the bank account number can send money to that account, but cannot access or use the balance in that bank account to make transactions.

Similarly public keys allows any individual to send cryptocurrency to the address represented by the public key, but they cannot use the wallet itself.

To access the bank account and make transactions from it's balance you need the password, which each individual keeps confidential.

Proof Of Work and Mining

Crypto-currency mining or crypto-mining is a process in which transactions for various forms of crypto-currencies are verified and added to the block-chain/ digital ledger. Block-chains contain details about every transaction in crypto-currency history which helps the users to validate the new blocks added to the block-chain.

When a block-chain transaction takes place a transaction slip is broadcasted in the block-chain network but in order for miners to attach the transaction in the existing valid ledger/ block-chain, the signature of the sender needs to be confirmed first. So who exactly does this?

Surprisingly anyone who is willing to and is a participant of block-chain network and using cryptography the signature is decrypted and verified.

All miners have a private copy of the ledger with themselves and each time a transaction takes place with a valid signature, they update the ledger.

With ledger spread across all over the network, due to traffic delays and occasional fraud there are different versions of ledger. In order to decide which version to use, like other democratic systems there is a vote but it is a different kind of vote involving mathematical puzzle.

Miners vote by trying to solve a special puzzle based on their version of ledger. The person to first solve the problem announces the solution and everyone else updates his version of ledger and in the process adds a “block” of transaction to the ledger.

In simple terms it is a kind of mathematical race designed to favour the majority. This is because as more number of people work on the problem based on a particular version of ledger the faster they will solve it.

The verification process is automatic, that is, the software mines, validates, verifies and propagates the transactions. Secondly, after the process of solving the puzzle and verifying the transactions end, it releases new currency through the reward system . Each time a crypto-currency transaction is made, a crypto-currency miner is responsible for ensuring the authenticity of information and updating the block-chain with the transaction.

How is the Block-chain Secured?

With a decentralized system, the foremost question is how to ensure that all transactions are recorded? Well the system is designed to ensures its own security. For example: Let us assume that everyone is working on Block 91. A miner wanted to alter a transaction in block 74. To do so he has to make changes in block 74 and redo all blocks from 74 upto 91. This is because each block contains the hash of the previous block, and hence any change in the chain leads to a domino effect.

This is not only expensive but also impossible because as said earlier everyone else in the mining network are working at block 91. So to be successful he has to not only redo all 18 blocks but has do it before everyone else works on just one block, that is block 91, and move further in the chain. But what stops him from altering the 91st block?

Well here, if he wants to trick the system he has to create a new block faster than the combined speed of the entire network. While trying to create this new block without his transaction in the chain, he creates a fork. For his block to be accepted his chain must grow faster than the other one. This is because as per rules the longer chain in the network is accepted. It is basically one hacker’s computer v.s the world’s computing power. As obvious as it seems, this is unfeasible.

Now one might go further and ask, what if hacker’s pool together in a mining network?

This will lead to what is called a 51% attack.

For a 51% attack to occur, the attackers will have to gain enough power to control

events in the network. They will then have a monopoly over generation of new blocks and can leave out or reverse any transaction they want. When a fork happens in the chain because of the other 49% miners, the attackers will work on their chain, which will last longer in the network as they have majority computational power. The longer chain gets accepted in the network and hence the attackers will have a monopoly or full control over all transactions.

Even though 51% attack might give them monopoly, it is not a profitable option. It will require a lot of mining power which is not only expensive but nearly impossible to achieve.

Blockchain Transformations

Alternative to SWIFT

Block-chain can work as it has been explained for crypto-currency, with a public ledger being used and updated for transactions, instead of using SWIFT to send just messages of said transactions. While SWIFT is capable of just sending messages, the block-chain can be used for the actual transaction, like in the case of crypto-currency.

If block-chain instead of SWIFT is used for international payments it eliminates:

1. Transaction fees at multiple levels.
2. The time lag of 2-3 days that often occurs with transactions through SWIFT.
3. Reduce the bank's cost of processing payments.
4. Reduce the paperwork.
5. Block-chain can not only be used for the money transfers but also for the transfer of documents which often occur during international trade. This further adds to cutting down the costs of overseas trade.

Smart contracts:

In global finance, forward rates are rates at which future exchanges of currencies take place. The rate, though is decided today, the actual exchange will take place at a predetermined date in the future.

Something similar to this is the concept of Smart Contracts. It essentially is a program, to fulfil a certain exchange of digital asset(s), if and only if conditions which we decide on today are met thereby acting as trigger to the completion of the the transaction.

An example: French Airline AXA is using block-chain technology to offer to its customers insurance against delayed flights with Fizzy, the platform being used for the same. One simply has to buy the flight delay insurance on Fizzy, the purchase is recorded on the blockchain and the contract (connected to global air traffic databases) is now rendered immutable. In case the flight does get delayed, your compensation reaches

you automatically without any cumbersome procedures to procure the same hence increasing efficiency and trust in operations.

Here is how smart contracts work:

1. The involved assets and the terms are made into a contract (cryptographic code) and put up on the block-chain.
2. Multiple copies of the same contract are distributed on the block-chain ,making it immutable. The outcome is also verified/validated by everybody on the network.
3. When the terms of the contract are met, the release of funds take place automatically through the smart contract. Or simply, if X happens(conditions are met), then Y happens(execution of the contract).

Smart contracts have potential use in many practical spheres, besides Insurance-

1. Voting- Doing away with red tapism, smart contracts can essentially make votes immutable after they are recorded, hence increasing efficiency and minimising the risk of any tampering of results.
2. Copyrights- They can keep track of ownership rights ensuring that royalty payments are made real time to the true owner.
3. Supply Chain- They can induce transparency and greater degree of coordination in the supply chains.
4. Trade Finance- They can be used to ease the transfer of credit between buyers and sellers reducing cumbersome payment making and receiving procedures otherwise involved.

Health care, mortgages and IOT are also areas where smart contracts have a future. Smart contracts are fast leading to considerable time saving and precise since all details are already incorporated into the contract. Transparent as they are, they do away with intermediaries in transactions and are hence cost efficient as well.

While smart contracts essentially make use of the blockchain, they ensure more efficiency, less paperwork, more transparency and less scope of corruption and red tapism. They can replace all forms of paper contracts that exist today, from government work such as construction contracts to private builders, retirement pension to employees, to private forms of contracts such as annuity payments and fundraisers.

Block-Chain A Case Study of Estonia

Using Estonia's example let's look at how we can incorporate block-chain technology into various sectors:

1. E Residency: Block-chain technology can be used to generate E residency. E residency program allows us to receive a government issued smart ID card that provides digital identification and authorisation which can be used to assess a number of services like establishing a company online, e-banking, sign documents online that have legal validity, etc. All this can be done while sitting at home. We

don't even need to be a citizen of any particular country to have an access to E residency. E - ID system is based on advanced encryption technology . This works by tying digital identity through block-chain .

And the proper working of E Residency in Estonia makes perfect sense to expand this digital service to the rest of the world.

2. E Health: Block-chain technology can also be used in healthcare sector to save people's medical records. Estonia became the first country in the world to incorporate the Block-chain into their healthcare system. Every Estonian has their health record digitized and stored on a Block-chain. It has established the block-chain technology in their healthcare system so that people can also log into their own records using their digital identities. This is especially critical in emergency situations where the doctors can simply use the patient's ID to get information such as blood type and allergies without losing any time.

Future of Cryptocurrency

Case study of Japan:

While the world is still a bit wary about the whole matter of crypto-currency and its relevance in today's economy, Japan does not seem to be slowing down it's accepting approach towards Crypto-currency and as of April 2017, recognizes Bitcoin and other digital currencies as legal tender under the Payment services act.

Crypto-currencies contribution towards Japan's GDP has been recognised as a result of which in December 2017, the National tax Agency ruled that gains on crypto-currencies should be categorized as 'miscellaneous income' and investors taxed at rates of 15%-55%.

Japan has a relatively high number of "smart" automatic teller machines (ATMs) capable of handing crypto-currency trading.

Japan: Heart of bitcoin, did not become the centre of emergence of crypto-currency because of the collaboration of prominent investment giants of the country but started out of the collaboration of Jed McCaleb , a programmer who in the late 2006 thought of building a website for its users of the card game 'Magic : the gathering online" where they can exchange their game cards just as stocks.

Jed purchased the domain name "mtgox.com" and later he felt that there was not enough potential in this and thus moved on to his other projects. With the slow emergence of crypto-currency around the world Jed felt the need to provide an exchange to trade bitcoin and other currencies. He handed over his site to french developer Mark Karpeles , in March 2011 saying "to really make mtgox what it has the potential to be would require more time than I have right now. So I've decided to pass the torch to someone better able to take the site to the next level."

The event of the great Mt Gox's 460 million dollars (33,79,85,00,000 Indian rupees) disaster has far been etched in the crypto-currency history as the biggest hacks of all

times and might as well be for the coming time but Japan did something completely opposite to what the world thought it would. Japan maintained a supportive regulatory environment and moved to regulate new exchanges and allowed retail payments. Exchanges are legal in Japan, but after a series of high profile hacks crypto regulations have become an urgent national concern. Japan's Financial Services Agency (FSA) has stepped up efforts to regulate trading and exchanges: amendments to the Payment Services Act now require crypto-currency exchanges to be registered with the FSA in order to operate – a process which can take up to six months, and which imposes stricter requirements.

Japan also has its own indigenous crypto-currency: Monacoin(MONA) which is a decentralized open source crypto-currency forked from Litecoin and launched in January,2014. New coins are issued as payment for mining activities, which allow the ownerships of tokens to be recorded into the MonaCoin block-chain.

The cap is 105,120,000, and no coins were 'pre-mined' before becoming available to the public. It is particularly successful in Japan community such that there are now shops in the country where bitcoin and Monacoin are accepted. 90% of users of monacoin are based in Japan and although it has little relevance outside Japan but is quite famous in Japan.

Currently there are five exchanges which facilitate the transactions of monacoin , 3 of which are situated in Japan. It is believed that Mona was formed more out of culture desire of japan to have its own indigenous crypto-currency rather than for profit purpose. The Crypto-currency was founded by- Mr Watanabe- who just like the founder of bitcoin - Satoshi Nakamoto- remains to be unknown.

Why is Japan so persistent in its commitment for the growth of crypto-currency?

Japan has witnessed ultra low interest rates for many years , that means the returns from the traditional assets have been low for many many years which has gone as far as having negative interest rate meaning now there is a cost attached to saving.

With the emergence of Crypto-currency, it provides a new source of investments with much higher returns than the traditional ways.

In such a situation investing into alternatives such as crypto-currency with higher yield seems to be more attractive to the investors. However, crypto-currency is still not as stable in the rest of the world as it is in countries like Japan and China.

Also the worldwide crack down of use of Crypto-currency will attract more investors in Tokyo , which encourages Japan to continue its quest to explore the field of Crypto-currency and hopes to use it in their favor to boom it's economy.

The case study of Japan puts forth one possible route to take with crypto-currency, that is trade in crypto-currency in a country as an alternative source of transaction or investment.

The block-chain will eventually grow, can also stabilize once it is government approved and the security related to crypto-currency is improved, and will grow in sync with the algorithm.

The only roadblock here is the possibility of everyone just trading in crypto-currency, elimination of the demand for high powered money and the central bank losing control over the supply of money. The possible solution to this would be for the central bank to mint the crypto-currency chain.

It can then control the reward rate, which will give them control over crypto-currency supply just as they have control over high powered money.

This will then require two assumptions.

1. **Fixed money base but no fixed supply:** While talking about the present crypto-currency we have a fixed supply of these coins(for bitcoins it's 21 million). This was done because in a decentralized system there is no body/institution regulating the monetary base.

Crypto-currency makes up for this lack of centralized system controlling the monetary base, by controlling it through algorithms which work with a cap on maximum amount of crypto-currency that can be created. This fixed cap does solve the problem of control over monetary base but creates a new problem of its own.

With fixed supply, the value of bitcoins is ever increasing. This means that with the same amount of bitcoins you can buy more and more goods which implies that the price of goods is decreasing.

If we look at a fixed money supply model with growing GDP, deflation takes place.

$$MV = PY$$

If M(money supply) is fixed and GDP is growing, the value of Y will increase. To maintain equity P will decrease (deflation). The general idea is that deflation is a decrease in the price of goods and services.

If we talk of crypto-currency particularly, an increasing value of a crypto-currency means the cost of paying for things using that crypto-currency is decreasing, i.e the price of that good is decreasing. Also in deflation people hoard money, unwilling to buy things presently, assuming that later it will be cheaper and hence more profitable. Investment will tend to be low in the economy which is not desirable.

Clearly deflation is not a desirable characteristic in an economy and hence under our model, crypto-currency will not have a cap on maximum amount of coins that can be produced.

We will still have a fixed money base. This means that the amount of coins produced by the central bank or any central authority will be fixed. The initial release of crypto-currency will be made by the central bank, the amount of coins released equal to the money base.

The control of central bank over money supply will not be established through minting new coins but through the reward rates.

2. Reward rate is the new interest rate:

With a fixed money base, we take away the control of central bank over the money supply, which is what the original system of crypto-currency demanded. This loss of control is in terms of not being able to print new currencies themselves. The need and importance of central bank having some control over money supply is undeniable and hence we need to make some alterations in the present system to incorporate the central bank.

The work which is presently done by the interest rate can be performed by the reward rate. Presently reward rate is determined in the crypto-currency using algorithms and alters with the idea what there is a maximum cap for the amount of coins that can be generated. Since we have removed the cap for reasons explained earlier we have to now find a new way for determination of reward rate. By substituting interest rate with reward rate, we solve both these problems.

If the economy requires higher money supply, that is higher money demand, the central bank can increase the reward rate. With higher rewards rate with each transaction more crypto-currency will be introduced in the system, hence the supply will increase without the government actually minting new coins.

Volatile market:

The crypto-currency exchange rates are highly volatile, which makes it less attractive to investors and general public as the risk increases.

The main theories behind this high volatility is:

1. The public perception of crypto-currencies is quite dichotomous. Various factors like increased interest in Asia, the Japanese stand on it, many enterprises showing interest in it etc have had a positive impact on the outlook towards crypto increasing it's demand, but on the flip side a hard-fork, negative changes in the legality of crypto-currencies, and hacks could very easily destroy their public interest. Like any other commodity crypto-currency price is highly determined by its demand, which seems to change a lot because of various factors and hence its price is quite volatile.
2. No intrinsic value: This again makes crypto-currency highly dependent on market sentiments, which are highly volatile.
3. Lack of regulations: this makes the crypto-currency more risky as market manipulation is easy and discourages institutional investment or large funds.

How can this volatility decrease?

With some more regulations and legal assurance a more mature outlook and a diverse set of investors will be invited into the crypto-currency market. This can ensure less fluctuations in the market prices.

Backing crypto-currency:

In our model, the supply of crypto-currency isn't fixed and only the monetary base is fixed. It is accepted as legal tender and people use these tokens for their transactions. Backing it up by the central government brings about the requirement of anchor reserves of that resource. It will work just like the currency that we have in the present. The Indian Rupee is backed by foreign exchange (95%) reserves and gold (5%). Rupee isn't actually backed by any real thing like gold or other precious metals. There are promissory notes where the RBI "promises" to pay a value of Rs 100 against a 100 Rs note. Indian Rupee has backing only in theory and it will be worthless if every Indian stops accepting it for some reason. The RBI or the Government of India does not promise back the INR with gold.

Many countries have backed the crypto-currencies they have created to world's most stable asset : gold . Gold stays relatively stable, while bitcoin's price fluctuates widely day to day. It's a safeguard against economic unrest or the inflation of a fiat currency and even if the stock market crashes, we have still got some physical assets sitting in a safe. So , backing crypto-currencies using gold is not a bad option . Many countries of Middle East , Dubai , Singapore have backed their crypto-currencies using physical gram of gold .

But the gold backing is not a viable option either, as India doesn't have much gold reserves . And also it creates the concern of storing a large supply of physical gold reserves.

Therefore the backing of crypto-currency in the model is done through the traditional way of the preferred backing option as 95% foreign reserves and 5% gold .Our model which has crypto-currency as the legal tender performs the same function as Indian Rupee and is built around the same framework(fiat currency and has no intrinsic value).

Conclusion

This paper sets out to provide a general exploration of block-chain and crypto-currency. Block-chain technology allows data to be decentralized yet never duplicated providing complete integrity over it since no third party can make any changes to it while the data is in transit. This technology can be used in several government services because it helps in connecting different authorities to one another and even different countries to one another while keeping all the data confidential. The uses so suggested work in different spheres but lead to the common goal of effective and transparent sharing of information. Block-chain can be exploited in any field which deals with or needs to share and spread data.

The issues which have to be addressed if crypto-currency gets accepted as fiat currency is the fear of Central bank losing control over money supply and the elimination of high powered money. If we assume a cap on the money supply, the problem of control over monetary supply will be solved but it will lead to something undesirable-deflation. Instead, if reward rates replace interest rates and can be adjusted by the central bank according to the requirement of money supply in the economy the government will not

have to mint more coins or reduce it preventing inflation or deflation from taking place. Hence, we can still have a fixed monetary base which equals the initial release of coins by the Central Bank and the money supply in the economy can be kept in check through reward rates. This also solves the problem of volatile market and extreme exchange rates.

While it may be too early to comment on whether and when a full scale adoption and legalization of crypto-currency takes place, we can definitely see it as possibility and also acknowledge that there will be need for even further advancements in technology to ensure higher standards of safety and acceptance of crypto-currency.

References

1. Allison, Ian "If Banks Want Benefits of Blockchains, They Must Go Permissionless".
International Business Times.
"If Banks Want Benefits of Blockchains, They Must Go Permissionless"
2. BBC Newsnight : published on 24 th January , 2018
<https://www.youtube.com/watch?v=cRxL2GKDU5E>
3. Greenberg Andy (20 April 2011).
"Crypto Currency". Forbes.com.
"Cryptocurrency"
4. Heller Nathan(2017)
Estonia : The Digital Republic
The New Yorker
<https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>
5. Iansiti Marco; Lakhani Karim R. (January 2017).
"The Truth About Blockchain".
Harvard Business Review. Harvard University.
"The Truth About Blockchain".Harvard Business Review" Harvard University
6. Iosrjournals.org. (2019). IOSR.
Available at: <http://iosrjournals.org/iosr-jef.html>
ISSN 2321-5925
7. Kufner Robert -April 11, 2018- Medium
"Breaking down the Smart Contract"
<https://medium.com/nakamo-to/breaking-down-the-smart-contract-45b249b8bc71>
8. Lee Sherman-July10, 2018
Forbes
"Blockchain smart contracts-More Trouble Than They Are Worth"

[https://www.forbes.com/sites/shermanlee/2018/07/10/blockchain-smart-contracts-more-trouble-t
han-they-are-worth/#6e21bb8f23a6](https://www.forbes.com/sites/shermanlee/2018/07/10/blockchain-smart-contracts-more-trouble-than-they-are-worth/#6e21bb8f23a6)

9. Nakamoto Satoshi
Bitcoin- a peer to peer electronic cash system
“Bitcoin: A Peer-to-Peer Electronic Cash System
10. Nakamura Yuji(April 10,2018)
While the World Cracks Down, Japan Emerges as a Crypto Haven
[https://www.bloomberg.com/news/articles/2018-04-10/while-the-world-cracks-down-japan-emer
ges-as-a-crypto-haven](https://www.bloomberg.com/news/articles/2018-04-10/while-the-world-cracks-down-japan-emerges-as-a-crypto-haven)
11. Seshnath.blogspot.com. (2019).
US,
Indian Rupee and Gold
<http://seshnath.blogspot.com/2011/04/us-dollar-indian-rupee-and-gold.html>
12. Virtual Currencies and Beyond: Initial Considerations (PDF).(2016)
IMF Discussion Note.
International Monetary Fund.
13. Zibell Lotte, Phair Nigel
How secure is the blockchain.
World Economic Forum
<https://www.weforum.org/agenda/2018/04/how-secure-is-blockchain/>