An Overview of Blockchain, its Mechanism, and its Revolutionary Influence on India

** Prerna Talreja*
*** Darshan Tom*
**** Celestin Anto*

Abstract

This paper offers an insight into blockchain and its mechanisims. The blockchain methodology has been broken into parts for easier understanding. This paper also depicts the corelation and risk and returns of five major cryptocurrencies, this forming a part of primary formulation. The risk and return graph helps in interpreting which of those five cryptocurrencies are the major investment gems. The concept of mining has also been covered in brief. Moreover, this paper also highlights the pros and cons of the blockchain mechanism. India with and without blockchain is compared. Furthermore, the impacts and advantages to the Indian economy are listed, thus forming a part of secondary source of methodology. Upon formulation it becomes clear that the five cryptocurrencies have a positive corelation and are highly corelated to each other.

Keywords: Blockchain, cryptocurrency

I. INTRODUCTION

Blockchain is a decentralized peer to peer system. In the system millions of computers agree on global record of the history of all transactions that have ever taken place in the system. This global record is called a ledger. When you transfer some money or service in the blockchain everyone in the system knows about it.

It is easy if you can think of it like another peer to peer service like Limewire or Torrents where instead of transferring files you are transferring a transaction entry into a very long notepad of all transactions and the notepad can be seen by everyone because there are millions of computers keeping track of all the transactions. This makes it impossible to cheat and create multiple fraudulent transactions.

Modern technology allows people to communicate directly. Voice and video calls, emails, pictures and instant messages travel directly from person to person maintaining trust between individuals no matter how far they are. When it comes to money people have to trust a third party to be able to complete a transaction. Blockchain technology is challenging the status quo in a radical way by using math and cryptography blockchain provides an open decentralized database of every transaction involving value, money, goods, property, work or even votes. Creating a record whose authenticity can be verified by the entire community.

The future global economy will move towards one of distributed property and trust where anyone with access to internet can get involved in blockchain based transactions. Third party trust organizations may no longer be necessary.

II. METHODOLOGY

This research is done purely on the basis of secondary data collection method. We collected information from various secondary data sources such as; newspaper articles, websites and references from other research papers. We \worked on various research gaps. We also dealt with formulation of risks and returns as well as the correlation through application of formulas.

III. OBJECTIVE

Our motive is to introduce in simpler terms the mechanism of blockchain, types, and mining of cryptocurrencies. Here the intent was also to justify through research the impact, importance, and scope of blockchain technology with regards to the economy of India; also to obtain the riskiness of various blockchain

Manuscript received January 15, 2018; revised February 8, 2018; accepted February 15, 2018. Date of publication March 6, 2018.

* P. Talreja is with St. Joseph's College (Autonomous), Bengaluru, India - 560027 (email: prernatalreja7@gmail.com)
** D. Tom is with St. Joseph's College (Autonomous), Bengaluru, India - 560027 (email: darshantom7@gmail.com)
*** C. Anto is with St. Joseph's College (Autonomous), Bengaluru, India - 560027 (email: celestinanto96@gmail.com)

DOI: 10.17010/ijcs/2018/v3/i2/123213

investments and their returns in comparison to their risks. Moreover, arriving at a correlation between the cryptocurrencies to know if they move in the same trend or not.

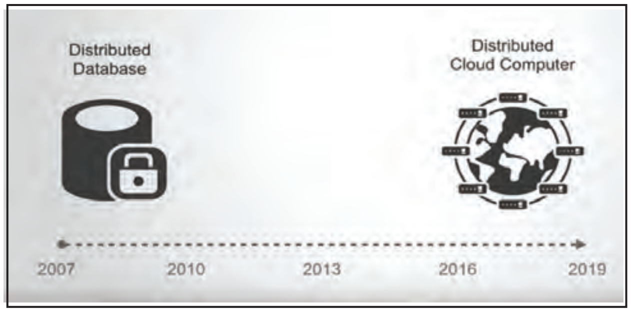
IV. ORIGIN AND EVOLUTION OF BLOCKCHAIN

The first blockchain was conceptualized in 2008 by an anonymous person or group known as Satoshi Nakamoto. The concepts are technicalities described in an accessible whitepaper termed Bitcoin, a peer-to-peer electronic cash system. These ideas were first implemented in 2009 as core component supporting Bitcoin where it is served as a public ledger for all transactions. The invention of the blockchain for Bitcoin made it the first digital currency to solve the double spending problem without the need of a trusted authority or central server. It was only later we came to separate the concept of the blockchain from that of its specific implementation as a currency in Bitcoin. The underlying technology had more general applications beyond digital currencies in its capacity to function as a distributed ledger tracking and recording the exchange of any forms of value.

A. Bitcoin and Other Cryptocurrencies

Cryptocurrency is a form of currency that is built on a global digital distributed ledger called blockchain. It is called cryptocurrency simply because it uses a form of mathematics called cryptography, which allows participants in the system to have a unique address called a wallet, kind of a bank account to which only the owner has access to. It mathematically proves that money sent or received to this wallet is actually going to the right person. A wallet can be mathematically checked for accuracy but can't be altered or tampered in anyway.

Fig. 1. Distributed Cloud Computing



Bitcoin is the first decentralized digital currency. Bitcoins are digital coins you can send through the internet. Compared to other alternatives Bitcoins have a number of advantages. There is a capital supply of 21 million coins for Bitcoins. Bitcoins are transferred directly from person to person via the internet without going through a bank or a clearing house.

Ethereum is another cryptocurrency which is an open source public Blockchain based distributed computer platform featuring smart contract functionality. It provides a decentralized Turing-complete virtual machine which can execute computer programs using a global network of nodes. Other prominent cryptocurrencies include Ripple, Cardano, Litecoin, and Bitcoin Cash etc.

The Bitcoin design has been the inspiration for other applications and has played an important role as a relatively large scale proof of concept. Within just a few years the second generation of blockchains emerged as a network in which developers could build applications. Essentially, since its beginning its evolution into a distributed virtual computer was made technically possible by the development of the Ethereum platform.

Ethereum was initially described in a whitepaper by Vitalik Buterin in late 2013 with a goal of building distributed applications. The system went live almost two years later and has been very successful in attracting a large and dedicated community of developers, supporters, and enterprises. The important contribution of Ethereum as the second generation of blockchains is that it worked to extend the capacity of the technology from primarily being a database supporting Bitcoin to becoming more of a general platform for running decentralized applications and smart contracts.

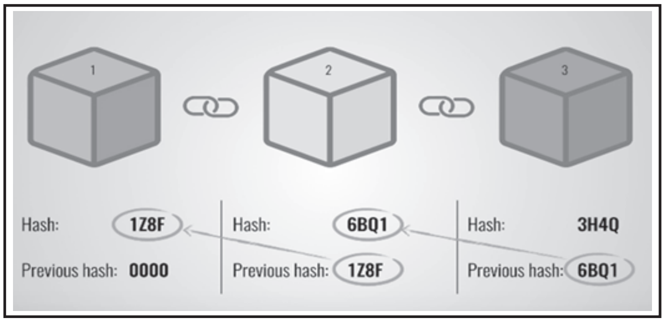
As of 2018, Ethereum is the largest and most popular platform for building distributors applications. Many different types of applications have been built on it, from social networks to identity systems to prediction markets, and many types of financial applications. Ethereum has been a major step forward and with its advent it has become ever more apparent that we are heading with the technology which is development of a globally distributed cloud computing platform on which we can run any application at the scale and speed of today's major websites with the assurance that it has the security resilience and trustworthiness of today's blockchains.

B. Blockchain Explained

A blockchain is a distributed ledger that is completely open to anyone. It has an interesting property: once some data has been recorded in a blockchain, it becomes very difficult to change it. This is because each block contains some data, the hash of the block and hash of the previous block. The data that is stored inside the block depends on the type of blockchain. The Bitcoin blockchain for example, stores the details about a transaction, such as the sender, receiver, and amount of coins. A block also has a hash. You can compare a hash to a fingerprint. It identifies a block and all of its contents and it is always unique, just like a fingerprint. Once a block is created, its hash is calculated. Changing something inside the block causes the hash to change. In other words, hashes are very useful when you want to detect changes to blocks. If the hash of block changes, it is no longer is the same block.

The third element inside each block is the hash of the previous block. This effectively creates a chain of blocks and it is this technique that makes a blockchain so secure.

Fig. 2. Blokchain hashing



Using hashes is not enough to prevent tampering. Computers these days are very fast and can calculate thousands of hashes per second. One can effectively tamper with the block and recalculate all the hashes of other blocks to make the blockchain valid again. To mitigate this problem, blockchains have something called proof-of-work.

1) Proof of Work: It is a mechanism that slows down the creation of new blocks. In the case of bitcoins: it takes about 10 minutes to calculate the required proof-of-work and add a new block to the chain. This mechanism makes it very hard to tamper with the block because if one block is tampered, the proof-of-work for all the following blocks needs to be recalculated. So, the security of a blockchain comes from its creative use of hashing and the proof-of-work mechanism.

There is one more way that blockchains secure themselves and that is by being distributed. Instead of using a central entity to manage the chain, blockchains use a peer-to-peer network and everyone is allowed to join. When someone joins the network, he/she gets the full copy of the blockchain. The node can use this to verify that everything is still in order.

When someone creates a new block, that new block is sent to everyone on the network. Each node then verifies the block to make sure that it hasn't been tampered with. If everything checks out, each node adds this block to its own blockchain. All the nodes in this network create consensus. They agree about the blocks that are valid and also the blocks that are invalid. Blocks that are tampered with are rejected by other nodes in the network. To successfully tamper with the blockchain one needs to tamper with all blocks on the chain, redo the proof-of-work for each block, and take control of more than 50% of the peer-to-peer network. Only then the tampered block can be accepted by everyone else. This is almost impossible to do!

2) Mining: Mining is the process by which the authenticity of transactions in the blockchain is verified and it is what keeps the blockchain running fine, like banks in case of paper money. It is not necessary that every blockchain should support mining. Mining can be explained in terms of Bitcoin blockchain. In the case of Bitcoin, miners use special mining software to solve mathematical problems (solves Bitcoin algorithms) and these are issued a certain number of bitcoins as reward. This provides a smart way to issue currency and it also creates an incentive for more people to mine. Since miners are required to approve Bitcoin transactions, more miners means a more secure network. The Bitcoin network automatically changes the difficulty of the mathematical problems depending on how fast they are being solved. In the early days, miners used to solve these problems with their processors and their computers.

Soon miners discovered that graphics cards used for gaming were much better suited for this kind of work. Graphics cards are faster, use more electricity, and generate a lot of heat. The first commercial Bitcoin mining products included chips that were reprogrammed for mining purpose. These chips were faster but still power hungry.

Application Specific Integrated Circuit (ASIC) Chips are designed specifically for Bitcoin mining. ASIC technology has made Bitcoin mining faster while using less power. As the popularity of Bitcoin increases, more miners join the network making it more difficult for individuals to solve the algorithm. To overcome this, miners have developed a way to work together in pools. Pools of miners find solutions faster than their individual members and each miner is rewarded proportionately to the amount of work he/she provides. Mining is an important and integral part of Bitcoin that ensures fairness while keeping the network stable, safe, and secure.

3) India Wihout Blockchain: Blockchain technology has not yet been introduced to the Indian economy. This means that there are a lot of drawbacks which India is facing currently. As we have discussed above, the blockchain technology brings a lot of progress in any field with incurring less cost. Now let us have a look at what the situation in India is.

a) Corruption: Many Indian hands are stained with corruption. A simple job needs a helping hand of corruption to become perfect. Any hard job can be made easy with a sum of bribe. At the same time, any easy job can be made hard and nearly impossible if the associated officials don't receive the sum of bribe they demand.

Any criminal (big or small) can be bailed out with the help of money and power. Any convict can be deemed to be an innocent or vice versa. We have become slaves of money and money has become the actual ruler.

b) Middlemen: In India there is no such thing called a perfect deal without a middleman. Deals or transactions are interfered with by middlemen. Commissions must be paid as demanded or middlemen might create some kind of issues between the deal or the parties to the specific deal. It has become mandatory to contact a middleman for any sort of deal. For example, a real estate deal, buying or selling goods, and services needed, etc.

c) Privacy: Do you actually think that our personal details are safe and private? No, they are not. Our private data and all other personal information are not in safe custody. This can be because of various reasons. Personal information can be unsurprisingly sold to a third party for money, it can be stolen if it is not properly safeguarded or it can also be lost if it is not properly stored.

Taking a simple example, when we register online for an entrance exam, the next day after a successful registration, we start getting calls and text messages stating information about different colleges for our future studies. How is this happening? It is basically that these institutions sell our basic personal information to a third party.

d) Transparency: There is no transparency to the transactions done. There are millions of currencies being transferred from one place to another around us. We have no idea where the money is going, to whom is it going, and for what is it going. The authenticity of a transaction is poor.

e) Safety: There is very less safety for our transactions . It can be interfered by a virus or malware which can disturb the transaction or even acquire our personal information, which is also called hacking. It is very dangerous to give our bank details or other personal details to a third party for any purpose. Cyber thefts are increasing on a daily basis. Even banks are unable to safeguard our accounts at times. If they could, there wouldn't be bank robberies and ATM thefts.

f) Sources and application of funds: Do you know where your funds have been utilized or have you ever doubted whether your funds are in safe hands? The government of India collects taxes. We don't have any idea whether our hard earned money is been utilized. Different bills are produced but we all know that bills can also be faked.

Many institutions never disclose their sources of funds to the public. Therefore, any personnel can directly or indirectly be a part of any financial or non-financial institution in India. Sometimes proofs for such sources and application of funds can be cooked up according to personal interests.

g) Taxation: The number of taxpayers in India is very less compared to the population that is earning. Tax is either exempted or evaded. Exemption under different sections upto a certain limit is allowed. Evasion of tax is a crime; it is against the Income Tax rules of India. Not filing Income Tax on your returns is also a crime There are a huge number of people who do not fill their IT returns. People who evade taxes are even more in number.

h) Manipulation of financial records: Many companies and individuals manipulate their financial records in order to show lesser income than their actual income to avoid tax and for various other purposes. The higher authorities manipulate the records however they want .

4) India with Blockchain: Distributed Ledger Technology or Blockchain is going to be the next big invention following the internet itself. It is expected that Blockchain promises "trust" through transparency that was difficult to secure on the internet.

The idea of a public, shared, distributed database of transactions maintained jointly by all participants is a powerful concept that can find application in nearly every sphere of life where transaction records need to be maintained. It is basically the opposite of the current system, which is where every participant privately records transactions and periodically achieves consensus via reconciliation. The current way of private recording is a direct fallout of the Double Entry Book-keeping system that originated around 17th century in Italy.

Start-ups, individual companies, industries, financial institutions, industrial bodies, governments, and regulators are all finding promising and appealing areas for blockchain application to deliver quick, efficient, cost-effective, transparent, and impactful solutions to current sub-optimal systems. Blockchain applications are appearing across a vast range of use-cases from alternative currencies to global payments, remittances, securities clearing, settlements, insurance contracts, land record management, tokenization, and sharing of physical and digital assets, document storage and management, proof of existence certificates, KYC, identity managements etc.

When India adopts such an innovative technology, it is going to progress very fast. The disabilities of Indian economy will mostly be solved by this technology. This technology is going to uncover the mask worn by corrupt. There will be high level of transparency in all the transactions. It gives no opportunity to commit any crime or mistake. There is no need of secrecy to be maintained towards the public. Let the public know what and how things are being managed and executed by the hands in power. No one is backing the power of controlling the blockchain technology. Therefore, no authority or individuals in power can correct or redesign the data and proofs.

There are high-speed cross border transactions available for us through this blockchain network. There is no involvement of any exchange or any central authority in these transactions. This service can be available to everyone for a very less fee compared to the exchanges that are working currently in the world.

a) Corruption free: When talking about eradicating all the misappropriate deeds carried out in the Indian economy, let us start from the most tainted one named “corruption”. There is no room for corruption by any human in the blockchain technology. There is proper maintenance of all the transactions across the blockchain network and anyone and everyone can see and understand these. All transactions in the blockchain network are backed with proof.

b) Elimination of middlemen: Now let us talk about eliminating middlemen. There is no role for any middleman in the blockchain network. It is a pure peer-to-peer network. It involves only two people in a transaction, one the sender and another the receiver. There isn't any role for any kind of third person in a transaction done this way. The country can attain freedom from the middlemen and their commissions in any given transactions. This can be eliminated by the adoption of blockchain technology.

c) Safe hands: There is high level safety and security in a blockchain network. No one can hack or manipulate the network. As the name suggests, blockchain is a chain of blocks that contains records of the transaction. Each block is connected to the other blocks which pre and post follow it. Therefore, it is impossible for a block to be hacked. Even if anyone tries to hack it, they need to change the data of each and every block that pertains to a complete transaction. Every block is protected with Cryptography. No one can manipulate the data for any given purpose. Our transactions will be highly protected against malware and viruses which can cause failures in the transaction.

d) Privacy: There is option of high level of privacy in the blockchain network. The information about a transaction is known only to those involved in the particular transaction. There is no outflow of the transaction through a third party such as middlemen, banks, or even the government.

e) Clear as crystal: There is complete transparency in a blockchain network. All the transactions are recorded in a valid ledger which is fully auditable. Entries to the ledger can be made only if they are validated by the system. Anyone can get a check of the transaction proofs and any ledger available in the network. Therefore, there is less need for financial reports. The public can know where the funds are flowing and the reasons for it. This technology doesn't allow anyone to hide anything from the public; everything is brought to light.

f) Taxation made easy: Taxes can be collected easily as the network maintains data of all the transactions. This provides an opportunity for the IT department to levy tax on everyone's income as the blockchain network collects all information of every individual and companies. Taxes can be computed automatically with the help of this network.

g) Voting made perfect: There are many problems regarding the voting system in India. There are many manipulations done in the system. As blockchain technology can't be manipulated, it can be very useful for voting. We can be sure that all our votes are valid and are counted. As blockchain technology works online, everyone can vote for their candidates from wherever they are comfortable. It can be done from your home, office, street, etc. There is no need to stand in long queues and under the harsh sun in order to just vote.

C. Research Gap

This research paper was based on secondary data collection. It purely pertains to the Indian economy and provides only an overview of the topic. Also, the accuracy of the correlations may defer as various systematic risks aren't taken into account. Furthermore, this paper only covers five major cryptocurrencies and does not talk about many other digital currencies.

D. Findings

The inference of our research was that this technology will go on to be the next big digital move in India and will enhance transparency by gaining the trust of citizens. One major shortcoming of blockchain in India is the lack of knowledge about it. Thus, this shortcoming might delay gaining trust of the market.

As we can see in fig. 3, Bitcoin, Bitcoin cash, Ethereum, Litecoin are having lesser risk as compared to the others. At the same time they are having less return. These are meant to be stable. Ripple, OMG, and QTUM on the other hand have higher risk and have higher return. These have high fluctuation. It can be seen in fig 1. that Ripple seems to be a better investment for the investors who are ready to take little higher risk in order to gain better profits.

Fig. 3. Risk and return analysis of top trending cryptocurrencies

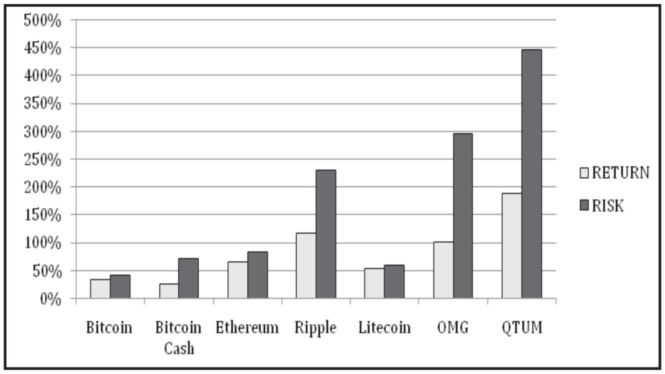


TABLE I.
CORRELATION OF MAJOR CRYPTOCURRENCIES

CORRELATION	BITCOIN	BITCASH	ETHEREUM	RIPPLE	LITECOIN
BITCOIN	-	0.98	0.95	0.83	0.94
BITCASH	0.98	-	0.88	0.88	0.97
ETHEREUM	0.95	0.88	-	0.86	0.96
RIPPLE	0.83	0.88	0.86	-	0.96
LITECOIN	0.94	0.97	0.96	0.96	-

Highly positive correlation between all variables as all are close to 1.

*

V. CONCLUSION

In this research paper we have encompassed the working mechanism of the blockchain system and briefly introduced various cryptocurrencies. This could blend very well with the current digitization policy of India. Thus, by introducing this system, India can minimize, if not eradicate corruption, manipulation, and also realize tax collection. Thus, these are early days for the Blockchain technology but the potential is phenomenal, and this potential can be enhanced by further research.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electron. cash system," 2009. [Online] Available: bitcoin.org

[2] M. Alexa, "Bitcoin can't be ignored, blockchain needs to encouraged: SEBI," *INC42* [Online] Available: inc42.com/buzz/bitcoin-sebi-cryptocurrencies. Accessed on: Dec 21, 2017.

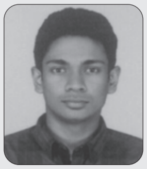
[3] S. Kumar, "Future of Cryptocurrencies," *Manorama.* Accessed on: Feb 9, 10, 11, 2018.

[4] B. E. Savjee, "*How does a blockchain work,"* [Online] Available: www.savjee.be. Accessed on : Nov 13, 2017.

[5] J. Redman, *"Difference between electron. fiat and cryptocurrency,"* [Online] Available: news.bitcoin.com/big-difference-electron.-fiat-cryptocurrency. Accessed on: April 27, 2017.

About the Authors

Prerna Talreja is a student of St. Joseph's College (Autonomous),Bengaluru, India. She has in-depth experience in stocks and share markets. She has completed her basics of investment management and is currently perusing NSE's Course in Advanced investment management. She specialises in finance and banking activities. She is skilled in many avenues of commerce and business. She is a strong business professional with a Bachelor's Degree in Finance/Commerce.



Darshan Tom is a student of St. Joseph's College (Autonomous), Bengaluru, India. He is an experienced Web Developer and Search Engine Optimisation specialist with a demonstrated history of working in the internet industry. He is also working for a Bengaluru based startup as a web developer and technical advisor. He is also a financial advisor, especially for investments in crypto currencies. He is skilled in multiple programming languages and in Blockchain technology. He is a strong marketing professional with a Bachelor's Degree in Finance/Commerce.

Celestin Anto is a student of St. Joseph's college (autonomous), Bangalore, India. He is a self motivated finance professional with a bachelor's degree in commerce. He is an experienced individual in the field of finance backed up with good knowledge and experience (intern) from a reputed accounting and audit firm. His knowledge and experience in financial markets made him a good observer of the stock markets.