IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

Crypto Currency a Tale of Innovation, Scam and Uncertainty

Nicholes Charles[1], Resmi K R[2]
Student, Computer Science Department, Santhigiri College, Kerala, India[1]
Assistant Professor, Computer Science Department, Santhigiri College, Kerala, India[2]

Abstract: *Blockchain and cryptocurrency are two terms that go parallelly. we are hearing it in our daily life. Cryptocurrencies also known as cryptos are game changers of our lives. Unlike money that is issued and regulated by the government crypto isn't controlled by any government or any persons. This is accomplished by the use of blockchain that makes the topic more curious. This work explains about the impact of the cryptocurrencies in the world. This paper says more about the non-technological aspects of cryptocurrencies that includes how it came into existence, why it used now, how it is seen by the world.*

Keywords: Cryptocurrency, Blockchain, Bitcoin, Volatile, Miners, Incentives, Bitcoin Mining, etc.

I. INTRODUCTION

The word cryptocurrency has been a talking point for several years. What makes it such a interesting topic. Is it because of the concern of the next financial crisis that can be caused by them or because it's a gold nugget for investors? What makes cryptocurrency also known as cryptos skeptical and curious at the same time. It all starts in 2008 when the popular investment bank lehman brothers filed for bankruptcy [1][2][3]. That bank was a financial giant that it's bankruptcy crumbled world economy and started 2008 financial crisis. And then came a person in the pseudonym "satoshinakamoto" with something known as bitcoin that later became history[4].
His idea and intention were to create an online transactional medium that can circumvent banks as the 3rd parties during online transactions. Making transactions directly between sender and receiver. Though the motive of the inventor of crypto was an innovation it grew beyond that. Because of the special characteristics of bitcoin and other descendants like pseudo-anonymity, decentralization, blockchain all inspired many including the mafia,hackers,money launders to use cryptocurrency. And the uncertainty of cryptocurrency as a digital asset all made it an ordeal for the government to surveil about. Since the creation of bitcoin, the first cryptocurrency it has gone through many changes. Cryptocurrencies have a long story to tell about innovations and controversies.

II. BEGINNING OF CRYPTOCURRENCIES

Technology is a game changer for humansit changes everything related to us. And such a thing that was never even imagined to rival or change was money. Because money is always linked with government but in this system crypto is unregulated. It has transformed from replacing banks during online transactions to a digital currency of binary code. Blockchain is a technology in which manipulation or hacking is almost impossible. Because it's a digital ledger that uses a network of computers to store each transaction. These transactions are verified by miners.
The core concept of cryptocurrency was proposed by a Chinese engineer called weidai. He published his essay on anonymous electronic cash system, but this wasn't executed in the real life. But His work was noticed by the founder of bitcoin Satoshi Nakamoto. And he adopted the concepts of weidai that include[5][6].

- Proof of work- In this process the prover has to show that he has done certain amount of work and it will be examined by the verifiers.
- The verified work has to be updated in the ledger.
- The worker has to be paid for what he has done.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

- Exchange funds should be authenticated using cryptographic hashes and complete through collective book keeping.

III. BITCOIN: A PEER ELECTRONIC CASH SYSTEM

On October 31,2008 the creator bitcoin Satoshi Nakamoto published a whitepaper explaining how bitcoin will work after its creation. Studying about that whitepaper is essential to understand the working mechanism of cryptocurrency. The white paper issued by Satoshi nakmoto consists 12 parts from abstract to conclusion. Each part of that paper is briefly explained in this topic. The whitepaper issued by Satoshi nakmoto is the part and parcel of the cryptocurrency. It begins with an abstract.

This abstract talks about bitcoin as a peer-to-peer electronic cash system that directly transfers money without relying on any third parties like bank or pay pal or anything else. It also provides a solution for double spending through proof-of-work.The conventional online transactional ways like bank all work in a model known as trust based model. This model is highly vulnerable to manipulation. This weakness Inherited by the companies working on trust-based model can be addressed by using electronic cash system using cryptographic proof. Bitcoin uses computationally impractical reversible transactional mode and also has a escrow to protect buyers. For the ease of understanding the core concepts of the Satoshi Nakamoto's whitepaper it is explained below.

a) Transactions

Double spending is a challenge that should be eliminated. For this purpose, Satoshi Nakamoto proposed something called "a chain of digital signatures ". In this process the current owner of a bitcoin before transferring a coin should sign in the hash of the previous owners and also next owners' public key.

Consider this example. You received an envelope of 100 dollars. It will contain the address and sign of the previous owner. And if you want to send this money to a friend of yours then you also have to write your address and put your signature on a envelope and send it to him. The next problem is double spending. how can bitcoin prevent double spending? In order to protect payee from double spent coin, a trusted central authority should be created or a mint. So how does mint work. Mint checks each transaction. And after each transactions the coin returns to mint and it is like a new coin. This coin isn't double spent coin. But the main disadvantages of this system is the dependency on the mint and also in the company which runs mint.

b) Timestamp Server

Timestamps are "proofs-of-existence". They can confirm whether data exist or not. Timestamp works by publishing the timestamped block publicly.

c) Proof of Work

Proof of work is used by the decentralized networks like bitcoin to verify the accuracy of new transactions. Because of the nature of decentralized networksProof-of work is used to ensure the credibility.

Proof-of-work is a consensus mechanism that determines who among the miners are allowed to verify new data.it is done by complex mathematical puzzle. The first to solve this will have the chance to create a new block to the blockchain. Winners are paid only after their work is verified and approved by other miners.

The mechanism of proof-of work is given below

- The data of each transaction in bitcoin is pooled into a block
- Blockchain works as a chain of blocks so the person to create the next block is determined by using a complex mathematical puzzle. The miner who solves this puzzle will be assigned to create next block and he will be paid for his work making this a lucrative process.
- The person has to show the proof of this computational work solving
- Other miners verify the data and hence made it into the blockchain. In a sense blockchain is an incorruptible that achieves this integrity through public collaboration.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

d) Network

Network of the bitcoin works like this**.** There exist a group of nodes and each new transactions will be sent to all nodes at the same time.

- Each node starts to solve the complex mathematical puzzle. That determines whom to create the new block.
- The node to find the proof-of-work will broadcast it to other nodes.
- The block will only be accepted if it's not double spent it is done on the basis of its hash, hash of previous block

e) Incentive

Incentive is the reward for their work. Each node is motivated to remain loyal and finish their work through the incentives that is paid through bitcoin. Mining is really expensive and complex. The incentives of the mining include transactional fee and a newly minted bitcoin too.

f) Reclaiming the Disk Space

In order to never run out of storage completed transactions will not be stored in ablock. Instead of that merkle roots are stored in the block's hash. Merkle root is also known as fingerprint of all transactions.

g) Simplified Payment Verification

This is a procedure to help lightweight clients to check if a transaction is on the blockchain without downloading the whole blockchain.

h) Combining and Splitting the Value

This part of the bitcoin whitepaper talks about the convenience of splitting and combining bitcoins at our will. For instance, you can combine 4 one dollars of bitcoin to a single 4 dollars' worth bitcoin. And you can also split your bitcoin like this. The smallest unit of bitcoin isn't 1 bitcoin it is 0.00000001 btc and is known as 1 satoshi.

i) Privacy

This part exposes the biggest myth of bitcoin that is its anonymity. Actually, bitcoin transactions are public that anyone on the network can see it but the users are pseudonymous. Anonymity is kept through keeping the public key anonymous no personal information is linked to the account.The whitepaper written by Satoshi Nakamoto ends with a conclusion that includes these core features.

- Double spending isn't possible through bitcoin
- 3rd parties don't exist in this system
- New coins are released during proof-of-work.

IV. WORLDS APPROACH TO THE CRYPTOCURRENCY

a) Cryptomania

The potential of cryptocurrency as a digital asset is unignorable. Just like a coin having two sides cryptocurrency has both pros and cons as well. Being a volatile thing cryptos can sometimes provide high return and sometimes it can burn out the money. But the credibility it provides because of the blockchain is really innovative and futuristic. Seeing this potential, the corporate world and Venezuelan government as well is trying to embrace the opportunity provided by the cryptos.

In order to harvest the coming opportunity of cryptocurrency venezuelan government launched its own official crypto known as 'PETRO'.This crypto currency is backed with the country's oil and mineral reserves.As said before cryptocurrency is considered as a gold-nugget for investment. And it includes even ElonMusk. He had made investments in the cryptocurrencies like bitcoin and dogecoin resulting in the price increasing of these cryptos. And tesla motors the pioneers of electric vehicle industry once used to accept payments in bitcoin. At

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

the end of the year 2021 tesla motors was holding bitcoins worth around 2 billion us dollar. Tesla isn't the only company to accept payments in bitcoin it also includes tech giants like Apple, Amazon and many more as pf 2022. Seeing this growth of cryptocurrencies particularly bitcoin Meta formerly known as Facebook planned to start its own cryptocurrency known as diem(formerly libra). But this ambitious project was abandoned by Facebook in January 2022.

b) Cryptophobia

Though corporates and few governments like Venezuela support crypto directly or indirectly the majority of governments are skeptical about cryptocurrency. Scared of the crypto bubble many countries have banned cryptos. And famous economist and former RBI governor also warned about the risks of cryptocurrencies. And the business tycoon jack ma who made his immense fortune from technology also warned about cryptocurrency risks and also praised about the possibilities of blockchain on which crypto is working.

V. ONE COIN THE HISTORICAL FINANCIAL SCAM

Cryptocurrencies like bitcoin and others are volatile means their price can skyrocket at any time and collapse at any time. Despite of all these risks many people consider missing the bitcoin opportunity as one of the worst mistakes of their life. Seeing this opportunity of fraudulence based on cryptocurrency a new cryptocurrency known as onecoin was created by a women called Dr rujaignatova [7]. Onecoin is considered to be one of the largest financial scams in the history. she had previous criminal records and was given a suspended sentence by the court for her and her father's connection with the buyout of a firm that was bankrupted dubiously. The company followed multi-level marketing scheme based on the educational courses it sold.

Onecoin claimed these courses were the main source of income for the company. The buyers of these courses got onecoin tokens that was used to mine onecoin cryptocurrency[8]. Unlike the other cryptocurrenciesonecoin wasn't traded on any exchange and it had its own exchange known as onecoin exchange to meet this need. Onecoin that claimed to be the bitcoin killer ended up shutting down without any notice in January 2017. It stole billions of dollars from the investors around the world.The estimated stolen money is 4 billion us dollar by the American government. Whereas other sources say it had stolen more than 19.4 billion us dollars. Since then, the self-proclaimed queen went missing leaving the investors empty handed.

VI. ILLICIT ACTIVITIES BASED ON CRYPTOCURRENCY

a) Cryptos for Child Exploitation Videos

Virtual currencies are increasingly used as payment for child exploitation videos. The factor that attracts these perpetrators is the belief that cryptocurrency transactions are untraceable. For instance "welcome to video" was a website hosted in the dark net to sell videos mainly child exploitation videos[9]. This website was a paid website that accepted cash only as bitcoins. This is not a rare incident where illegal websites for pornography uses bitcoin. The government officials fail at bringing these perpetrators to the light because of several reasons. And these law breakers keep victimizing the children.

There was an incident in 2017 when law enforcement officials from Central America uncovered a website using for selling child exploiting videos. This website had data of many bitcoin transactions that could have been used to find law breakers but accidentally the whole data was lost leaving those criminals untouched.

b) Silk Road the Amazon of Drugs

Silkroad was the first digital black marketplace. It was infamous for selling illegal drugs and fake driving licenses. The seller's account was limited and through auction new sellers can buy an account. A fixed fee was charged for each transaction. This was a tor hidden service that took all precautions to remain anonymous. In 2013 silk road was shut down by FBI by then it was serving 1,00,000 users and was selling 10,000 products where 70% was drugs. It had a review system to find out legitimate sellers and to takedown fraudulent sellers[10]. It used bitcoin as a payment option and DEA(drug enforcement administration) seized bitcoins that

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

was worth millions at that time. And in 2020 US government seized bitcoins that is worth approximately 1 billion US dollars that was connected to these accounts[11].

d) Ransomware Attacks

Cryptocurrencies are increasingly becoming popular among the hackers as a mode of payment during ransom ware attack[12][13]. As per the fbi report in 2017 around 58.3 million usd was stolen by hackers. Another reason why they choose crypto is because of the anonymous or pseudonymous feature of crypto and less transactional fee charged by bitcoin.

c) Money Laundering

It said that the amount of money laundered is between 500 billion usd to 1 trillion usd. Theses perpetrators can use cryptocurrency for money laundering[14][15]. These money that may be originated from drug deals or through any other illicit activities are invested in crypto. Then the next step of "layering" starts in this system technologies like mixers which are made for this purpose is used. After mixing this cryptocurrency the next process known as integration starts means adding them to the bank accounts. But investing huge amount without proper documents will be noticed by the government so other ways are used to credit the money on their or related accounts.

VII. CONCLUSION

Cryptocurrency is something that many government and famous economists warn about. And seeing the dark side of cryptocurrency for draining the money of investors many governments was forced to prohibit cryptocurrencies. But this is really mesmerizing thing for risk takers. Many countries in the world still haven't banned crypto providing a chance for them to be involved in this. Users have to be always vigilant about dos and don'ts of crypto world. Our approach and our understanding determine the rest of the things. But cryptocurrency has opened up a new door of opportunity. Like the volatility of the cryptocurrency no one can predict whether cryptocurrencies can remain forever.

REFERENCES

[1] https://fortune.com/2019/11/06/is-onecoin-the-biggest-financial-fraud-in-history/
[2] https://www.bbc.com/news/technology-58678907
[3] https://news.bloomberglaw.com/banking-law/bitcoin-on-the-brink-of-fresh-2020-high-following-paypal-embrace.
[4] https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020.
[5] http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm
[6] https://www.bloomberg.com/opinion/articles/2017-11-07/are-cryptocurrencies-an-asset-class-yes-and-no
[7] https://doi.org/10.1007/s10611-017-9756-5
[8] https://www.mirror.co.uk/news/uk-news/heartbroken-man-took-life-after-26260173
[9] https://www.theguardian.com/technology/2013/dec/04/bitcoin-bubble-tulip-dutch-banker
[10] https://www.dw.com/en/why-is-the-indian-government-cracking-down-on-cryptocurrency/a-60148889
[11] https://thediplomat.com/2021/07/south-korea-tightens-regulations-on-cryptocurrencies/
[12] https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf
[13] https://link.springer.com/article/10.1007/s12599-021-00686-z
[14] https://fortune.com/2021/01/07/bitcoin-price-today-soars-ether-cryptocurrency-marketcap/
[15] https://marketexclusive.com/bitcoin-major-currencies-today-crypto-currency-daily-roundup-june-25/2018/06/
[16] https://finance.yahoo.com/news/chinese-bitcoin-trader-commits-suicide-121816354.html

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

BIOGRAPHY

Nicholes Charles is a Computer Science undergraduate student at SanthigiriCollege Computer CciencesKerala.

Resmi K R,received PhD degree in Computer Science from Mahatma Gandhi university Kerala,India in 2021.She is currently working as Asst. Professor, Computer Science, Santhigiri College of Computer Sciences, Thodupuzha, India. Her research interests include biometric, pattern recognition, image processing and computer vision.