International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

THE HISTORY AND TECHNOLOGY BEHIND THE ADVENT OF CRYPTOCURRENCIES: STRATEGIES FOLLOWED BY VARIOUS GOVERNMENTS IN CONTROLLING THE UNREGULATED CURRENCY

Aaryan Krishan Mehra

Apeejay School Noida

DOI: 10.46609/IJSSER.2022.v07i10.030 URL: https://doi.org/10.46609/IJSSER.2022.v07i10.030

Received: 29 October 2022 / Accepted: 3 November 2022 / Published: 5 November 2022

ABSTRACT

The paper discusses the advent of cryptocurrencies and the blockchain technology behind its invention. The fact that the currency is an unregulated one has led to most of the governments of the world to shun its existence. But, in recent years with the increasing popularity of the currency, for various reasons have led to a rethink of the way in which to handle its growing importance. At present, the methods adopted by most governments is to introduce their own digital technology. They have acknowledged its presence by imposing capital gain tax and other taxes on its usage. As this is a hit and trial method, no concrete solution has been discovered to counter the negative impact of this unregulated currency.

Research Question: The paper will attempt to study the growing impact of cryptocurrency as an alternative to the currency backed by the central government of a country. The technology behind it has grown in importance and is being used in other spheres as well. The sudden surge of the currency as an alternative to a regulated one has increased in recent years. An analysis will be attempted on the security issues, that the adoption of this currency might entail.

1. Introduction

Cryptocurrency has in recent times become the 'mantra' of the day. The popular use ofthis word in every newspaper, news channel, financial discussion has led to increasing amount of research in this regard. The question that arises is the security issue,

- Firstly, in the development of this type of currency.
- In adoption of it as an alternative or as a parallel currency to the one that prevails as legal

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

tender and that which is backed by the central bank in the economies of the world today.

- The security aspects involved in its adoption.

Cryptocurrencies are of different types, just like the different currencies that are prevalent in the world today. The earliest amongst them was Bitcoin, subsequently there are a large number of them, some of them are Ethereum, Litecoin, Ethereum Classic, Peercoin, Stellar, Dash ,etc.

Figure 1: Images of Different cryptocurrencies

Source: Google image

2. Origins of Cryptocurrency

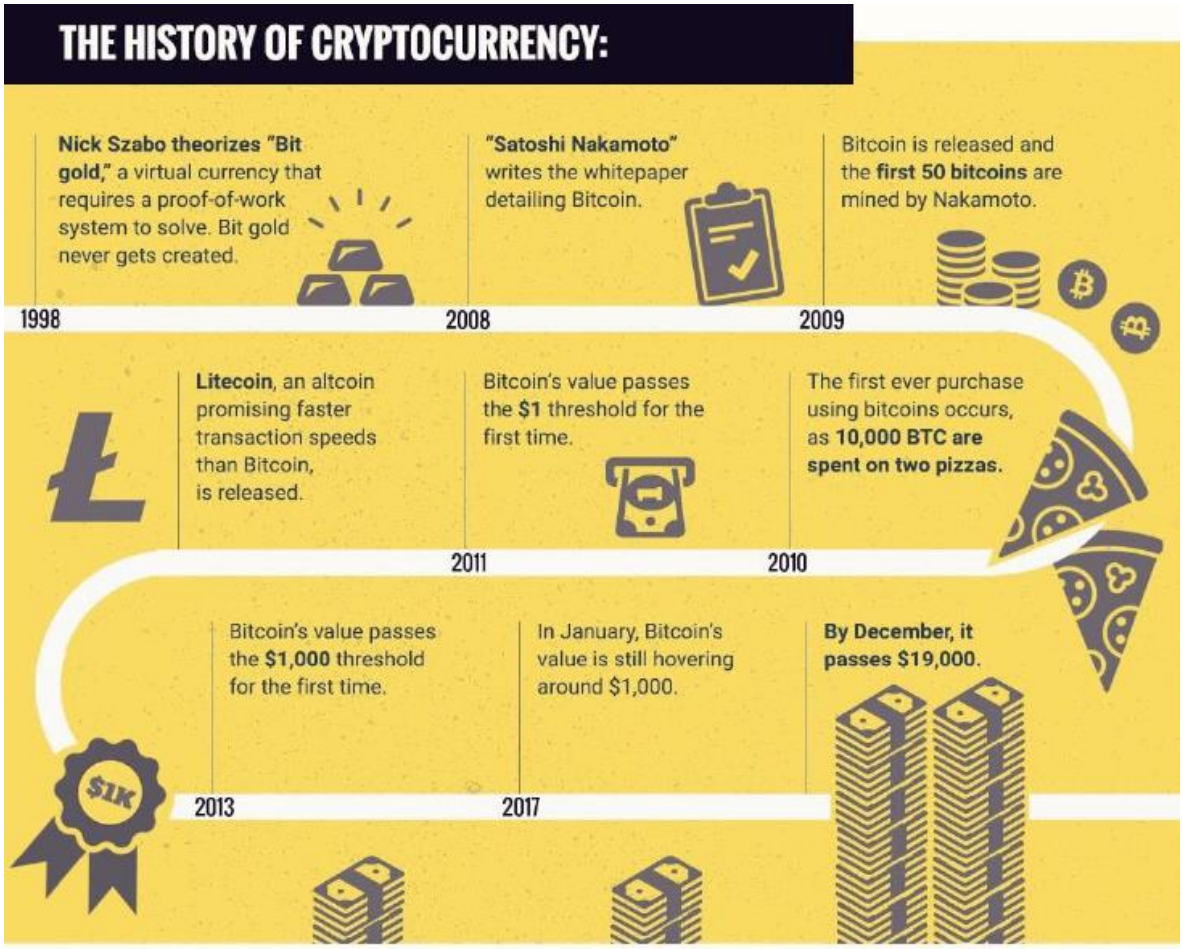
Cryptocurrency was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto. It started being used in the year 2009 when it was released under an open source software. Most people believe that Satoshi Nakamoto is a pseudonymous developer and the name that has been claimed may also be a pseudonym. The currency used what is known as an SHA-256, also known as a cryptographic hash function. The name Cryptocurrency indicates that encryptions are used to verify transactions. Indicating, an advanced coding which is involved in storing and transmitting cryptocurrency data between wallets and public ledgers. The

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

primary aim is to provide security.

Figure 2: The History of Cryptocurrency



Source: Crypteligence.com

3. Working of Cryptocurrency

Cryptocurrency or crypto is a form of currency that exists digitally or virtually. It does not have a centrally issuing or regulatory authority like a central bank and uses in fact a decentralized system to record transactions and issue new units. The banks, as we know them in the world today, do not verify the transactions. It essentially is a peer to peer system. It enables any one to send and receive payments anywhere. No physical money is carried around or exchanged as this system exists purely as digital entries in an online database, which in turn describes specific transactions. Thus, Cryptocurrencies are stored in digital wallets.

ISSN: 2455-8834

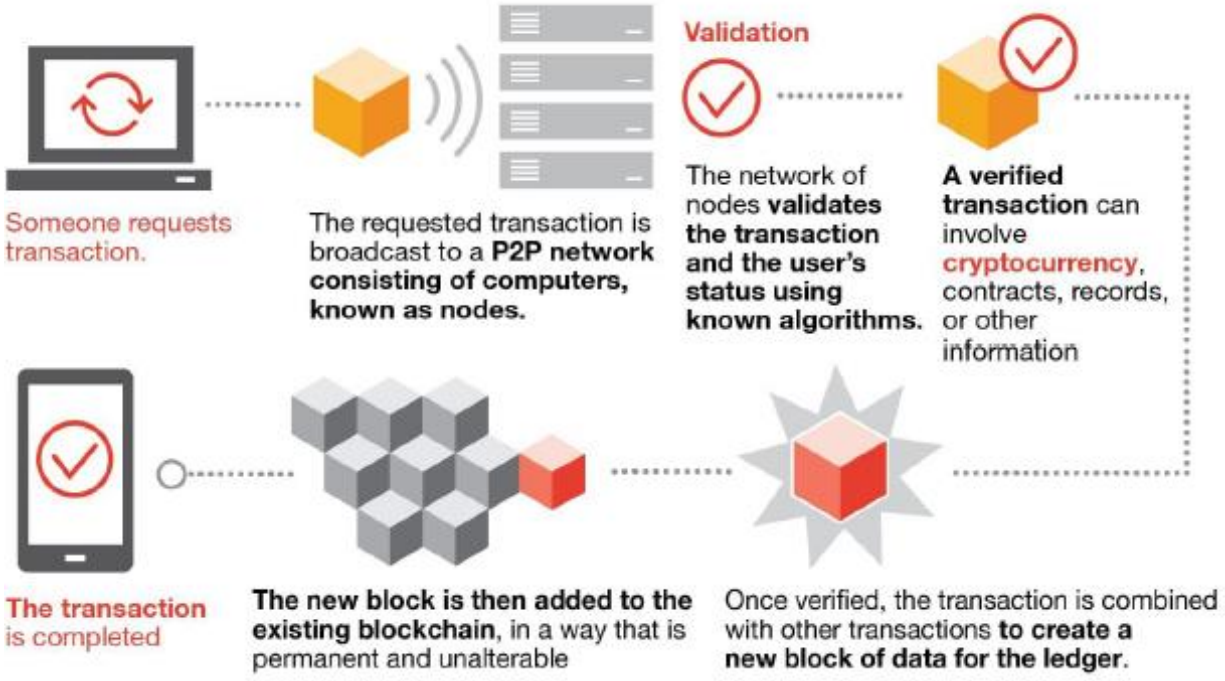
Volume:07, Issue:10 "October 2022"

The whole system runs on a public ledger known as 'Blockchain'. Units of Cryptocurrency are created through a process of mining. Users can also buy Cryptocurrency from brokers. Owners of Cryptocurrency do not own anything tangible, all they own is a key.

3.1 Blockchain in Cryptocurrency

Blockchain is an interlinked systematic chain of blocks that contains transaction history and other user data. It works on the principle of decentralization.

Image 3: Use of Blockchain technology in Cryptocurrency



Source: Pwc.com

The figure above indicates the manner in which Blockchain as a technology is used for various popular Cryptocurrencies like Bitcoin and Ethereum. To understand how it works it is important to secure record and transfer information which is easily done by the use of this technology.

Blockchain is a distributed digital ledger technology which allows records to be kept across multiple computers. Blockchain has been developed as a system which is so foolproof that the information that is recorded in it cannot be changed or hacked.

3.2 Detailed functioning of a Blockchain technology

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

- The first step in a Blockchain is transaction data.
- The second step is chaining the blocks with a hash.
- The third step is the manner in which the signature (hash) is created.
- The fourth step involves answering the question as when does the signature become essential and who signs a block.
- The fifth step is how and what makes the Blockchain so sacrosanct that it cannot be replicated.
- The sixth question is what or who is responsible for governing the Blockchain.

To answer all these questions, we need to understand that Blockchain is a digital concept which is used for the storage of data. These blocks are chained together and once they are chained the data cannot be changed which means that things like property rights, identity, money balance, medical records, insurance, any original document cannot be tampered with nor changed once it is put under the form of Blockchain technology. No information from these Blockchains can be changed. If you have to add data which may be a transaction that has occurred, then it would come in another block. So, Document 1 is written in a block. Once this is done the first block shuts and cannot be changed. If there is a further transaction which has to occur which is related to the first block, then this information is put in the second block. Even if one wants to change a single digit, the block will get a new signature which occurs through hashing. Block one is linked to block two by adding the signature of block 1 to the data of block 2. It is the signatures that link the blocks to each other which makes them a chain of blocks.

The blocks on a Blockchain are available to anyone. Altering a single block means that a new signature is required for every block that comes after it till the end of the chain. This seems very difficult as one would have to understand how the signatures have been created.

3.3 Definition of Nodes

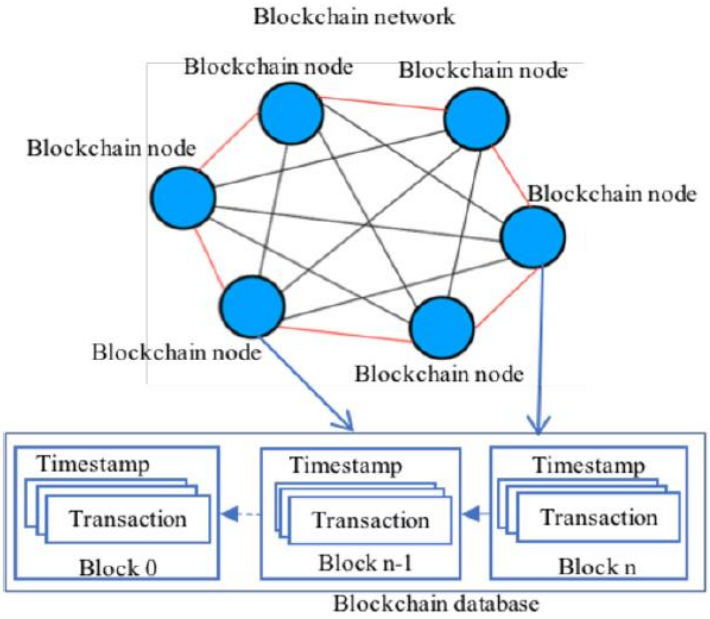
Nodes and master nodes are very commonly used terms in Blockchain technology. Nodes are a critical component. Without nodes a Blockchain's data is not accessible. At times people call nodes the Blockchain. The Blockchain exists out of blocks of data, and it is these blocks of data that are stored on nodes. Nodes then can be any kind of device which could take the form of computers, laptops or even bigger servers. The nodes on a Blockchain are connected to each other and they are constantly exchanging the latest Blockchain data with each other. Thus, the nodes are always up to date on data. They in fact store, spread and preserve the Blockchain data.

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

A full node is one which contains a full copy of the transaction history of the Blockchain.

Figure 4: Blockchain Network



Source: ResearchGate

Nodes can be offline or online. In case of online nodes, they receive, save and broadcast all the latest blocks of transaction, while an offline node does not. When an offline node comes online, it is required to catch up with the rest of the Blockchain by downloading all blocks that were added to the Blockchain ever since the node went offline. This is often referred to as synchronization with the Blockchain. It is possible for a Blockchain to run on a single node, but this would be vulnerable to power issues, hackers and systemic crashes. If the Blockchain runs on a larger number of full nodes, then the greater the resilience against such major problems.

When the Blockchain is spread over a number of devices, it is not possible for any one entity to corrupt all the devices and wipe out all the data. Supposing all nodes go offline, it takes only one node which has the Blockchain history to come online and make the data accessible again. These nodes are being run on a regular basis by crypto and Blockchain enthusiasts.

Master nodes on the other hand are firstly online 24/7 and besides validating, saving and broadcasting they also govern voting events. They can execute protocol operations and also enforce the law. In effect the master node is a huge server on the network. The master node requires more energy, maintenance, and storage. For running the master node which is powerful, it requires the host to deposit a minimum amount of crypto as collateral and the minimum

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

amount is huge.

4. Emergence of cryptocurrency

Bitcoin was the first cryptocurrency in 2009 and it still remains the most popular and valuable till date. This is a decentralized currency which means that it does not come under the jurisdiction of a central bank of the country. It is powered by the number of users, and they are not dependent on any central authority. In fact, bitcoin could be considered an alternative to the US dollar. The US dollar is controlled by the government and the central bank. The national currency of all countries are always controlled by both the government as well as the central bank.

Cryptocurrency on the other hand does not come under the purview of neither the government nor the central bank. The year that bitcoin started was a tumultuous one for the United States of America as it was entering the recession period, and there seemed to be a distrust of banks and the central government. It took time for one to understand the financial value of this currency and today it can be considered as one of the fastest growing asset class. The increasing popularity of bitcoin is basically due to its property of decentralization and encryption, has resulted in alternative currencies to bitcoin example: Namecoin, Litecoin etc which normally offer greatest speed as additional advantage to the original. Presently there may be over thousand cryptocurrencies in circulation. Amongst the most popular is Ethereum this was marked by the emergence of Initial Coin Offerings (ICOs) as an alternative to Initial Public Offering (IPOs).

5. Issues in its universal adoption

There are certain unresolved issues that prevent the universal adoption of cryptocurrencies. Though the cryptocurrencies are based on a near foolproof system of 'Blockchain technology' and it is one of the prime application of this technology in finance. There are a few shortcomings which can have disastrous consequences. These shortcomings may actually be related to the technology itself or even the process of adopting it for daily use. The main reasons are listed below:

1. The possibility of a 51% Cyber Attack:
A 51% Cyber Attack means that a single user is in a position to manipulate the data and transactions taking place through a Blockchain network. This is possible if the user manages to garner more computational resources than the other users in the network. Heuses this to prevent others from a) viewing data, b) changing verification of the transaction, c) changing approval criteria of the transaction, and d) changing any other information present in the Blockchain.

There are not many solutions that can prevent these attacks. Once the system is compromised and the perpetuator has full control then there is no way of reducing thelosses that are likely to

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

arise due to this monopoly.

2. All transactions require buyers and sellers for it to become a universally accepted currency and for the development of a sophisticated infrastructure. Cryptocurrencies has a distinct lack of merchants who accept this as a currency, main reasons being a) lack of data security, b) lack of knowledge, c) there are chances that existing users would rather keep their stock of cryptocurrencies rather than spend it as their market value may increase phenomenally.

3. In recent years there were certain online platforms where trading of cryptocurrencies like Bitcoin and Ethereum were possible, which have stopped in recent years due to safety issues.

4. Scalability issues:
Currencies cannot be increased progressively to conduct several thousand transactions ata given point in time. Due to this they are exorbitantly priced. Scalability refers to how a system can handle an increasing number of transactions. The main problem with Blockchain as regards to this is that all participants have to agree on the validity of transactions. This could arise from application code, hardware resources and database limitations. The reason that we need to increase scalability is to increase the transaction speed without sacrificing decentralization or security.

Figure 5: Cryptocurrency issues

Source: Allerin

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

Besides the issues that have been raised above, the most important is the breach in data security. This is a reality as far as cryptocurrencies are concerned. The reason being the presence of complexity and contradiction in their usage prevents the use of these currencies as a daily occurrence. The understanding of concepts like private and public keys, hot and cold user wallets and other such terms have to be properly researched and learnt before one starts trading in the currency.

6. Measures taken by governments to safeguard their economies against the negative impact of Cryptocurrency

A number of governments around the world have tried to safeguard their economy from the adverse impact of cryptocurrencies with regard to it not being under centralized control. Some of the governments have completely banned the use of these types of currencies in their economies, other have instituted capital control to prevent outflow of a currency as exports could debase its value. Other governments have exercised control in the form of both fiscal and economic policy.

There have been new regulations that have been instituted as and when adverse impacts of the use of such currency are discovered. Regulations are in place to:

- protect long term investors
- prevent fraudulent activity within the crypto ecosystem
- provide clear guidance to allow companies to innovate in the crypto economy.

The government are wary of unregulated crypto markets as they may become conduits for money laundering, fraud and terror financing. There have been a number of cases where frauds due to the use of cryptocurrency are being investigated, financial frauds and terror financing. The governments all over the world are extremely wary of the popularity of cryptocurrency but they also realize that there is a large section of the public which is dealing/dabbling/speculating in this unregulated monetary asset. Some governments have tried to accept this currency in certain spheres. For example: in India the government has banned the use but does recognize that it is being used and thus to be in a position to earn revenue on it, it announced in the budget of 2022 a flat 30% tax on gains from cryptocurrency transactions as well as TDS of 1%. But, taxing it does not make it legal. China has completely banned cryptocurrency as it fears economic instability. USA has banned it but realizes that consumers are flocking towards this currency and looking for a more decentralized era. Thus, they are using various ways to keep the importance of their legalized currency intact.

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

Conclusion

In spite of the problems of cryptocurrencies, there has been an increasing amount of people who have decided to dabble in it. The larger the number of people that are dealing in it has led to its growing popularity. Most governments have realized this new trend. To avoid the declining importance of the regulated currency some governments like the US and India have moved towards setting up a regulated digitalized currency. This they feel is the only way that they can compete with the unregulated cryptocurrency. The basis on which the currency has developed i.e. the Blockchain technology has been extensively used in fields like finance, insurance, the reality sector to name a few.

Thus though one is wary about cryptocurrency, the increased popularity has made most governments to look for alternatives.

Bibliography

1) Alaa, A. (2022). Bitcoin:Bitcoin standard in 2022: the way to mastering bitcoin.

2) Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps (1st ed.). Apress.

3) Freeman. (2022). The Only Cryptocurrency Investing Book You'll Ever Need: An Absolute Beginner's Guide to the Biggest "Millionaire Maker" Asset of 2022 and Beyond- Including How to Make Money from NFTs. Independently published.

4) Lewis, A. (2021). The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT). Mango.

5) Lipton, A., & Treccani, A. (2021). Blockchain And Distributed Ledgers: Mathematics, Technology, And Economics. WSPC.

6) McVeigh, S. (2022). The Blockchain Bubble or Revolution: We've been doing it your way long enough.

7) Raghavan, T. C. A. S. (2020). From Cowrie to Crypto: Blockchain and the Future of Money. Westland Publications Private Limited.

8) Shin, L. (2022). The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze. PublicAffairs.

9) Trend, R. (2021). Blockchain and Cryptocurrency: 2 Books in 1: Blockchain Basics &

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

Cryptocurrency for Beginners. The Complete Guide for Beginners to Understand Blockchain Technology and Start Cryptocurrency Investing. Independently published.

10) Vigna, P., & Casey, M. J. (2019). The Truth Machine: The Blockchain and the Future of Everything (Reprint). Picador.

