J. Adv. Res. in Cloud Computing,Virtualization and Web Applications
Volume 3, Issue 2 - 2020, Pg. No. 1-5
Peer Reviewed Journal

Article

A Brief Review on Cryptocurrency in a Nutshell

Harshit Vijayvergiya[1], Alisha Goyal[2], Ankita Joshi[3]

[1]Student, [2,3]Professor, Department of Computer Science and Engineering, Global Institute of Technology, Jaipur, Rajasthan, India.

I N F O

Corresponding Author:
Harshit Vijayvergiya, Department of Computer Science and Engineering, Global Institute of Technology, Jaipur, Rajasthan, India.
E-mail Id:
16egjcs074@gitjaipur.com
How to cite this article:
Vijayvergiya H, Goyal A, Joshi A. A Brief Review on Cryptocurrency in a Nutshell. *J Adv Res Cloud Comp Virtu Web Appl* 2020; 3(2): 1-5.

Date of Submission: 2020-10-21
Date of Acceptance: 2020-11-07

A B S T R A C T

Cryptocurrency is particular kind of the virtual currency which relies on the principles of cryptography and transmission. Dozens of Cryptocurrencies were emerged within the past few years, while the foremost popular is that the first ever introduced i.e. Bitcoin. Cryptocurrencies attracted plenty of attention in recent years. during this paper, basics of cryptocurrencies are briefly introduced. There are some technologies which is that the backend process of Cryptocurrencies and their transactions. Blockchain is one in all the trending technology which is employed in cryptocurrency. These are legally considered property; cryptocurrencies generally don't seem to be considered monetary system like government or financial institution issued paper currency denominated banknotes and coins. because it is thought that there are several rules and regulations regarding cryptocurrencies. These don't seem to be legal in several countries. there's a quick discussion regarding rules and regulations in India, during this paper.

Keywords: Cryptocurrency, Virtual Currency, Bitcoin, Blockchain

Introduction

How well can a virtual currency function a technique of payment? Since the creation of Bitcoin in 2009, many critics have denounced cryptocurrencies as fraud or outright bubbles which could burst. More nuanced beliefs have argued that these kinds of currencies are only there to support payments for illegal or criminal activities or just waste of resources. However, cryptographic principles supported to make sure security these new currencies can support payments without the need to designate a third-party that operates the currency or payment instrument possibly for its own profit. This emerging technology can go far if it gets legal all told countries. Worldwide acceptance may increase its usability. But every technology has its own disadvantages. All cryptocurrency payments between anonymous sides are hardly traceable. This fact is that the main reason of their usage in criminal operations. Very hard transactions traceability and no central guaranty of the currency are main reasons of criticism and legislation restriction of cryptocurrencies. Governments and security authorities also are fearful of virtually untraceable transactions that may be connected with financing criminal activities or terrorist organizations. Blockchain network is that the biggest element of the cryptocurrency. Once a transaction is completed cannot be undone because blockchain is unidirectional. The chain of transactions is saved in blocks. These transactions are made public on the ledger but it never shows the name of the individual a novel secret is also provided which may be a sequence of characters. The person holding the private secret is the owner of that currency. The cryptocurrency has not any centralised server, it's decentralised. It also follows the concept of peer to see transaction. The emergence of Bitcoin has sparked debate about its future and same is also for the other cryptocurrencies. Despite Bitcoin's recent issues, its success since its launch in year 2009 is inspiring the creation of different cryptocurrencies like Litecoin,

Etherium and MintChip. The cryptocurrency that likely to become a part of the mainstream national economy would need to satisfy divergent criteria. That possibility is looking remote, there's little doubt that Bitcoin's success or failure in coping with all the challenges. It faces may determine fortunes of other cryptocurrencies within the upcoming years. Not only bitcoin, but there are also several cryptocurrencies like etherium, ripple, litcoin, monero, bitcoin cash etc. People invest their money in cryptocurrency to earn profit. Since within the cryptocurrency isn't backed by the govt this can be not completely secure. There are several risks associated like scam, fraud. Volatile nature of cryptocurrency makes it unreliable.

Working of Cryptocurrency

How it Works?

Exchange is sent shared utilizing a few virtual products that is classified "digital money wallets." The individual making the exchange utilizes the specific wallet to move adjusts starting with one record then onto the next. To move reserves, information on a secret key or a private key is required which is related with the record. Exchanges made distributed are encoded and afterward it communicated to the digital money's organization. These exchanges are then lined up to be added to the public record. Exchanges are recorded on the public record through a cycle called "mining". All clients of a given digital money approach the record on the off chance that they need to get to it, for instance by downloading and running the product which is known as a "full hub" wallet. The exchange sums will be public, yet who sent the exchange is encoded. Every exchange drives back to an interesting arrangement of keys. The arrangement of keys are possessed by the individual who claims he measure of digital money related with those keys. Numerous exchanges added to record without a moment's delay. These "blocks" of exchange is added successively by diggers. That is the reason the record and the innovation behind it are designated "blockchain." It is the "chain" of "blocks" of exchanges.

Technology Behind

The biggest element of how digital currencies work is their blockchain networks. However, when we talk about the blockchain a specific currency, we're referring to a singular implementation of Blockchain protocol. That implementation is what create digital currency.

In simple terms, the Blockchain allows digital currency to be created and used as viable form of the money. This is because it provides framework for creating digital items that are: (i) Unique and non-duplicable (ii) Non -repudiable and impossible to "double spend" (iii) Scarce and limited in supply (iv) Durable and immutable (v) Divisible and uniform.

Making cryptocurrencies would be impossible without blockchain. The individual blockchain networks of every digital currency are essentially different style of that protocol.

The Blockchain software is sort of a universal blueprint that creates digital currencies possible, but it's not a currency in and of itself. But when that outline is employed to create a blockchain network, a digital currency is born.

The Anatomy of Cryptocurrency

Adaptive Scaling

Adaptive scaling means cryptocurrencies are built with measures to make sure that they're going to work well in both large and little scales. Other measures are included in digital coins to permit for adaptive scaling including limiting the availability over time (to create scarcity) and reducing the reward for mining as more total coins are mined.

Cryptographic

Cryptocurrency uses a system of cryptography to regulate the creation of coins and to verify transactions.

Decentralized

Most currencies in circulation are controlled by a centralized government so their creation are often regulated by a 3rd party. Cryptocurrency's creation and transactions are open source, controlled by code, and believe "peer-to-peer" networks. There is no single entity which will affect the currency.

Digital

Traditional sorts of currency are defined by a object, but cryptocurrencies are fully digital. Digital currencies are stored in digital wallets and transferred digitally to other peoples' digital wallets. No physical currency ever exists.

Proof-of-Work

Most cryptocurrencies use a proof-of-work system. A proof-of-work scheme uses a hard-to-compute but easy-to-verify computational puzzle to limit exploitation of cryptocurrency mining. Essentially, it's almost like a difficult to unravel "captcha" that needs many computing power. NOTE: Other systems like proof-of-work (such as proof-of-stake) also are used.

Pseudonymity

Owners of cryptocurrency keep their digital coins in an securely encrypted digital wallet which might only be accessed by the unique private key. A coin- holder's identification is stored in an encrypted address that they need control over it's not attached to a person's identity. The connection between you and your coins is pseudonymous instead of anonymous as ledgers are hospitable the general public (and thus, the ledgers might be wont to glean information about groups of people within the network).

Value

For something to be an efficient currency, it's to possess value. The US dollar accustomed represent actual gold. The gold was scarce and required work to mine and refine, therefore the scarcity and work gave the gold value. This, in turn, gave the US dollar value.

Cryptocurrency works similarly regarding value. In cryptocurrency, "coins" (which are nothing quite publicly agreed on records of ownership) are generated or produced by "miners." These miners are people that run programs on specialized hardware which is created specifically to resolve proof-of-work puzzles. The work behind mining coins gives them value, while the scarcity of coins and demand for them causes their value to vary. The idea of labor giving value to currency is named a "proof-of-work" system. the opposite method for validating coins is named proof-of-stake. Value is additionally created when transactions are added to public ledgers as creating a verified "transaction block" takes work also. Further, value comes from factors like utility and provide and demand.

Blockchain in Cryptocurrency

How Blockchain Works

In simple terms, the blockchain is thought of as a distributed database. Additions to the current database are initiated by one among the members (i.e. the network nodes), who creates a replacement "block" of information, which might contain all varieties of information. This new block is then broadcasted to everyone within the network in an encrypted form (using cryptography) in order that the transaction details aren't made public. Those within the network (i.e. the opposite network nodes) collectively determine the block's validity in accordance with a pre- defined algorithmic validation method, commonly named as a "consensus mechanism". Once validated, the new "block" is added to the blockchain, which essentially leads to an update of the transaction ledger that's distributed across the network.

In principle, this mechanism is used for any quite value transaction and might be applied to any asset that may be represented in an exceedingly digital form.

Transaction

Blocks are signed with a digital signature employing a private key Every user on a blockchain network features a set of two keys. a personal key, which is employed to form a digital signature for a transaction, and a public key, which is thought to everyone on the network. A public key has two uses: 1) it is an address on the blockchain network; and 2) it's accustomed verify a digital signature/ validate the identity of the sender.

On the Bitcoin blockchain, this translates into the subsequent example. Suppose that Anita wants to send 100 Bitcoins to Jitu, then first of all she is going to must digitally sign this transaction using her private key (which is barely known to her). she is going to must address the transaction to Jitu's public key, which is Jitu's address on the Bitcoin network. Next, the transaction, which can be collated into a "transaction block", will must be verified by the nodes within the Bitcoin network. Here, Anita's public key are going to be accustomed verify her signature. If Anita's signature is valid, the network will process the transaction, add the block to the chain and transfer 100 Bitcoins from Anita to Jitu. A user's public and personal keys are kept in an exceedingly digital wallet or e- wallet. Such wallet is stored or saved online and/or offline.

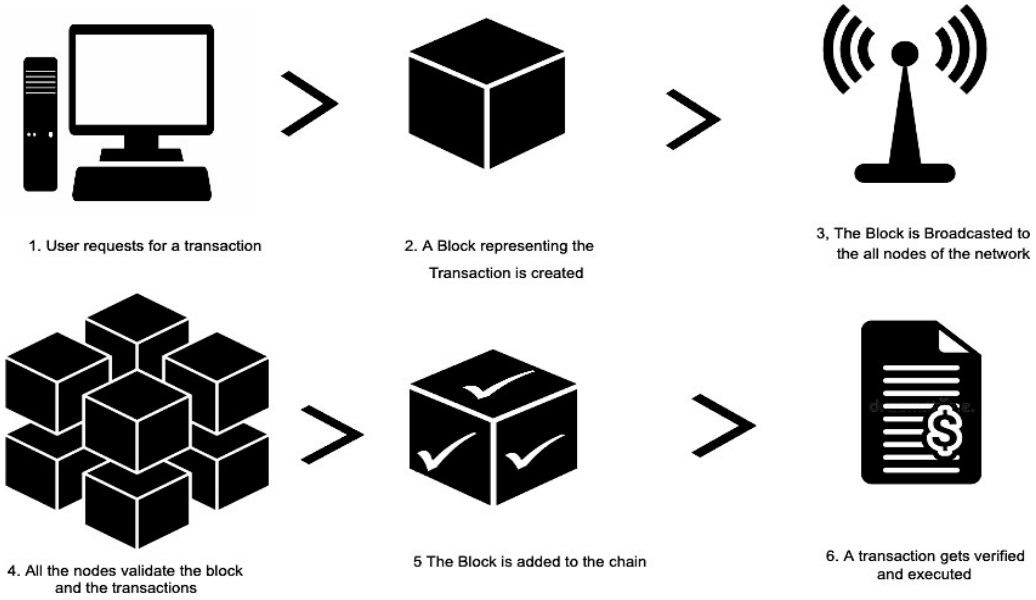

Figure 1.How blockchain works

No Middleman

One of the vital preferences of blockchain innovation is that it permits to streamline the execution of a wide cluster of exchanges that would ordinarily require the intermediation of an outsider. Fundamentally, blockchain is tied in with decentralizing trust and empowering decentralized confirmation of exchanges. Basically, it permits to remove the "go between".

As a rule this will probably prompt effectiveness gains. Notwithstanding, underline that it might likewise open connecting gatherings to specific dangers that were recently overseen by these intermediates. For example, the Bank for International Settlements as of late cautioned in a report of 2017 named Distributed record innovation in installment, clearing and settlement, that the selection of blockchain innovation could present new liquidity hazards. More by and large it appears to be that when a middle person capacities as a cushion against significant dangers, for example, foundational hazard, he can't just be supplanted by blockchain innovation.

Regulations in India

The government of India stated in year 2018 that cryptocurrencies like bitcoin are not legal tender in India. While the government is not enacted a regulatory framework for cryptocurrencies, the Federal Reserve Bank of India (RBI) has advised caution on their use and has issued three notifications that "cautioned consumers, holders and traders the risk of these currencies and clarified that it has not given any type of licence or authorisation to any entity or company to operate such schemes or deals." Recently on 6th April 2018, the RBI issued a notification prohibiting banks, lenders and other regulated financial institutions from "handling with virtual currencies," which stipulated that "in view of the associated risks, it's been decided that, with quick effect, entities regulated by the Federal Reserve Bank should not deal in VCs or provide services for facilitating a person or entity in handling or settling VCs. Such administrations incorporate upkeep of records, register, exchange, settle, clear, give credits against virtual tokens, acknowledge them as security, opening records of trades taking care of them and move/ receipt of cash in records concerning buy/offer of VCs." Moreover, the RBI expressed that "controlled substances which as of now offer such types of assistance will leave the association inside a quarter of a year from the date of this roundabout." However, Deputy Governor

B.P. Kanungo, in a strategy public interview, perceived "that the blockchain innovation or the circulated record innovation that lies underneath the virtual monetary standards has possible advantages for monetary consideration and improving the effectiveness of the monetary framework" and expressed that the RBI has "constituted an inter-departmental committee in Federal Reserve Bank of India who will produce a report and that they will explore the feasibility and desirability of issuing a digital currency by the central bank." Reports in early 2018 indicated that the government is in the process of drafting a law to manage trade of cryptocurrencies in India and "has formed committee to means the method ," consistent with the Hindustani Times. The government has expressed two main concerns that the law will address: "the source of money being used to trade in cryptocurrencies; and regulation of exchanges of VC [virtual currency] to protect the common man," one government official was quoted as saying.

An interdisciplinary advisory group, led by the Special Secretary (Economic Affairs), was set up in April 2017 "to inspect the current structure concerning Virtual Currencies." The panel has nine individuals including delegates from the Department of Economic Affairs, Department of money related Services, Department of Revenue (CBDT), Ministry of Home Affairs, Ministry of Electronics and information Technology, Reserve Bank of India, National Institution for Transforming India (NITI Aayog), and State Bank of India. The job of the advisory group is to (I) increment the size of this status of Crypto Currencies both in India and all around the world; (ii) analyze the predominant worldwide administrative and legitimate constructions administering Digital Currencies; (iii) give recommendation for taking care of such Digital Currencies including issues relating to user protection, money laundering, etc.; and (iv) examine any other matter related to Virtual Currencies which may be relevant to the matter.

7th August, 2017, Business Line reported that the committee had submitted its report, but details of the report had not been made available to the people.

29th December, 2017, India's Ministry of Finance released a press statement that cautioned all investors about the "real and heightened" risks of trading in cryptocurrencies such as bitcoin, saying virtual currency investments are similar to "Ponzi schemes." According to a February 1, 2018, news report, the Minister of Finance told lawmakers in Parliament that "the government does not consider cryptocurrencies legal tender or coin and can take all measures to eliminate use of those crypto-assets in financing illegitimate activities or as a part of the payment system, but the govt will explore use of blockchain technology proactively for introduction the digital economy.

13th November, 2017, the Supreme Court of India admitted under article 32 of the Constitution a Public Interest Litigation writ petition against the Union of India and issued a notice to the Ministry of Finance, Minister of Law and Justice, Ministry of Electronics and Information Technology,

Securities and Exchange Board of India, and Reserve Bank of India. The petition seeks "a regulatory framework to be laid down on Crypto Currency and wanted that the virtual currency be made accountable to the exchequer." The Supreme Court previously heard a petition in the month of July year 2017 that sought "a similar kind of regulatory framework": A Public Interest Litigation [PIL] was filed (Writ Petition (Civil) no. 406 of 2017) under Article 32 of the Constitution against Union of India, Ministry of Finance and therefore the Federal Reserve Bank of India over the utilization and business of Bitcoins, Litecoins, Ethereum. Ripple etc. The Supreme Court on July 14, 2017, directed the RBI and therefore the other concerned ministries to clarify their stance and enact a bill on an equivalent before disposing off the PIL.

KYC Regulation for Preventing Illegal Activities

According to the study, it is analysed that Bitcoin addresses from the corpus of the Dark Web, revealed other addresses perpetrators have owned, and traced money flows from these addresses to their destinations. Although we have shown that it is possible to reveal to where the perpetrators have moved funds, it is difficult to investigate further and identify the perpetrators. It is also observed that many of the perpetrators sent their unlawfully earned Bitcoins to Bitcoin exchanges, and if these exchanges maintain user record of users, then law enforcement may be able to apprehend the perpetrators. Government authorities around the world have recently begun to regulate Bitcoin exchanges to comply with KYC (Know Your Customer) policies. Such movements are expected to reduce cyber crimes occurring in the Dark Web gradually. On the other hand, since KYC policies break pseudonymity of cryptocurrencies, a feasible, scientific, and political compromise is required.

Conclusion

Virtual currencies and specifically cryptocurrencies which is very recent topic object in economy. There are multiple aspects of Virtual Currencies and their use in economy. Their high volatility causes maximum risk of trading cryptocurrency and is reflected in the formation of price bubbles. However, the large growths of their exchange rates attracted many speculators, but it is obvious that cryptocurrencies can only hardly keep continuing their value. This fact can lead to change in understanding of cryptocurrencies as payment medium, but rather as specific material. In comparison with commodities, cryptocurrencies have advantage of easy portability through its virtual character, but on the other hand, their virtual character makes them useless or non-existent outside of electronic environment unlikely other substantial commodities.

All the mentioned aspects generate trust in cryptocurrencies. If potential users will trust in cryptocurrencies, they might be used in bigger scale. If the trust in cryptocurrency will be not reaching to the sufficient level, the boom of cryptocurrencies might subside. This might be the case of the Bitcoin in past months, when a few marketplace crashes shook its price significantly. Then cryptocurrencies might become only medium of exchange in black economy market or speculation tool of few speculators still daring to trade cryptocurrency for standard currencies. In this case the value of cryptocurrency will be set by demand and supply of it in unofficial economy, where anonymity of transactions is highly valued characteristic of cryptocurrency usage.

References

1. Basic Aspects of Cryptocurrencies. Martin Vejačka, Technical University of Kosice - Technicka univerzita v Kosiciach. 2014.
2. Regulation of Cryptocurrency Around the World, The Law Library of Congress, Global Legal Research center. 2018.
3. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem Malte Möser Department of Information Systems University of Münster Münster, Germany.
4. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams Marie Vasek and Tyler Moore.
5. Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web Seunghyeon Lee, Changhoon Yoon.
6. The Economics of Cryptocurrencies – Bitcoin and Beyond, Jonathan Chiu (Bank of Canada), Thorsten V. Koeppl (Queen's University).
7. Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion.