IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOCURRENCY AN ERA OF DIGITAL CURRENCY

[1]Manishaben Jaiswal

Abstract: Bitcoin is the internet-based world's top-ranking cryptocurrency. It is one of the common cryptocurrencies that are readily available. Bitcoin is most experienced due to the people's anonymity and openness in the device. Daily styles in the bitcoin exchange have acquired popularity amongst fans, investors, individuals, and many more. Bitcoin cost data show preferable residential properties where some classical opportunity collection prophecy approaches use the actions, making unsatisfactory predictions without a probabilistic interpretation. This paper conducts an extensive research study on the development of Bitcoin and an organized evaluation of it. It deeply provides the information for the difference between the digital and virtual currencies, decentralized bitcoin network and compares it with others. The nature and characteristics of bitcoin. Also, depth in the study of the benefits, risks, and challenges of bitcoins. The future and application of bitcoin focus on its stability.

Index Terms – Cryptocurrency, Bitcoin, Exchanges, Digital currency, Virtual currency, Finance, Ethenium, Decentralization, Distributed network, Centralized network, Risk, Transaction, Bank

I. INTRODUCTION

Digital currency refers to currencies that are transacted over the internet with physical handling like the old currency. Digital currencies are soft money that is not tangible and gains physical value after exchanging. Digital currencies are only transacted using digital devices such as computers, tablets, and mobile. Further, digital currencies are only kept in digital wallets that are only available online. Digital currency differs from physical currencies such as mint coins and notes that can only be transacted when the business faces. Like the physical currency, digital currency can buy goods and services, although depending on the type of currencies, they can be restricted in some areas or sites. The advantage of digital currency is that they have intrinsic value and can be used to make transactions across borders on a real-time basis as far as the sites support the system. The good thing is that digital currency can be converted to any currency on a real-time basis without visiting any physical offices. Digital currencies are also less costly as there are no intermediaries parties. The sender and the receiver are on the same network platforms allowing the currency to be used. They also have fewer clearing hours and are necessary as the transactions receipts displayed on both sides enhance transparency. Digital currency exists in various forms and can be considered a virtual currency that has played a significant role in globalization and expanding the global market. Another form of digital currency is a cryptocurrency that is highly used in the development of centralized currencies.

While cryptocurrencies are digital currencies, not all digital currency is cryptocurrencies. When offered and controlled by the central bank, it is referred to as "Central Bank Digital Currency" (CBDC). Uruguay and England are some countries that have shown interest in releasing their decentralized digital currency that the central bank will only regulate. However, the idea is proving hard to implement as the countries within the union are finding it hard to agree. The primary reason for the disagreement is over sovereignty and the control of digital currency. Also, the countries engage in businesses outside the union that might not recognize their digital currency, increasing economic instability, and currency crush. The accomplishment of a digital currency depends on its acceptability by all other countries. Digitization has increased globalization leading to countries engaging in businesses with almost every other country; thus, having a virtual currency that is not recognized in other countries will lead to an economic crisis.

II. HISTORY

Bitcoin, which is also known as intelligent contracts changing financial technology. Most central banks and corporations adopt new technology known as the blockchain network to be a node on that network. With the use of blockchain, investors are getting more money and becoming billionaires. However, as per the professional founder, only twenty-four percentage of people are familiar with this technology. This paper discusses the two major companies which are very different from adopting bitcoin technology in the past.

The company which adopted bitcoin is as follows.

- There are significant companies like Microsoft, Overstock, and so on who accepted bitcoin as a currency. Let's go through Microsoft. Microsoft is the first technical company who grant bitcoin as an official payment since 2014. Users can buy Windows 10 licenses, movies, and applications into Windows or Xbox using the bitcoin currency. The history of how Microsoft adopted bitcoin currency is as follows.
- Microsoft is the first multinational technology corporation in America, developing, supporting computer software and multiple services. The company was established in 1975, and the founder was Bill Gates and Paul Allen. The company has its headquarters in Richmond, Washington. Microsoft is interested in bitcoin and blockchain technology for its

projects. In 2014, Microsoft first time began granting bitcoin currency using the online payment system. Unfortunately, bitcoin payments shut down three times due to several reasons like lack of cash, finance, and economic issue.

- Furthermore, Microsoft users can restock the bitcoin currency without the risk of giving it back. Users can use it for the purchase of Microsoft services. For the last few years, many large-scale organizations, government, and finance sectors and users refuse bitcoin as a currency. On the other hand, bitcoin is the usage of digital money across the world. In 2016, due to global economic instability and financial issues in the market, some parts of Asia, like India and China, can only use bitcoin. The reason behind that is banknotes, unavailability of cash, rapid reduction of money into the market, and capital outflows become unstable. By 2016, most investors conclude that bitcoin is the only safe global currency to prevent financial and economic issues. From onwards, it was outplaced for available cash and assets. Its demands are going high continuously. As per the last couple of years, bitcoin's prominent role is to protect houses and businesses' wealth. For the last couple of years, Microsoft devised bitcoin as a currency, and billions of users developing Microsoft office as regular users to buy the window license and box store products.
- The recommendation to the company to support bitcoin is as follows.

  - ✓ The significant transaction is challenging because of trustworthy facilities like bank or money transfer, which must require a middle person or agency which charges the fees.
  - ✓ Sometimes it affects the small businesses who lose 2-5% of card processing fees. It is also inconvenient, and users are forced to pay in cash to save their processing fees.
  - ✓ Physical cash still requires spending too much time checking and authentication in the transaction of the bill.
  - ✓ The cash amount can be a secret amount, which may not be on the record. It allows the black market to form and criminals to transact illegal activities.
  - ✓ Bitcoin is the only solution to overcome the above problems, increase the overall cash assets, and ensure that the transaction must be free, impartial, and visible.
- On the other hand, the company that refused the bitcoin transaction is Alibaba group from China, Amazon.com, etc. For the last couple of years, wild speculation about the company most users is supporting e-commerce. They want to adopt digital currency. However, this company has many firms of interest. The company does not have a specific plan to adopt this currency, and the company is just looking at this option as an approach. Most multinational companies support cryptocurrency, the co-founder of Alibaba Group, Jack Ma, informed that bitcoin is only a market value that can be escalated. The company is no longer interested in this payment method.
- The reason for the Alibaba group to refuse the bitcoin currency is as follows.

  - ✓ Alibaba Group is supporting the e-commerce firms on which it personally conducts the business via the internet. E-commerce is a big platform to buy and sells good and services through the internet.
  - ✓ According to the company's view, bitcoin is acting as a bubble. The company describes that bitcoin is an economic cycle that can escalate the market value, especially assets' price.
  - ✓ The currency that fasts increases and follows in the digital market can decrease its value, also known as bubble burst or error, changing the user's behavior.
  - ✓ Bitcoin also supports the credit cycle at one level. It helps the business to make more support in terms of decisions and investment. The recurring phrase is easy but tight borrow capacity.
  - ✓ The average cycle period is longer than the business cycle, taking time to decline the property value and show up at the regular price.

Bitcoin is a great way to rephrase the technology to view it and use the money for it. Bitcoin is the leading online translation domain due to several problems like black money, actual function, or strength over the market. The USA is the most prominent country in terms of bitcoin startup and total transactions. The decentralized currency found is known as bitcoin. Although many companies support bitcoin like Microsoft, on the other hand, some companies like Alibaba group refuse to adopt this currency.

III. DIGITAL CURRENCY VS. VIRTUAL CURRENCY

Figure II History

Although virtual and digital currency is used interchangeably while describing currencies based on a digital medium, the term “digital” has a terrible connotation. “Virtual” alerts something this is “apparently real”; however, now no longer strictly “real” while regarding foreign money. It is saved in a “virtual” or digital register.

Numerous socioeconomic forces call for opportunity currencies as follows.

(a) Localism

By selling network trade or “shop excessive street,” localism keeps consumption inside a set of unbiased outlets or a geographic region for job advent and progressed commercial enterprise conditions.

(b) Technology

It emerged as a good deal less complicated to apply with progressed software programs and coffee access barriers contributing to community effects.

(c) Political economy

There is disillusionment approximately the excessive pay of CEOs and bankers and the notion of conventional banks being too large to fail. With excessive debt and quantitative easing, there's fantastic soreness with financial uncertainty.

(d) Environmentalism

There are ecology issues and the query of whether or not we've reached the factor of most extraction of herbal assets, including oil.

(e) Inefficiencies

Financial offerings are overpriced, and the complete monetary device is too expensive.

(f) Financial freedom

Some virtual currencies, including cryptocurrencies, have the gain of transferring price via the internet, in which manipulation is weak. Such virtual currencies may permit customers to pass capital controls and offer secure harbor through a fiat foreign money crisis.

(g) Speculation

Buyers of a few virtual currencies, including cryptocurrencies, watch for price appreciation because of broader acceptance. It could be immaculate to create a cryptocurrency as an opportunity for foreign money at no cost today.

However, a maximum of those new creations will stop circulate inside a surprisingly quick time. With many opportunity currencies in competition, just a few might be globally adopted, attain enough scale, or discover an appropriate market. Unless the concept of countrywide virtual currencies takes off, it's miles probable that lots of those opportunity currencies will stop circulating due to superseding improvements in technology, tighter regulation, and inadequate calls.

IV. NATURE AND CHARACTERISTICS OF THE BITCOIN

Figure IV Nature and charactstics of the bitcoin

Nakamoto's decentralized currency was an action to the economic dilemma and federal governments' reactions to it and the function of banks and various other settlement intermediaries in mediating financial deals. Bitcoin is not the first instance of decentralized digital money; however undoubtedly the most famous so far. In straightforward terms, bitcoins are transferred from computer to computer using cryptographic hashes and kept secure with public-private essential cryptographic keys. Customers can save their currency in a "wallet," which takes either a software program mounted on their computer or a web-based account.

Initially, money is a tool of exchange utilized as an intermediary in the profession to prevent the aggravations of a barter system. Second, money offers a method of accounts. It serves as a conventional mathematical device for measuring the value of products and services to alter offerings on the market much more comparable. However, to work as a reliable unit of account, a currency must be more than decimal and readily divisible. It should provide a measure of relative worth that customers can understand on a nearly user-friendly level. Otherwise, customers must expend time and initiative to identify what the currency and its connected unit of account imply. In addition, a currency can work as an effective unit of account just if customers accept its authenticity. Third, currency serves as a shop of the value of existing revenues for future costs. Noncirculating cash can circulate in the future, and that possibility for future blood circulation represents wealth or value that a specific participant can exploit. Undoubtedly, bitcoin can act as a circulating medium. However, it is still a weak barter driver offered the minimal variety of venues approving electronic money. It is suspicious whether electronic currencies can be taken into consideration fundamentally and without effort valuable.

To establish just how much digital currencies deserve, users usually convert their value into value expressed in a standard unit of account. By checking out the string of information, rarely can any individual recognize its worth. It is difficult to identify the worth of products in bitcoin without knowing the bitcoin currency exchange rate at a particular time. The question emerges regarding whether bitcoin meets with a "store of value" function to be reliable and safe. Anytime, regulators from various jurisdictions might do something about it versus bitcoin and its individuals. At any moment, the bitcoin market may break down due to transforming views amongst bitcoin users: A technically more powerful decentralized currency may show up and weaken bitcoin to a plain historical occurrence. As well as naturally at any moment, technical problems may bring bitcoin down without any warnings. Provided the massive volatility of bitcoin, feasible technical troubles, the absence of oversight, as well as lawful unpredictability surrounding bitcoin. It is problematic whether bitcoin can be a reputable store of value. Besides, saving wealth in any tool that is easily susceptible to collapse or cost variations is ill-advised.

To summarize, presently, bitcoin cannot be considered as money in the economic feeling. It is still surrounded by significant lawful and factual uncertainty, which questions its capacity to store of value. As a result of its limited usage and huge volatility, it cannot work as an accounting device. It’s worth having to be first converted right into the worth of a conventional currency. Nonetheless, bitcoin has the potential to end up being financial cash in the future. Time will inform whether bitcoin will be reputable and secure adequate to achieve this aim.

V. CRYPTOCURRENCY

Cryptocurrencies have recently gained significant popularity, and many people embrace them, primarily due to their mining capabilities, enabling people to invest and earn profits. Cryptocurrencies are digital money that exists in the form of tokens that are recharged when exhausted. The tickets can trade and make payments like any other currency, only that they do not have any physical condition and cannot be withdrawn by the owner. Any withdrawal will mean the exchange of the digital currency to the known physical currencies. The development of cryptocurrency is done by forming a specific code. Their founders and principles are used for the transactions and the controls. The primary aim of the cryptocurrency developers is to make the currency free from the government so that the currency would be recognized globally. However, the situation has been received with heated debates that the currencies will increase crimes as criminals and terrorists transfer money worldwide without any control. Currently, they are various types of cryptocurrencies that have been developed, and although not recognized by individual states, they are being used by the citizens as it lacks government control. Cryptocurrencies are the functions of algorithms that are developed through "Artificial Intelligence" applications. Cryptocurrency has received significant popularity recently, especially with its mining capability.

Further, businesses and industries embrace these digital currencies as a payment method as it enables real-time transaction, transparency, and minimizing added costs associated with other known currencies. Also, online mining created by different companies allows users to access smaller amounts of the cryptocurrencies that have been popularized. It is about the same as forex trading that enables users to earn money through buying and selling the currencies as the prices keep falling and rising. Some of the currently existing cryptocurrencies are.

Ethereum

Ethereum was the second to be developed after bitcoin, and its advantage is that it combines the aspect of decentralization and smart contracts. The primary trading currency there is, it also has enabled decentralization and elimination of the third party.

Litecoin

Litecoin is an additional type of cryptocurrency that has gained popularity since its inception in 2011. Litecoin is not controlled by any centralized institution and pillared on an open-source global payment network. At the same time, Litecoin has a high similarity with bitcoin. Its difference is based on the speed of transactions influenced by its faster block generation rate. Litecoin has gained significant acceptance.

Cordano

Cordano is also referred to as the "Ouroboros proof-of-stake" coined by a group of mathematicians and engineers. Its development was aided by one of the former ethereum engineers who were unhappy with the performance of the Ethereum. The primary goals of the Cordona are to integrate the ability of financial operations with other solutions such as chain insurability, legal contracts, and voter fraud.

Bitcoin

Bitcoin it is the oldest and still the most robust cryptocurrency since its inception in 2009. The currency was developed by an anonymous person who used the pseudo name Satoshi Nakamoto. It is still a misery why a person who invented the longest-standing digital currency could opt to remain anonymous for so long. Although bitcoin has not been authorized as a legal tender globally, it's popularly used even by giant companies. Bitcoin is the mother of all the other altcoins as they are improvements having additional characteristics but retaining the same masterpiece. The immediate success of bitcoin is framed on its decentralization nature and use of blockchain technology, making it a complex system for hackers to penetrate despite being worth billions of money. Blockchain and bitcoin have been confused with being one thing for the longest time until recently. Blockchain is a ledger system that anyone can use, and bitcoin is a cryptocurrency that utilizes blockchain technology for its inception.

For all its strength, the blockchain network is just a mechanism for verifying and circulating bitcoins. Converting it into valuable services needs the production of an entire range of corresponding capacities. There is already an arising constellation of service companies that intend to create a duty independently by taking care of bitcoins better and conveniently for users. The following is indicated to be an illustrator rather than a complete checklist of advancements being developed. The highlighted suppliers are once more meant to be illustrators than always to lead ones in each area.

VI. BITCOIN EXCHANGES

Figure VI. Bitcoin excchanges

So as for bitcoins to become widely accepted, individuals will need the support to liquidate their bitcoin holdings at will. Bitcoin exchanges are online marketplaces where bitcoins may be bought and sold out against one or many other currencies. A survey of the exchanges and their sites is given in Bhaskar and Lee. Some websites, like Local bitcoins, just facilitate the meeting of bitcoin consumers and marketers. They act as dealers, very similar to how eBay works: Sellers post their offers online, and buyers choose the actual seller they require to shop from consumers to pay the seller directly through a mechanism planned by the vendor. As an outcome of the transfer of paper money associated bitcoins isn't coincident in time, there's selected counterparty risk. Like BTC China and the recently bankrupted Mt.Gox of Japan, the more meaningful exchanges operate bitcoin markets on an eternal basis, exchanging the counterparty risk. Before transacting, market participants must be compelled to fund an account at the exchange with the currency they want to sell: depositing bitcoins to eliminate bitcoins or depositing other currency if they're going to shop for it. Exchanges generally settle for each market order buy/sell transaction to be dead at the prevailing market-clearing price and limit orders to be executed if the value reaches a definite threshold. Once transactions are completed, users withdraw their new noninheritable currency: causation bitcoins to their bitcoin case if they bought bitcoins or

transferred cash to their checking account if they sold-out bitcoins. Transacting at the exchanges is comparatively quick. However, depositing and retreating benefit a user's account at the exchange can take longer, betting on the interbank money transfer arrangements in every country. Exchanges are the most vital intermediaries that link other currencies with cryptocurrencies. It's possible to be the primary target of regulation. The price of compliance is envisaged to extend once the principle is in place. On the income side, it is estimated that ratios are squeezed as in most exchanges. Ironically, the most crucial threat can return from inside the bitcoin protocol with peer-to-peer mechanisms in bitcoin and bitcoin-fiat/fiat-bitcoin space. This sector is clearly at the forefront of margin squeeze with increasing cost and decreasing margin. It's anticipated that the age of consolidation will come loads quicker than expected. Unless revenue growth or bitcoin use rises faster than cost, the coalition is most severe during this section of the ecosystem.

VII. DECENTRALIZATION IN BITCOIN

Bitcoin security systems are based on its decentralization nature that is made possible by utilizing blockchain technology. Blockchain technology is a numerical ledger that allows the distribution of data without any changes. Bitcoin, like any other currency transaction, needs a database system to keep its records. Since Bitcoin is a digital currency, the documents need to be put in computerized systems. However, unlike most currency databases, the computers used to store bitcoin data are not under one facility but distributed across different geographical areas depending on where it is being applied. Blockchain is one such database system that is used by bitcoin to allow such distribution of information. In a typical currency transaction company, many computers, supposedly thousands, hold accounts information for their clients and are run under one roof and operated by specific individuals authorized to handle such information. Bitcoin also has such a kind of system where its data is held in several computers. Still, in this case, there are distributed in different geographic areas and run by diverse people who, in most cases, do not realize each other. Such is the aspect of decentralization. Blockchain uses networks refereed as nodes that are the primary block towards its high-security mechanisms. Blockchains are some of the highest secured systems in an information system that has proven challenging to cyber hackers. The designs have proven to be the most comprehensive existing security system that hackers have not devised to get through it. However, the system's complexity is based on nodes' interrelationship, requiring any hacker to change more than half of the nodes to get through the system. The high costs incurred in terms of infrastructure and lengthy time make it unprofitable for hackers.

The blockchain nodes contain the complete information of every transaction that has ever been made since the technology was incepted. The nodes have a self-correction mechanism that helps to protect any changes in the information. The idea is if an error occurs in one node, it uses the rest of the nodes as reference points to correct itself. There is no possibility of any node changing the information kept in it as other nodes on the systems will automatically update it. Such indicates the independence of the system that enables decentralization. When a blockchain user tries to temper the information, the other nodes cross-check it and correct it automatically. Changing data in the blockchain would mean changing the data for 51% of the nodes, which would be costly and time-consuming. Bitcoin achieves its decentralization based on such characteristics as the system does not trust anybody for its maintenance. Unlike other systems that need cross-monitoring to protect them from hacking, blockchain is self-correcting. Such decentralization in bitcoin enhances the transparency of its transaction, and both parties can track the transaction. The information in blockchain is publicly visible and thus enables any willing party to follow their bitcoins anytime, anywhere. The below table summarizes decentralization, centralization, and distributed networks operate in different fields.

Table V.I: comparison of a decentralized network, centralized network, and distributed network

	Decentralized network	**Centralized Network**	**Distributed Network**
Hardware	Individual network members own Resources	Resources and controlled and maintained in a centralized location by a single firm	Owned by network providers and distributed in different physical locations
Solution components	The ledger is the same and can be accessed by every member of the network	A central entity has control and responsible for the maintenance	The solution provider has control and maintenance powers
Data	It can only be added or changed through a consensus	Central entity has the control	The customer owns and manages the data
Control	Has no individual ownership and control	The system owners have the control	The control is shared between the end-user and the service provider based on the terms of the agreement
Performance	It changes as the number of members in the network increases	The specific entity controls and maintains performance	The performance increases as resources scale-up
Security	Increases as network members increases	Maintained by the entity	Security management is a shared responsibility between the system user and the service provider
Typical example	Blockchain used in Bitcoin	Bank system	Cloud computing

Further, the decentralization blockchain enables bitcoin to differ significantly from bank systems. Such comparison is illustrated in the table below.

Table V.II: bitcoin v. bank

Feature	Bitcoin	Bank
Fees for transaction	The transaction differs, and users have bargaining power. However, it ranges from 0 – 50 dollars. The bargaining power creates a free marketplace where every network member can choose their transaction fee.	Bank has ongoing fees that vary depending on transactions engaged, and in most cases, they are cut directly from the account when services are sought. Thus the trades are not open as the transactions are set and controlled by the bank entities.
Opening hours	The systems are open on a 24/7 hourly basis	All banks are opened under limited hours, especially during the day, and closed on holidays ate on holy days.
Speed of transaction	The speed of the transaction depends on network congestion and can take up to15 minutes.	Most of the transactions range between 24-72 hours, and mostly the transactions are only possible on business days.
"Know Your Customer Rules"	Bitcoin operates anonymously, and anybody or anything that can access the network can participate in the network.	Bank requires procedures and collects customer information before opening an account with the bank.
Transfer easiness	The network members only need a connection to the internet network and a device to support the internet.	Government identification, mobile devices, and bank accounts are required on the minimum to operate in a bank system.
Privacy	Blockchain networks can be private or public as the owner wishes. While the ledger information is shared, bitcoin allows anonymous buying.	The bank account owner's privacy depends on the security levels of the bank systems towards hacking as the information is stored on the bank's data servers.
Security	High level of security as it uses highly decentralized blockchain technology.	The level of security depends on the security systems installed by the banks. They are always the risk of the information being hacked and accessed by hackers and cybercriminals.

A key concern for bitcoin users is that the secure storage of personal keys. The bitcoin protocol incorporates several security measures preventing stealing as bitcoins travel through blockchain-like networks. However, there are vulnerabilities on the shopper aspect, especially with bitcoin private keys' safe storage. A variety of suppliers are attempt this risk in an exceeding number of ways:

- Bitcoin paper wallet could be a packaged answer for generating secure bitcoin keys and printing on any connected printer. Printouts hold the public and personal keys in each text string and QR format. Printouts are designed to be accordion up and taped shut to avoid casual snooping. There is the likelihood of tape recording them with tamper-evident and serialized holographic strips on the market for purchase from the constant company. This procedure permits users to keep their bitcoin keys in bits of paper that are straightforward to store firmly and are entirely on the far side of the reach of hackers.
- The paper could be a dedicated hardware electronic computer that generates secure bitcoin keys victimization its own high-standard random range generator. The keys will then be held inside the device, written out using an incorporated thermal paper printer, or transferred via a USB port to a USB memory stick or an external printer. Thus, it permits for duty of keys in paper format or on offline digital storage devices.
- Bitcoin key holders could use exceedingly plastic cards instead of writing on paper. The personal secrets are printed on a QR code placed between plastic layers within the cardboard and can't be scanned while not physically destroying the plastic card. There is no digital record of the private keys excluding the card itself, limiting potential double-spending or fraud but exposing its holders to complete loss if they lose the plastic card.
- Trezor could be many smaller hardware pieces that do not solely generate and hold bitcoin personal keys; however, it conjointly lets users sign transactions with those keys. It is linked to the USB port of a user's computer, and thru that, it permits the safer offline language of bitcoin transactions processed through online wallets. Another security concern for a few bitcoin users is protecting their anonymity, that is, keeping their bitcoin anonym whole break free their real identity. The priority with the high degree of traceability of bitcoin dealings, their identity is worked out, either by analyzing transaction patterns or tracing the pseudonym back to previous transactions. Wherever identity was disclosed (e.g., for regulative reasons).

Business services have arisen that promise to boost the barriers to tracing identity. Bitcoin mixers or laundries mix the funds of the many users into a group of shared bitcoin addresses to alter the path of bitcoin back to individual users. Blockchain info and big laundry operate the larger ones. Combining services requires users to trust the intercessor mixing the addresses since they ought to hold the personal bitcoin keys to shift cash around instead of the users. Combining services will be utilized by money launderers.

VIII. BENEFITS OF THE DECENTRALIZATION NATURE OF BITCOIN

- **Trustless environment.**
  Each party engaged in the transaction has access to the transaction ledger, and thus no trust is required. Further, the system does not tolerate any alteration as it is automatic. Such enables transactions to occur even between two strategies.

- **Enhances information reconciliation.**
  Unlike in other transactions, decentralization enables the bitcoin transactions to be managed under a decentralized system where any willing party can view it in real-time without the fear of data being compromised. The anonymity characteristics of bitcoin enable sharing of information without knowing the origin.

- **System weakness reduction.**
  Centralized systems always risk system failures due to reliance on specific actors such as services providers, leading to inefficient services and recurrent server failures. Bitcoin network systems are decentralized and can be accessed from any network with any device, thus reducing such weakness as specific actors do not control their systems.

- **Optimizes distribution of resources.**
  Bitcoin wallet optimizes the resources as the only required infrastructure is a mobile device and internet connection. With such, anybody can become a member and place without visiting physical facilities like banks to open accounts. Also, decentralized bitcoin eliminates the need for intermediaries, significantly when the transaction to different geographical locations reduces the actions involved. The transaction costs and time value is relatively low enhanced resource utilization. Time value is a significant resource that is overlooked in most cases but is very costly for all-around busy individuals.

IX. RISK OF THE BITCOIN

- **Internal modification and volatility**

As a community-driven task, bitcoin remains to undertake adjustments as software programmers boost and transform the software program with an agreement of network users. At the same time, the price of bitcoins continues to fluctuate as current events affect the cost. Some considerable cost adjustments are claimed to appear like a traditional speculative bubble, which might happen when hopeful media protection draws in financiers. It may make it challenging to determine precisely how great bitcoins are as a store of value, and vendors approving bitcoins as a result often convert them out right into fiat currency very promptly. It is also challenging to anticipate the bitcoin economic climate as it is the first commonly available cryptocurrency. However, researchers are already working on models that will try to describe habits in the bitcoin globe. At a parallel moment in time, it may be possible that the value of bitcoins might become less unstable as knowledge of bitcoin increases with time.

- **Facilitation of criminal activity**

With the pseudo-anonymity and ease of payments provided by bitcoin, it is no wonder that governments are interested in using bitcoin to assist in criminal tasks. Undoubtedly, among the most famous illegal uses of bitcoin was on the silk road website, an underground market typically used to trade unlawful medications and counterfeit tickets. Silk Road used a mix of bitcoin repayments and the anonymizing network to develop an industry for such illegal goods and solutions. Another primary concern relating to bitcoin is its usage to launder money and terrorist activity. Currency was shut down on money laundering concerns. It is essential to think that bitcoins are like cash, utilized for both authorized and illegal functions. Various other cash transfer methods have been used to fund criminal offenses and money laundering before bitcoin existed. Nevertheless, many bitcoin exchanges are starting to employ antimoney laundering, including keeping the records of their customers, which will decrease the attractiveness of bitcoin to lawbreakers.

Bitcoin, however, likewise uses benefits over traditional money that is secure against some forms of economic crime. For example, the mining process of confirming transactions, which addresses the double-spending problem, makes it very tough for bitcoins to be double-spent or counterfeited. An enemy needs to generate adequate computing power to get rid of the mixed network computing power to have the ability to attempt to change the present and future purchases before the remainder of the network catch-up.

- **Legal regulatory perspective**

As bitcoin is unique, its guideline by federal governments runs the range of being liberal to outright restrictions. The regulatory landscape remains to change as federal governments grapple with the dangers and benefits of bitcoin in their country. For a beginning, regulators in some regions are starting to provide policies and support electronic money approaches. In their country, specifically in actions connecting to antimoney laundering and countering terrorist financing, along with taxes. The challenge for supervisors is to encourage beneficial uses and future developments while lessening the risks postured and doing so without preventing such technologies from spawning.

X. DRAWBACKS OF BITCOIN INVESTMENTS

Bitcoin may be the future of monetary swap, but it is every bit as essential that you recognize the issues encompassing cryptocurrency committing. Right here are some serious dangers connected with bitcoin financial investments.

- **Instability:** The cost of bitcoin is constantly splashing backward and forward. If you took place to acquire bitcoin in December 2017, the price was $20,000. In the following weeks, you could not sell your assets for much higher than $7,051. The bitcoin exchange is frequently changing. With such an uncertain market, you may hardly get an excellent return on your investments. To avoid substantial loss, maintain a close eye on the market.

- **Threat and hacking**: Bitcoin swaps allow you to buy and offer your cryptos using a mobile phone app or website. Also, bitcoin kept on substitutions is not guaranteed through the FDIC.
- **No regulation:** A little bit of or no law. The bitcoin market currently operates along with no major requirements. It is not taxed, and governments possess no precise posture on it. Therefore, you might stand uncovered to fraud and negligence.

- **Limitation of use:** Bitcoin is currently only taken through a handful of online businesses. Many providers do not realize bitcoin as a legitimate swap, creating an unfeasible financial investment ship.

- **Loss of wallet:** If hard disk drive crashes or infection harms your budget report, you drop your bitcoins. You may go coming from a prosperous to the bankrupt investor within seconds, along with no technique to recover.

Finally, the bitcoin market currently functions along with no primary guidelines. Bitcoin swaps allow you to buy and sell your cryptos using a mobile phone application or website. Many providers do not recognize bitcoin as a legitimate swap, creating it an unworkable expenditure vessel. If your hard disk crashes or the virus contaminates your purse data, you drop your bitcoins.

XI. BITCOIN APPLICATIONS AS A FACTOR OF ITS DECENTRALIZATION NATURE

- More and more stores are accepting bitcoin payment, and thus it is being used to buy goods and services like any other currency.
- Bitcoins enable anonymous transactions and thus gaining application by individuals who would need their identity concealed.
- They are being applied in international transactions as the currency is easily moved around as it is not affiliated with any country.
- Bitcoin enhances the freedom of transaction as there is no need for authorization from any entity. The release enables individuals to transact any amount they may wish, at any place at any time.
- Online security has been a significant issue, especially in financial transactions, and bitcoin is gaining considerable popularity in that line.
- Bitcoin has no credit card payments, and thus the fees incurred are at the minimum.
- Another bitcoin application is that can be used as an investment as its value changes over time. It can be equated to the stock shares whose value can increase or decrease over time.
- Another significant application is that it can be used in gambling sites like Royal Bitcoin and Peerbet. The characteristics enable individuals across the globe to participate on the gambling sites with ease without any limitation to load or withdraw cash from their gambling sites.
- Bitcoin is also gaining a platform on popular applications due to its ability to be self-secure and thus no need for the users to provide personal identities. Personal information is sensitive, and people tend to embrace systems that require less or no personal information disclosure.

XII. FUTURE OF BITCOIN

Bitcoin is a decentralized system and a digital unit of currency that uses a peer-to-peer unit to verify and process transactions. As opposed to counting on trusted third parties, like banking companies and card processors, to refine repayments. The bitcoin technology utilizes cryptographic evidence in its computer software application to process deals and confirms the validity of bitcoin as it spreads the processing job amongst the network. In between, bitcoin financing is utilized for a currency unit or even an electronic deal developed by the bitcoin device.

While bitcoin has recently gained significant applications, influenced by its decentralized nature, its future is not guaranteed and has many uncertainties. Most people believe that the recent bitcoin price changes and their significant application show how

digital currency will likely overcome individual country currencies and become a global currency. However, while the system lacks any centralized control, its price fluctuates from time to time. The recent spontaneous increase of bitcoin has raised an alarm of the possible collapse in the future. The problem is that, while countries can intervene and correct the impact of inflation on their currencies, bitcoin has no specific authority.

Finally, bitcoin is designed to operate merely with the complete agreement of all system consumers. It ensures that program programmers who customize the bitcoin resource code in their versions of the software application can quickly not push a wicked modification in the bitcoin protocol without compromising the rest of the system. The power to transform the bitcoin protocol needs the entire arrangement, bitcoin developers, and individuals. The several facts which can attribute to the bitcoin application are as follows.

- Bitcoin cannot attain the level of a global currency. Due to its decentralized nature, making bitcoin currency, a global currency may disrupt economic functionality and involve political instabilities as nations lose monetary sovereignty. The European Union has tried to integrate their monitor value, but occupied countries have not yet agreed on its mechanisms.
- Bitcoin has no future in being integrated into the monetary mainstream systems to maintain its anonymity characteristics. Mainstream financial institutions such as banks require personal information of their customers and their transaction instructions that are limited when using bitcoin.
- Bitcoin has no physical currency, and people need to find an individual to buy the bitcoins to be competent to withdraw the cash for local use. If everybody trades in bitcoins, there will be no one to accept the bitcoins and even the risk of the value depreciating at significant rates. In general, as far as each country protects its sovereignty, bitcoin will remain as an online currency without gaining any global currency status.

Bitcoin runs on a Blockchain network, and it uses a Proof-of-Work consensus algorithm, which uses significant energy resources. We all must understand that the incentive to make money through mining bitcoin also makes us increase the use of non-renewable energy, which takes us against going carbon neutral to save our planet from global warming effects. Government and miners should come forward to make a deal to use renewable energy for mining cryptocurrencies. No great technology should be adapted if it comes at the cost of the future of the earth. If Bitcoin and other cryptocurrencies move to efficient consensus algorithms like proof-of-stake, which also assists in saving energy, it certainly can be considered the future of currency.

XIII. CONCLUSION

Technology has evolved significantly, disrupting almost every aspect of human interaction and the business field through technology innovations such as smart homes. Artificial intelligence vehicles and robotics have been developed. Financial banking also has been disrupted by cryptocurrencies that are slowly gaining popularity and application. Bitcoin is one such cryptocurrency that has increased in value and popularity recently. Bitcoin uses blockchain technology that enhances its decentralization nature. The decentralization is achieved using the blockchain ledger that allows the information to be stored in the secured system that provides access to the public and bars any alteration. The decentralization nature eliminates the need for any intermediary when transacting as the system has no single central entity that controls or manages its functions. The decentralization enables people to transact anonymously in the blockchain and increases transparency.

While the decentralization nature is advantageous to the use of bitcoin, it presents a challenge for the future development of the currency as it cannot gain acceptance as individual currencies due to fear of losing sovereignty. Also, bitcoin is highly volatile, thus influencing high economic instability when made a global currency. Another issue is that bitcoin is only virtual and has no tangible currencies, thus making it hard to use in small-scale businesses that need daily hard cash. The recent buildup in bitcoin value has led earlier investors to get high profits and become rich quickly. However, bitcoin has no physical currency, and people need to find an individual to buy the bitcoins for them to be able to withdraw the cash for local use. If everybody trades in bitcoins, they will be no one to accept the bitcoins and even the risk of the value depreciating at significant rates. In general, its decentralization nature has its advantages and disadvantages, and like any other technology, bitcoin is expected to progress. Finally, bitcoin is a novel development in terms of the settlements and decentralized systems we understand today. It brings several advantages and threats that individuals ought to be aware of and conversant with they must wish to cope. This phase has generally discussed the highlights of bitcoin. The other cryptocurrencies are likely to possess identical features and a clear understanding of bitcoin. Cryptocurrency with an efficient consensus algorithm saves more energy than it consumes; it will undoubtedly help recognize various other cryptocurrencies.

XIV. REFERENCES

[1] Oro, B.S., & Ferreira, N.A. (2016). The social benefits of Bitcoin as currency, Anuario Mexicano de Derecho Internacional 16: 499-523.

[2] Osterrieder, J., & Lorenze, J. (2017). A statistical risk assessment of Bitcoin and its extreme tail behavior, Annals of Financial Economics 12(1), 1750003. DOI: 10.1142/S2010495217500038

[3] Anandakumar, H., & Umamaheswari, K. (2017). An efficient optimized handover in cognitive radio networks using cooperative spectrum sensing. Intelligent Automation & Soft Computing, 1-8.

[4] Pavlovski, C.J. (2015). Reference architecture for cryptocurrency in banking, Information Technology in Industry 3(3), 74–80.

[5] Peng, Y.; Albuquerque, P.H.M.; Camboim de Sa, J.M.; Padula, A.J.A.; & Montenegro, M.R. (2018). The best of two worlds: Forecasting high frequency volatility for cryptocurrencies and traditional currencies with support vector regression, Expert Systems with Applications 97: 177-192. https://doi.org/10.1016/j.eswa.2017.12.004

[6] Phillip, A.; Chan, J.; & Peiris, S. (2018). A new look at cryptocurrencies, Economics Letters 163: 6-9. https://doi.org/10.1016/j.econlet.2017.11.020

[7] Pick, L. (2015). Goldman Sachs report: 80% of Bitcoin trading in Chinese yuan, Goldman Sachs Global Investment Research, Finance Magnates. https://www.financemagnates.com/cryptocurrency/trading/goldman-sachs-report80-of-bitcoin-trading-in-chinese -yuan/

[8] Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets, Information Economics and Policy 3, 1-14. https://doi.org/10.1016/j.infoecopol.2017.02.002

[9] Pinzón, C., & Rocha, C. (2016). Double-spend attack models with time advantange for Bitcoin, Electronic Notes in theoretical Computer Science 329: 79-103. https://doi.org/10.1016/j.entcs.2016.12.006

[10] Ram, A.; Maroun, W.; & Garnett, R. (2016). Accounting for the Bitcoin: Accountability, neoliberalism and a correspondence analysis, Meditari Accountancy Research 24(1), 2–35. DOI: 10.1108/MEDAR-07-2015-0035.

[11] Santos, R.P. dos. (2017). On the philosophy of Bitcoin/blockchain technology: Is it a chaotic, complex system? Metaphilosophy 48(5), 620-633. DOI:10.1111/meta.12266

[12] Sotiropoulou, A., & Guégan, D. (2017). Bitcoin and the challenges for financial regulation, Capital Markets Law Journal 12(4), 466–79. DOI: 10.1093/cmlj/kmx037.

[13] Talan, G., & Sharma, G. (2019). Doing well by doing good: A systematic review and research agenda for sustainable investment, Sustainability 11(2), 353. https://doi.org/10.3390/su11020353

[14] Tan, B.S., & Low, K.Y. (2017). Bitcoin – Its economics for financial reporting, Australian Accounting Review 27(2), 220–27. DOI: 10.1111/auar.12167.

[15] Tiwari, A.K.; Jana, R.K.; Das, D.; & Roubaud, D. (2018). Informational efficiency of Bitcoin – An extension, Economics lLeters 163: 106-109. https://doi.org/10.1016/j.econlet.2017.12.006

[16] Tranfield, D.; Denyer, D.; & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review, British Journal of Management 14: 207–22. https://doi.org/10.1111/1467-8551.00375

[17] Trimborn, S., & Härdle, W.K. (2016). CRIX: An index for blockchain based currencies, SFB 649 Discussion Paper 2016-021, Economic Risk, Berlin. DOI: 10.2139/ssrn.2800928

[18] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey of decentralized digital currencies, IEEE Communications Surveys & Tutorials 18(3): 2084–2123. DOI: 10.1109/COMST.2016.2535718.

[19] Urquhart, A. (2017). Price clustering in Bitcoin, Economics Letters 159: 145–48. DOI: 10.1016/j.econlet.2017.07.035.

[20] Weber, B. (2016). Bitcoin and the legitimacy crisis of money, Cambridge Journal of Economics 40(1), 17-41. https://doi.org/10.1093/cje/beu067

[21] Ying, W.; Jia, S.; & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group, International Journal of Information Management 39: 1-4. https://doi.org/10.1016/j.ijinfomgt.2017.10.004

[22] Yli-Huumo, J.; Ko, D., Choi, S.; Park, S.; & Smolander, K. (2016). Where is the current research on blockchain technology? A systematic review, PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journalpone.0163477

[23] Zimmer, Z. (2017). Bitcoin and Potosi silver: Historical perspective on cryptocurrency, Technology and Culture 58(2), 307-334. DOI: 10.1353/tech.2017.0038.

[24] Zohar, A. (2015). Bitcoin: Under the hood, Communications of the ACM 58(9): 104–13. DOI: 10.1145/2701411

[25] Malik, V. (2016). The history and the future of Bitcoin. Praha: Bankovní institut vysoká škola Praha.

[26] Xue, T., Yuan, Y., & Wang, C. (2018, June). An Approach for Evaluating User Participation in Bitcoin. In 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC) (pp. 858-864). IEEE.

[27] McNally, S., Roche, J., & Caton, S. (2018, March). Predicting the price of bitcoin using machine learning. In 2018 26th euromicro international conference on parallel, distributed and network-based processing (PDP) (pp. 339-343). IEEE.

[28] Bisht, A., & Agarwal, P. (2017). Analysis of Bitcoin using Linear Regression and Data Mining Techniques. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Department of Computer Science and Engineering, SRM University Chennai India, 6(11).

[29] Jang, H., & Lee, J. (2017). An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information. Ieee Access, 6, 5427-5437.

[30] Shah, D., & Zhang, K. (2014, September). Bayesian regression and Bitcoin. In 2014 52nd annual Allerton conference on communication, control, and computing (Allerton) (pp. 409-414). IEEE.

[31] Velankar, S., Valecha, S., & Maji, S. (2018, February). Bitcoin price prediction using machine learning. In 2018 20th International Conference on Advanced Communication Technology (ICACT) (pp. 144-147). IEEE.

[32] Rane, P. V., & Dhage, S. N. (2019, March). Systematic erudition of bitcoin price prediction using machine learning techniques. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 594-598). IEEE.
[33] Mangla, N., Bhat, A., Avabratha, G., & Bhat, N. (2019). Bitcoin price prediction using machine learning. International Joutnal of Information and Computing Science, 6(5), 318-320.
[34] Vockathaler, B. (2015). The bitcoin boom: An in-depth analysis of the price of bitcoins.
[35] Hencic, A., & Gouriéroux, C. (2015). Noncausal autoregressive model in application to bitcoin/USD exchange rates. In Econometrics of risk (pp. 17-40). Springer, Cham.
[36] Jang, H., Lee, J., Ko, H., & Lee, W. (2018, August). Predicting bitcoin prices by using rolling window LSTM model. In Proceedings of KDD Data Science in Fintech Workshop (DSF) (pp. 1-9).
[37] Indera, N. I., Yassin, I. M., Zabidi, A., & Rizman, Z. I. (2017). Non-linear autoregressive with exogeneous input (NARX) Bitcoin price prediction model using PSO-optimized parameters and moving average technical indicators. Journal of fundamental and applied sciences, 9(3S), 791-808.
[38] Mern, J., Anderson, S., & Poothokaran, J. (2017). Using bitcoin ledger network data to predict the price of bitcoin. cs229. stanford. edu.
[39] Poyser, O. (2017). Exploring the determinants of Bitcoin's price: an application of Bayesian Structural Time Series. arXiv preprint arXiv:1706.01437.
[40] Sin, E., & Wang, L. (2017, July). Bitcoin price prediction using ensembles of neural networks. In 2017 13th International conference on natural computation, fuzzy systems, and knowledge discovery (ICNC-FSKD) (pp. 666-671). IEEE.
[41] Arulkumar, C. V., Jeyakumar, K., Malarmathi, M., & Shanmugapriya, T. (2012). Secure communication in unstructured P2P networks based on reputation management and self-certification. International Journal of Computer Applications, 15, 1-3.
[42] Arulkumar, V., & Vivekanandan, P. (2018). An intelligent technique for uniquely recognising face and finger image using learning vector quantisation (LVQ)-based template key generation. International Journal of Biomedical Engineering and Technology, 26(3-4), 237-249.
[43] Anandakumar, H., & Umamaheswari, K. (2017). Supervised machine learning techniques in cognitive radio networks during cooperative spectrum handovers. Cluster Computing, 20(2), 1505-1515.
[44] Al Kawasmi, E.; Arnautovic, E.; & Svetinovic, D. (2015). Bitcoin-based decentralized carbon emission trading infrastructure model, Systems Engineering 18(2), 115-130. DOI: 10.1002/sys.21291 Alabi, K. (2017).
[45] Digital blockchain networks appear to be following Metcalfe's law, Electronic Commerce Research and Application 24(July 2017): 23-29. https://doi.org/10.1016/j.elerap.2017.06.003
[46] Albuquerque, B.S. de; & Callado, M. de C. (2015). Understanding Bitcoins: Facts and questions, Revista Brasileira de Economia 69(1): 3–16. DOI: 10.5935/0034-7140.20150001
[47] Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. The Journal of Economic Perspectives, 29(2), 213-238.
[48] Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. Hastings Sci. & Tech. LJ, 4, 159
[49] Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. Scientific reports, 3, 3415.
[50] Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (Vol. 2013).
[51] Muhammad, M., Muhammad, M.R. and Mohammed Khalil, M, (2013) Towards Shari'ah Compliant E-Commerce Transactions: A Review of Amazon.com, Middle-East Journal of Scientific Research, 15(9), 1229-1236
[52] Reid,F. and Harrigan,M., "An analysis of anonymity in the Bitcoin system," in Privacy, security, risk and trust (PASSAT), 2011 IEEE Third Internatiojn Conference on Social Computing (SOCIALCOM). IEEE, 2011, pp. 1318- 1326.
[53] Ron D., Shamir A. (2013) Quantitative Analysis of the Full Bitcoin Transaction Graph. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg
[54] Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal (No. w19747). National Bureau of Economic Research
[55] Androulaki E., Karame G.O., Roeschlin M., Scherer T., Capkun S. (2013) Evaluating User Privacy in Bitcoin. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg