BLOCKCHAIN & CRYPTOCURRENCY

Amey Deshpande ,Sujata Patil
Dept.Master of Computer Application
Trinity Academy of Engineering
Pune, India

Abstract— The paper's recognition of the emerging phenomenon of cryptocurrencies. The rise of cryptocurrencies' value on the market and the growing recognition around the arena open some demanding situations and concerns for business and commercial economics. The studies changed realized by way of the technique description, literature evaluation, and carried out research. This paper discusses the primary developments in the academic studies related to the Present Scenario of Cryptocurrency, a short overview of Cryptocurrency, cryptocurrencies through market capitalization, Cryptocurrencies Trending in Asia, Cryptocurrency in India, Cryptocurrency Exchanges, and cryptocurrency rules internationally.

Keywords: Cryptocurrency, Bitcoin, Ethereum, Ripple, Virtual Currency, Blockchain *, Cyber Security, Blockchain Wallets, Distributed Ledger.

INTRODUCTION

As a rising decentralized structure and distributed computing paradigm underlying Bitcoin and different cryptocurrencies, blockchain has attracted extensive attention in each study and application in recent years. Cryptocurrencies have transpired as one of the trending economic software structures. [3] Blockchain, the center concept or the electricity behind the fulfillment of Bitcoin is one of the maximum trending and not unusual subjects for virtual forex in recent times. The blockchain serves as a public ledger and transactions stored using this technique are almost impossible to tamper with. Blockchain and its use are not best restricted to cryptocurrency however in numerous different fields as properly. [1]

LITERATURE REVIEW

1) [7] At the center of the economic common sense of cryptocurrencies lies the hassle of surmounting the double-spending hassle, which poses accounting and duty challenges that effective cryptocurrencies have sought to conquer. This discussion paper evaluates the salient literature to be able to better inform academic and practitioner inquiries on the double-spending issues in cryptocurrencies. [10] The U.S. Has approximately 1,600 cryptocurrencies. No cryptocurrency is certified to be known as money due to the fact none has been specified via the U.S. Government as being felony tender. Cryptocurrencies are called virtual currencies because they possess some of the traits of cash. In this text, three issues related to cryptocurrencies are analyzed. First, bitcoins are considered, because they are the primary cryptocurrency. Second, an evaluation of the processes the Federal Reserve and the principal financial institution of Sweden are going through to evaluate the possibility of issuing a few no longer-but-fully-described new forms of electronic forex. Third, an examination of the viability of blockchain, which became brought as an inner aspect of Bitcoin, as a successful stand-alone technology.

2) this paper is prompted by using speculation that the lengthy-time period value of a cryptocurrency is determined with the aid of its future use as cash. For a cryptocurrency to be used as a medium of price, it has to fulfill three impartial functions: a medium of change, a unit of account, and a store of value. Currently, cryptocurrencies are held for funding purposes in place of being used for transactions and for that reason as a medium of change. For cryptocurrency to emerge as extensively adopted as a method of price, it first needs to go through a very volatile duration due to the fact speculative investors see long-run destiny costs within the cryptocurrency.[6] Cryptocurrencies, along with Bitcoin, were an essential component in some monetary activities. For instance, Bitcoin is the main payment approach for ransomware attackers and retailers on the Darknet. It is therefore beneficial to understand the functions of cryptocurrencies and their monetary implications. In this study, we use bitcoin, Ether, and XRP, the three cryptocurrencies with the highest marketplace values as of this writing, in addition to Libra, which is impending and topical, as examples to investigate their functions. Specifically, we argue that these cryptocurrencies are extraordinary due to variations in the following elements: the identity management of their ledger writers, their consensus algorithms, and their coin supply. We discuss how these elementsdetermine cryptocurrency performance, which includes safety, privacy, and economic influence.

RESEARCH METHODOLOGY

This paper uses the handiest secondary data that has been accumulated from the Web of Science Core Collection (WOS), Science Citation Index Expanded (SCI-EXPANDED), Social Sciences Citation Index (SSCI), Emerging Sources Citation Index (ESCI) and refers to various sources such as newspaper articles, websites, finance reports, and World Bank report.

OBJECTIVES OF THE STUDY

a) To understand the concept of cryptocurrency,

b) To study the advantages and drawbacks of cryptocurrency

c) To analyze the legal status, challenges, and opportunities of cryptocurrency.

CRYPTOCURRENCY: A BRIEF OVERVIEW

Blockchain

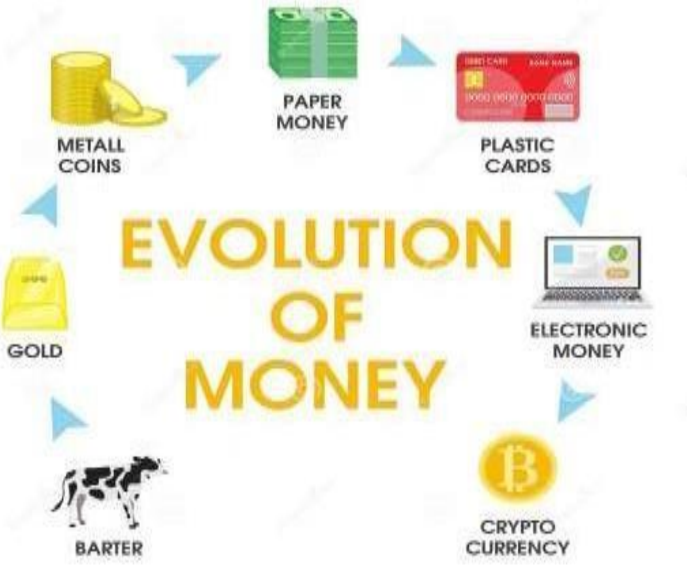
The blockchain is the decentralized allotted ledger machine used to report statistics transactions throughout multiple computers. In other phrases, it's miles an encrypted chain of facts held over an allotted network with an unalterable timestamp. It won recognition due to its ability to keep any virtual asset or transaction no matter the enterprise.

Cryptocurrency

Cryptocurrency is decentralized digital cash, based on blockchain technology. You may be familiar with the most popular versions, Bitcoin and Ethereum, but there are more than 5,000 different cryptocurrencies in movement, in keeping with Coin Lore. You can use crypto to shop for ordinary goods and services, although many humans put money into cryptocurrencies as they could in different belongings, like shares or precious metals. While cryptocurrency is a singular and interesting asset elegance, buying it may be volatile as you must take on an honest amount of studies to recognize how every system works. (Kate Ashford and John Schmidt,2020).

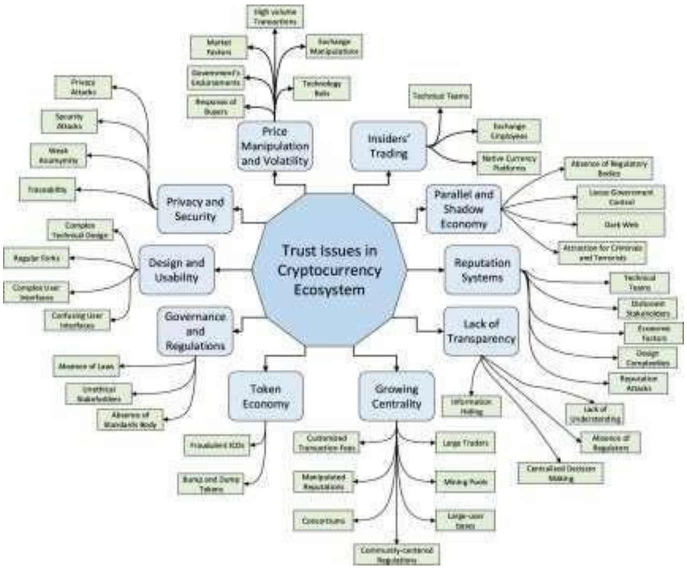
Types of Cryptocurrencies

There are three big types of cryptocurrencies - Bitcoin, altcoins, and tokens. Bitcoin is self-explanatory - it's the crypto coin that everyone usually talks about. Altcoins are usually derivatives of Bitcoin, but there are lots of standalone coins, too. Finally, tokens are broadly speaking used for dApps.[26]



Cryptocurrency Ecosystem

The current growth inside the blockchain-based cryptocurrency environment has been attracting researchers, developers, investors, regulators, and speculators to expand new economic and enterprise models for change, funding, and taxation. Currently, the cryptocurrency the atmosphere is immature with multifaceted agree with issues in any respect degrees from technology providers to customers and governments.



BEST CRYPTOCURRENCIES BY MARKET CAPITALIZATION
These are the 10 biggest trading cryptocurrencies by
Using the marketplace capitalization as tracked through CoinMarketCap, a cryptocurrency statistics, and analytics issuer

Table 1: Cryptocurrencies by Market Capitalization

Cryptocurrency	Market Capitalization
Bitcoin	$ 1 trillion
Ethereum	$427.0 billion
Binance Coin	$87.9 billion
Solana(SOL)	$87.7 billion
XRP(XRP)	$33.6 billion
Dogecoin(DOGE)	$30.2 billion
Cardano	$22.4 billion
Avalanche(AVAX)	$19.9 billion
Toncoin(TON)	$18.6 billion
Shiba Inu(SHIB)	$17.1 billion

Source:
https://www.usatoday.com/

Data current as of April 2, 2024.

Top 5 Cryptocurrencies of 2023, From Bitcoin to Dogecoin, cryptocurrencies have seen a significant jump in popularity and adoption in 2023.

.

Bitcoin (BTC): Bitcoin continued to be the most popular and widely accepted cryptocurrency. It's often seen as digital gold and is used for various transactions and investments.

Ethereum (ETH): Ethereum is another major cryptocurrency known for its smart contract functionality, which allows developers to create decentralized applications (dApps) on its blockchain.

Binance Coin (BNB): Binance Coin is the native cryptocurrency of the Binance exchange, one of the largest cryptocurrency exchanges in the world. It's used for various purposes on the Binance platform, including trading fee discounts.

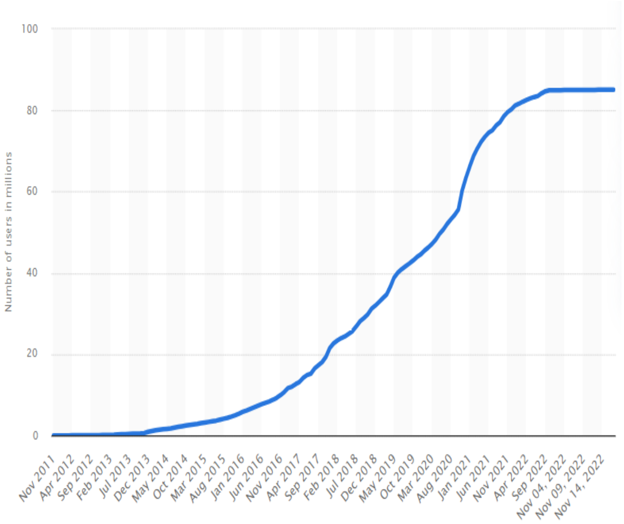
Solana (SOL): Solana is a cryptocurrency known for its fast transaction speeds and low fees. It's often used for decentralized finance (DeFi) applications and has gained popularity for its scalability.

Dogecoin (DOGE): XRP, created by Ripple, is a global payments network designed to be an alternative to the Society for Worldwide Interbank Financial Telecommunications. SWIFT is the global system banks and other financial institutions use to transfer money. But Ripple claims its technology is faster, cheaper, and more transparent than the SWIFT system.

Cryptocurrency Users Statistics and Cryptocurrency Demographics

A blockchain wallet, or cryptocurrency wallet, is a device, medium, or other application or service that can shop your cryptocurrency. This wallet, not handiest stores your cryptocurrency statistics but also encrypts the information and most effectively lets you log in together with your credentials to facilitate a clever settlement, crypto transaction, or other legally binding transaction. Almost 70 million people use a blockchain wallet internationally. About a third of Nigerians use cryptocurrency, while 1 in 5 in Vietnam and the Philippines do.

Figure 5: Number of Blockchain wallet users worldwide from November 2011 to November 17, 2022 (In millions)



TOP 10 CRYPTOCURRENCIES TRENDING IN ASIA

Asia is emerging as considered one of the biggest crypto markets in the international.

With it is the house of India and China, the most populous international locations. It is primed to grow to be the chief within the crypto international. Asia has been the primary marketplace for many cryptos and exchanges. CoinMarketCap, the largest destination online for crypto costs, in a tweet, gave an overview of the top 10 cryptos in Asia.

1. Xenon Pay II (X2P)
2. MoonStar (MOONSTAR)
3. IRON Titanium Token (TITAN)
4. SHIBA INU (SHIBA)
5. Mozart Finance (MELODY)
6. Bitcoin (BTC)
7. Safe Energy (ENERGYX)
8. Keep Network (KEEP)
9. SafeMoon (SAFEMOON)
10. Baby Doge Coin (BabyDoge)

CRYPTOCURRENCY IN INDIA

Cryptocurrency is a recent and significant innovation in the monetary industry. The purpose is to provide forex that isn't tied, created, or sponsored by using a central authority. Cryptocurrency uses blockchain generation as a monetary platform. The cryptocurrency adoption degree has improved, and the market has grown dramatically[2] Though India began regularly buying and selling bitcoin as early as 2015, the cryptocurrency made its real debut as fiat cash in November 2016 whilst the Modi-led government demonetized 86 percent of paper foreign money. [5] As in line with facts from blockchain analytics company Chainalysis, Indian investments in the cryptocurrency have surged to US$250 billion in 2022, driven by a shift inside the considering young traders – shifting far away from gold and other precious metals. Another motive is the

safety and transparency provided by using this technology. According to a record, over 10 million crypto traders have been added using India in 2022. This is noteworthy in mild speculation that the federal authorities plan to impose a ban on using cryptocurrency. However, nothing may be stated conclusively except the law regulating digital forex is passed. [9] Cryptocurrencies draw a variety of attention from investors, entrepreneurs, regulators, and most people. Many current public discussions of cryptocurrencies were brought on with the aid of the substantial adjustments of their expenses, claims that the market for cryptocurrencies is a bubble with no fundamental value, and also worries approximately evasion of regulatory and criminal oversight [11]

CRYPTOCURRENCY REGULATIONS ACROSS THE WORLD

Cryptocurrency has been here for a long time now. However, its mainstream adoption has boosted lately with 2022 being a remarkable year to add to its significance. But 2023 is a major push as countries across the globe have tried accepting cryptocurrency in some form or the other. Similarly, these countries have also been working on cryptocurrency regulations to govern the process of exchanging through crypto. We still have yet to witness international regulations on cryptocurrency. However, looking at the evolving landscape of crypto, it is quite evident that we may witness it soon. Today, we will learn about different countries that have managed to set government regulations on cryptocurrency.

Cryptocurrency Regulations in India

While there have been signs and symptoms in 2017 and 2018 that India was thinking about much less prohibitive cryptocurrency policies, the latest reviews suggest a trade of course. In July 2019, an inter-ministerial committee advocated a blanket ban on cryptocurrencies except for proposed reliable digital foreign money. The leaked, alleged draft invoice counseled prison time for folks who “mine, generate, preserve, sell, deal in, difficulty, transfer, dispose of, or use cryptocurrency inside the territory of India.” Although that draft bill did not make it to the parliament floor, India’s aversion to cryptocurrency maintains and, in overdue 2021, leaks suggested that the government was drafting a new invoice to ban cryptocurrency buying and selling. While it has come down tough on cryptocurrency from a regulatory attitude, India’s authorities have stated that it is open to exploring the ability of blockchain generation to enhance its monetary services industry [8]

THE BENEFITS THAT CRYPTOCURRENCIES OFFER OVER FIAT MONEY ARE SEVERAL

A cryptocurrency or crypto/virtual asset is a truly digital form of cash that exists only digitally.

The foremost difference between crypto and the virtual cash that we already use on each daily foundation (credit score/debit cards, e-banking, etc.) is that a cryptocurrency is not issued by way of any government or bank, is specifically decentralized and is primarily based on blockchain technology

CRYPTOCURRENCY SECURITY

While nonetheless no longer completely understood by the general public the world over, it's miles important to recognize that many banks, governments, and global businesses are privy to cryptocurrencies, and they're analyzing and evaluating their use and emergence as a feasible currency on an ongoing basis. While the Bitcoin we recognize nowadays turned into a built-in

the evidence-of-work principle that transactions may be securely processed on a decentralized peer-to-peer network, without the want for a primary series group, the mining and transaction strategies are not cozy. In truth, conspiring participants can impose upon the issues discovered within the process. Here are five key protection concerns that can result in probably dangerous assaults and threats with using cryptocurrencies:

- Selfish Mining
- Double Spending
- Wallet Software/Distributed Denials of Service Attacks
- Acquiring Greater Than 50% Computing Power
- Timejacking

A. Bitcoin essentials

In his now-famous work, Satoshi Nakamoto showed a solution to the problems that the implementation and usability of digital currency faced, especially the double-spending problem [14]. While the true identity of Nakamoto is a point of speculation, what is known is that until 2010 he remained active on the Bitcoin project, and then he stepped back and gave the project to the community for further development [13].

He proposed a system with P2P distributed timestamp server that serves as a generator of the computational proof of the chronological orders of transactions [12]. An electronic coin is defined as a chain of digital signatures. Each transaction is defined as a set of digitally signed hash of the previous transaction and the public key of the next owner. The private key is used

for signing the transaction, and the public key is used for verification of the transaction, as shown in Fig.1 [14]. The public key is kept in the wallet, which can be implemented in software, hardware, or online.

The Bitcoin ledger is defined as a state transition system, consisting of a state that shows the ownership status of all existing bitcoins and a state transition function, in the form of transactions other than transactions. The output of the state transition function is a new state [15]. The results of this process are state changes of the sender and recipient if the sender has enough bitcoins to make a transaction or an error, otherwise.

B. Bitcoin transactions

Each transaction is determined with its hash value representing a transaction identifier and a set of inputs and outputs. Each output of the transaction can only be used once as an input in the entire blockchain [13]. The attempt to reference the same output twice leads to the double-spending problem and is forbidden in the network. If the output of the transaction hasn't been referenced before, it is called an unspent transaction output (UTXO), and if it has been referenced, it is called a spent transaction output (STXO). A transaction can have multiple inputs and only up to two outputs. Multiple inputs can be used to combine smaller amounts of coins being transferred, and outputs can be either an amount sent to the other party or the change that is sent back to send the sender [14].

Bitcoin distributed ledger describes all transactions and ownerships in the network. Every node in this P2P network keeps a copy of the ledger record [15]. If one user wants to send some amount of coins to another, he can do that by publicly announcing this transaction and it is up to the network to verify its correctness. However, a user can try to manipulate the network and issue more than one transaction of the same coin to different users (double-spending problem). Moreover, the same user can set up several instances to confirm his initial intent and thus perform a Sybil attack.

C. **Proof-of-work and blockchain**

These situations are prevented (or at least minimized) in the honest time stamp of it coin network by demanding a proof-of-work from each node that verifies the transaction. The nodes have to do some heavy computations to prove that they are valid members of the network. As long as the total computational power of the honest nodes is greater than the computational power of the attacker, the system will remain consistent and all legit transactions will occur [13], [15].

A set of transactions, together with the hash of the previous block and a nonce, declares a block. A timestamp server makes a hash of a block and publicly

announces it, thus proving that the data inside the block must have existed at the time of hashing. The timestamp server has to verify that the timestamp of the block is greater than the timestamp of the previous block in the chain and less than two hours into the future. These hashes are linked in a chain and this is called a blockchain, as shown in Fig. 2 [14]. The important property of the blockchain is that the transactions can be traced back at any time in history.

Figure 2**. The blockchain scheme**

The proof-of-work hashing scheme Bitcoin uses is similar to Hash cash [16] and based on the SHA-256 hash function [17]. The proof-of-work is done by incrementing a nonce in the block until the value is produced that has the required number of zero bits at the beginning of the block hash. Once it is done, it cannot be undone without repeating the computations

. If it is somehow changed by a malicious attacker, then all the following blocks would have invalid hashes. The rule is that the longest chain that has the majority consensus in the network is the correct one, so if the attacker wishes to change a block, he needs to have enough computational power to overcome the voting of the majority of honest nodes, thus entering the race problem.

The transactions within a block are hashed in the Merkle tree[19], [20]. A Merkle tree is a type of binary tree with many leaf nodes, and a root of the leaf nodes is a hash of its children. Any inconsistency in the tree will reflect somewhere in the chain, so the Merkle tree is vital for long-term maintainability [15]. This is done to free up the storage space needed to store the blockchain on the nodes. The current size of the Bitcoin blockchain is about 144.8 GB [21]. After the transactions are incorporated in a block and this block is verified, the network discards all hashes in a tree except the root hash included in the block header. Bitcoin introduced a Simplified Payment Verification (SPV), which doesn't require the nodes to keep a full record of transactions, but only a copy of the block headers of the longest chain [14].

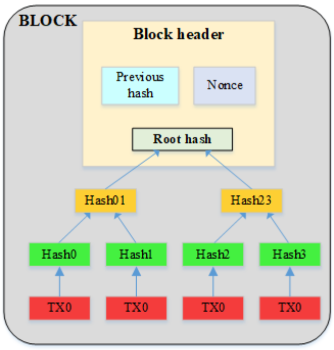


Figure 3. A Bitcoin block with hashed transactions into a Merkle tree

D. Bitcoin scalability problem

With a block size of 1MB, Bitcoin has severe scalability issues. The amount of transactions that can be supported with this block size is less than seven transactions per second (t p s) [21]. In comparison, the payment network Visa achieved 47,000 t p s during the 2013 holidays and currently averages hundreds of millions per day [22]. To achieve such a rate on a Bitcoin network with a 1MB block size, assuming that the transaction is 300 bytes in size, it would require a throughput of 8GB per Bitcoin block every ten minutes, which would lead to over 400TB of data per year [19]. This would highly centralize the Bitcoin network to support only those nodes with such storage capacities, and this is the very opposite of what Bitcoin and blockchain are intended for.

CONCLUSION

The emergence of Bitcoin has sparked a debate approximately its future and that of other cryptocurrencies. Despite Bitcoin's latest problems, its fulfillment is the reason that its 2009 release has inspired the creation of opportunity cryptocurrencies including Ethereum, Litecoin, and Ripple. A cryptocurrency that aspires to emerge as part of the mainstream financial device could have to fulfill very divergent criteria. While that possibility seems far off, there's little question that Bitcoin's success or failure in managing the demanding situations it faces may additionally determine the fortunes of different cryptocurrencies within the years in advance.[3]Cryptocurrency continues to be loaded in its early ranges and a few people are nevertheless skeptical about it but it's miles right here to live and has been tailored into our lives and will be currency utilized by everybody that is best a count of time. With the acceptance and how widely talked about it is the future of Cryptocurrency is sure to be bright.

ACKNOWLEDGMENTS

"We would like to express our deepest gratitude to all those who provided us with the possibility to complete this research paper.

We want to thank [Name], and [Title], for their valuable guidance and support throughout the research.

We also extend our thanks to [Institution], for providing us with the necessary resources and facilities.

Additionally, we acknowledge the contributions of our colleagues and peers who provided insightful comments and feedback.

Finally, we are grateful to our families for their understanding and encouragement during this research endeavor."

REFERENCES

[1] Akhtar et al (2019) "Potential of Blockchain Technology in Digital Currency: A Review," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 85-91, doi:10.1109/ICCWAMTIP47768.2019.9067546.

[2] Härdle, W. K., Harvey, C. R., & Reule, R. C. (2019, April 29). Understanding Cryptocurrencies Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3360304.

[3] AdamBaron(2019)https://www.investopedia.com/articles/forex/091013/future- cryptocurrency.asp

[4] BilalJafar(2021)https://www.financemagnates.com/cryptocurrency/news/top-5- cryptocurrencies-of-2021/

[5] Bradley Dunseith (2017) https://www.india-briefing.com/news/cryptocurrency- bitcoin-india-usage-regulation- 15343.html/.