IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 7.301

Volume 3, Issue 3, April 2023

Cryptocurrency: An Overview of its History, Technology and Future Prospects

Divya Sharma[1], Deepanshu Pant[2], Ashwani Kumar[3]
UG Students, Department of Computer Science and IT[1,2]
Assistant Professor, Department of Computer Science and IT[3]
Dronacharya College of Engineering, Gurgaon, India

Abstract: *Cryptocurrency has emerged as a novel form of digital currency that operates independently of traditional financial institutions. This research paper provides an overview of the history and technology behind cryptocurrencies, including the development of Bitcoin, the first and the most well-known cryptocurrency. We explore the decentralized nature of cryptocurrencies, their advantages and disadvantages, and the underlying blockchain technology that enables their secure operation. Additionally, we examine current and prospects for cryptocurrencies.*

Keywords: Cryptocurrency, Blockchain, Mining, Decentralized

I. INTRODUCTION

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units. However, serious limitations have become apparent. Decentralized organization of markets without trusted intermediaries can be very costly, and the volatility of the value of cryptocurrencies is a big obstacle to their becoming an alternative to legal tender. Cryptocurrency is stored in digital wallets. Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety. The emergence of Bitcoin in 2009 paved the way for the development of hundreds of other cryptocurrencies, each with its own unique features and characteristics. Cryptocurrencies are the first—and therefore most developed—application of blockchain technologies.

II. HISTORY

The cryptocurrency was first mentioned in the 1980s, more precisely in 1989. However, it was only in the early 1990s that cryptographic protocols, as well as software, began to be developed that would enable the creation of a truly decentralized digital currency. However, it was not until 2009 that the first cryptocurrency, Bitcoin, was created. Bitcoin was designed to be a decentralized form of digital currency that could operate without the need for traditional financial institutions. After the success of Bitcoin, many other cryptocurrencies have been introduced, such as Ethereum, Litecoin, Ripple, and many more. Each cryptocurrency has its unique features, but they all share the same basic concept of being decentralized and operating on a blockchain. The history of cryptocurrency is still evolving, and it remains to be seen how it will shape the future of finance and commerce.

III. ARCHITECTURE

Cryptocurrency is produced by an entire cryptocurrency system collectively, at a rate which is defined when the system is created, and which is publicly stated. In centralized banking and economic systems such as the US Federal Reserve System, corporate boards or governments control the supply of currency. In the case of cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate

DOI: 10.48175/IJARSCT-9232

entities which hold asset value measured in it. The underlying technical system upon which cryptocurrencies are based was created by Satoshi Nakamoto. Most cryptocurrencies are designed to gradually decrease the production of that currency, placing a cap on the total amount of that currency that will ever be in circulation. It uses different technologies of attaining the system. These are:

- **Blockchain** A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. he innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. This data structure inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain. Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.
- **Nodes** A node is a computer that connects to a cryptocurrency network. The node supports the cryptocurrency's network through either relaying transaction, validation, or hosting a copy of the blockchain. In terms of relaying transactions, each network computer (node) has a copy of the blockchain of the cryptocurrency it supports. When a transaction is made, the node creating the transaction broadcasts details of the transaction using encryption to other nodes throughout the node network so that the transaction (and every other transaction) is known.
- **Time Stamping** Cryptocurrencies use various timestamping schemes to "prove" the validity of transactions added to the blockchain ledger without the need for a trusted third party.The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and scrypt.
- **Mining** Bitcoin mining is the process by which new bitcoins are entered into circulation. It is also the way the network confirms new transactions and is a critical component of the blockchain ledger's maintenance and development. "Mining" is performed using sophisticated hardware that solves an extremely complex computational math problem. The first computer to find the solution to the problem receives the next block of bitcoins and the process begins again.
- **Gpu price rise** an increase in cryptocurrency mining increased the demand for graphics cards (GPU) in 2017. The computing power of GPUs makes them well-suited to generating hashes.
- **Wallets** A cryptocurrency wallet is a means of storing the public and private "keys" (address) or seed which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet.
- **Anonymity** Bitcoin is pseudonymous, rather than anonymous; the cryptocurrency in a wallet is not tied to a person, but rather to one or more specific keys (or "addresses"). Thereby, Bitcoin owners are not immediately identifiable, but all transactions are publicly available in the blockchain. Still, cryptocurrency exchanges are often required by law to collect the personal information of their users.

IV. ADVANTAGES OF CRYPTOCURRENCY

4.1 Protection from Inflation

Inflation has caused many currencies to urge their value to decline with time. At the time of its launch, almost every cryptocurrency is released with a tough and fast amount. The ASCII computer file specifies the quantity of any coin; there are only 21 million Bitcoins released within the planet. So, because the demand increases, its value will increase which might maintain with the market and, within the long run, prevent inflation.

4.2 Self-Governed and Managed

Governance and maintenance of any currency is also a serious factor for its development. The cryptocurrency transactions are stored by developers/miners on their hardware, which they get the transaction fee as a gift for doing so. Since the miners have become acquired it, they keep transaction records accurate and up-to-date, keeping the integrity of the cryptocurrency and also the records decentralized.

4.3 Decentralized

A major pro of cryptocurrencies is that they are mainly decentralized. Many cryptocurrencies are controlled by the developers using it and those who have a significant amount of the coin or by a corporation to develop it before it's released into the market. The decentralization helps keep the currency monopoly free and in restraint, so nobody organization can determine the flow and so the worth of the coin, which, in turn, will keep it stable and secure, unlike fiat currencies which are controlled by the Government.

4.4 Cost-Effective Mode of Transaction

One of the most uses of cryptocurrencies is to send money across borders. With the help of cryptocurrency, the transaction fees paid by a user are reduced to a negligible or zero amount. It does so by eliminating the need for third parties, like VISA or PayPal, to verify a transaction. It removes the requirement to pay any extra transaction fees.

4.5 Currency Exchanges Finish Smoothly

Cryptocurrency can be bought using many currencies rather like the US dollar, European euro, British unit of measurement, the Indian rupee, or Japanese yen. Varied cryptocurrency wallets and exchanges help convert one currency into another by trading in cryptocurrency, across different wallets, and by paying minimal transaction fees.

4.6 Secure and Private

Privacy and security have always been concerns for cryptocurrencies. The blockchain ledger relies on different mathematical puzzles, which are hard to decode. It makes cryptocurrency safer than ordinary electronic transactions. Cryptocurrencies are for better security and privacy, and they use pseudonyms that are unconnected to any user account or stored data that might be linked to a profile.

4.7 Easy Transfer of Funds

Cryptocurrencies have always kept themselves as an optimal solution for transactions. Transactions, whether international or domestic in cryptocurrencies, are lightning-fast. It will be because the verification requires little time to process as there are only some barriers to cross.

V. DISADVANTAGES OF CRYPTOCURRENCY

5.1 Illegal Transactions

Since the privacy and security of cryptocurrency transactions are high, it's hard for the government to trace down any user by their wallet address or keep tabs on their data. Bitcoin has been used as a mode of payment (exchanging money) during many illegal deals in the past, like buying drugs on the dark web. It has also been used by some people to convert their illicitly acquired money to hide its source, through a clean intermediary.

5.2 Risk of Data Loss

The developers wanted to make virtually untraceable ASCII documents, strong hacking defenses, and impenetrable authentication protocols. It would make it safer to position money in cryptocurrencies than physical cash or bank vaults. But if any user loses the private key to their wallet, there is no getting it back. The wallet will remain locked away along with the number of coins inside it. It might result in the loss of the user.

DOI: 10.48175/IJARSCT-9232

5.3 Power Lies in Few Hands

Although cryptocurrencies are known for their feature of being decentralized, the flow and amount of some currencies within the market are still controlled by their creators and some organizations. These holders can manipulate the coin for enormous swings in its price. Even hugely traded coins are at risk of these manipulations like Bitcoin, whose value doubled several times in 2017.

5.4 Buying NFTs with other Tokens

Some cryptocurrencies can only be traded in one or some fiat currencies. It forces the user to convert these currencies into one all told the most currencies, like Bitcoin or Ethereum first and then through other exchanges, to their desired currency. It can apply to just some cryptocurrencies. By doing this, the extra transaction fees are added within the method, costing unnecessary money.

5.5 No Refund or Cancellation

If there is a dispute between concerned parties, or if someone mistakenly sends funds to a wrong wallet address, the coin cannot be retrieved by the sender. It might be utilized by many folks to cheat others out of their money. Since there are no refunds, one can easily be created for a transaction whose product or services they never received.

5.6 High consumption of Energy

Mining cryptocurrencies require plenty of computational power and electricity input, making it highly energy intensive. The main culprit during this is often Bitcoin. Mining Bitcoin requires advanced computers and plenty of energy. One cannot do it on ordinary computers. Major Bitcoin miners are in countries like China that use coal to produce electricity. It has increased China’s carbon footprint tremendously.

5.7 Vulnerable to hacks

Although cryptocurrencies are very secure, exchanges don’t seem to be that secure. Most exchanges store the wallet data of users to figure their user ID correctly. This data is often stolen by hackers, giving them access to lots of accounts. After getting access, these hackers can efficiently transfer funds from those accounts. Some exchanges, like Bitfinex or Mt Gox, have been hacked within the past years, and Bitcoin has been stolen in thousands and countless US dollars. Most exchanges are highly secure nowadays, but there is always a possibility for a further hack.

VII. CURRENT AND FUTURE PROSPECTS OF CRYPTOCURRENCY

Despite the challenges facing cryptocurrencies, they continue to gain in popularity and adoption. Many major companies and financial institutions have begun to explore the potential of cryptocurrencies, and some have even begun to accept them as payment. Additionally, the development of new technologies, such as decentralized finance (DeFi) and non-fungible tokens (NFTs), are creating new opportunities for cryptocurrencies to disrupt traditional industries.

REFERENCES

[1]. Cryptocurrencies and Blockchain – worldbank eca economic update 2018
[2]. Andrew Miller, Arvind Narayanan, Edward Felton, Joseph Bonneau, Steve Goldfeder, “Bitcoin and Cryptocurrency Technologies”, 2016
[3]. The basics of Bitcoin and Blockchain, by Antony Lewis
[4]. https://academy.binance.com/en/articles/what-is-crypto-mining-and-how-does-it-work

DOI: 10.48175/IJARSCT-9232