*International Refereed Journal of Engineering and Science (IRJES)*
*ISSN (Online) 2319-183X, (Print) 2319-1821*
*Volume 13, Issue 2 (Mar.-Apr. 2024), PP. 11-18*

# History, Current, and Prospective of Bitcoin and Cryptocurrency

Prashant Awasthi
*IT Professional, Symbiosis Institute of Computer Studies and Research (Guest faculty)*

Murugaiyan Dhandapani
*IT Professional*

***Abstract-****A cryptocurrency is a sort of digital OR virtual money generated using encryption methods, in which records are preserved and transactions are authenticated by a decentralized system using encryption rather than a central authority. Cryptography is used to secure transactions in cryptocurrency. The first cryptocurrency was created in 2009 and is still the most well-known today: Bitcoin. Investing in cryptocurrencies for financial gain is a major draw. Apart from Bitcoin, there are multiple other cryptocurrencies like Ethereum, Litecoin, Ripple, Steller, Coinbase etc in the financial world. In 2023 and beyond, cryptocurrencies have the potential to drastically change how we utilize money. It is a sought alternative to conventional currencies due to its decentralization, transparency, affordable transaction costs, quick transactions, and global accessibility. The regulation of cryptocurrency assets was one of the primary agenda issues on the G20's financial track during India's presidency, and the group of finance ministers and central bank governors has already held discussions on reports from the IMF and FSB.*

Date of Submission: 09-03-2024 Date of acceptance: 23-03-2024

## I. CRYPTOCURRENCY INTRODUCTION

Cryptocurrencies is a form of electronic asset that is built on a network that covers many computers. They are distinct from governments and governing bodies because of their distributed structure. The name derives from the fact that all its exchanges are fully encrypted, thereby increasing their security. It is a decentralized means of payment, in contrast to traditional currencies, which are administered and regulated by a central organization. Payments made with bitcoin exist only as electronic files in a digital repository that provides specific transactions. Blockchain, a distributed public ledger, is used for saving information about digital currencies. Currency is kept in digital wallets. According to some scientists, blockchain technology is going to have an effect on sectors such as legal and financial services. Two benefits associated with cryptocurrencies are quicker and less expensive money transfers, and they are also autonomous networks without no single point of malfunction.

Mining is the practice of using powerful computers to solve incredibly complex issues with the aim to generate cryptocurrencies. The motivation for effectively finishing trades with the digital currency bitcoin usually involves some form of the necessary payments. Said in another context, trade in cryptocurrency usually contributes to the acceptance of brand-new ones into the global market. A digital coin has a finite supply and is occasionally equated to precious metals like silver as well as gold.

Developed in 2009, Bitcoin was the first cryptocurrency and continues the most famous today date. the digital currency is an online "digital currency" which enables for quick and easy untraceable payments without a requirement on a governing body. Despite being praised by some as the digital currency of the future, it is frequently criticized as a currency that is too unstable to invest in.


**Figure 1**: Bitcoin; **Figure 2**: Ethereum
**Sources: https://economictimes.indiatimes.com/**

**USAGE OF CRYPTOCURRENCY IN FINANCIAL INDUSTRY**

Cryptocurrency has grown in popularity among both consumers and corporations in recent years, which has made it a hot topic in the financial industry. The potential of cryptocurrencies and their impact on the banking industry are increasingly clear. In financial sector blockchain technology has developed a significant future and adaption. Even blockchain has use cases which will clearly resolve many problems and ideally benefit financial sector.

In financial industry blockchain technology is considered to save significant amount on transactions fees with improving transparency among all parties.

a) Access to Financial Services:
Cryptocurrencies have made it possible for anyone to obtain financial services even if they don't have access to or can only use limited banking services. This is particularly critical in developing countries where traditional financial services are typically in short supply. A rapid and easy method of sending money across borders without the involvement of middlemen is also being made available by cryptocurrencies.

b) Lower Transaction Costs: Another advantage of cryptocurrency for both individuals and companies is lower
transaction costs. To avoid using middlemen like banks or payment processors, this is done to enable transactions. Transaction costs have decreased, making it more affordable for businesses to accept cryptocurrency payments.

c) Faster Speed of Transaction Processing: Cryptocurrencies also provide faster transaction speeds than traditional financial systems. For businesses that must promptly pay suppliers or employees, the ability to complete transactions in minutes as opposed to days is tremendously helpful.

d) Security of Transactions: transactions based on cryptocurrencies provide greater financial transaction security. The basis of cryptocurrencies is blockchain technology, which is very secure and impossible to hack. Because of this, those who are concerned about the security of their financial transactions might utilize bitcoin as a more secure alternative.

e) Transparency: On the blockchain, each transaction is recorded and made available for public inspection. This provides people and organizations with a high level of accountability and transparency, which is essential in fields like finance and accounting.

**Moral Services on a Digital Currency ?**

Blockchain is a decentralized technology that powers cryptocurrency. Blockchain technology is the foundation of most cryptocurrencies. It is a networking protocol that enables computers to collaborate in order to maintain a shared, impenetrable record of transactions. Making sure that everyone can agree on the accurate copy of the historical ledger is the challenge in a blockchain network. People wouldn't be able to have confidence in the security of their possessions without a recognized method to validate transactions. There are various ways to achieve "consensus" on a blockchain network, but the two that are most frequently employed are called "proof of work" and "proof of stake."

**Proof of work** is one strategy for motivating users to contribute to the upkeep of a trustworthy historical record of who owns what on a network built on blockchain technology. Proof of work plays a significant role in the cryptocurrency discussion because Bitcoin makes use of it. Users are relied on to compile and submit blocks containing recent transactions for inclusion in the ledger, and the Bitcoin protocol compensates them for doing so successfully. Mining is the term for this action.

With a scenario many people attempt to submit blocks in order to compete for these incentives, but only one can be chosen for each new block of transactions. Users of Bitcoin must solve a challenging puzzle that consumes a significant amount of energy and computer resources in order to determine who receives the reward. The "work" in proof of work is the solution to this puzzle. The Bitcoin rewards for successful miners more than covers the associated expenses. However, the extremely high up-front cost also serves as a deterrent for dishonest players. The payoff may not be worth the danger of tampering with the records and having your submission rejected, which would mean losing the opportunity to form a block. Attempting to alter the historical record in this case would have cost a lot of money in energy costs. Proof of work's ultimate objective is to increase the rewards of following the rules rather than attempting to breach them.

**Proof of stake** is another method of gaining agreement on the reliability of the historical record of transactions on a blockchain. It does away with mining in favor of a method called staking, where users stake some of their own cryptocurrency holdings to guarantee the accuracy of their work while verifying new transactions. Cardano, Solana, and Ethereum (which is in the act of switching from proof of work) are some of the cryptocurrencies that use proof of stake.

Proof of stake systems and proof of work protocols are similar in that both require on users to gather and submit fresh transactions. But they have a different strategy for rewarding truthful conduct among those involved in that process. It basically means that everyone who wants to add fresh blocks of data to the record has to risk some money. In numerous situations, raising your bet will boost your chances of getting a new block and the goodies that come with it. People that provide false information risk losing some of the money they have staked.

**USE OF BLOCKCHAIN TECHNOLOGY IN CRYPTOCURRENCY**

Highly secure cryptocurrency like Bitcoin works on a peer-to-peer, or P2P, foundation, removing the requirement for a middleman (such as a financial institution or card company) while offering a low price for transactions. t's swift and totally open, for instance, each Cryptocurrency payment you make goes in a publicly available record. It isn't convertible . Since blockchain transactions are permanent, this is a considerably reduced risk for fraud and more safety for your money. Exchanges such as The Wazir which offers investors an environment that is secure and safe, enables anyone to make trade bitcoins.

This study shows how blockchain will pivotal role in data and security of the software in various industries and functions. Key components of blockchain technology are:

a) **Distributed ledger:** The shared ledger and its permanent history of activities were visible to all members of the network. Actions are documented just once on this public record, decreasing the repetition of work that is typical of traditional business systems.

b) **Immutable records:** When an activity is signed into a public ledger, none of the participants may modify nor interfere with it. If a mistake occurs in the transaction document, an additional one must be submitted to resolve this problem, so both of those transactions are now accessible.

c) **Smart contracts:** A set of instructions referred to as a smart contract, which is archived on the distributed ledger and performed autonomously to speed up operations. A smart contract may define criteria for corporate debt payments, the exchange of journey coverage, and numerous other things.

The widespread use of the blockchain technology has drawn blockchain programmers and technologists due to its ability to revolutionize the way companies and industries work. We may start by learning about the many kinds of digital currencies that exist on the market.

a) **Blockchain under Public methods :** Because of the unrestricted non-restrictive character of this distributed digital ledger, anyone having a web connection can participate in the blockchain network. Such a blockchain is primarily utilized for mining and trading cryptocurrency. In addition, it maintains its trust of the whole membership as everyone on the network is inspired to make a contribution in improving the public network richer. the digital currency is the first version of a blockchain which has made transactions achievable for all individuals. Just few of instances of public the ledgers are Ethereum and Litcoin.

b) **Blockchain under Private methods :** Private blockchains function within restricted networks and are permission-based, as opposed to public ledgers. This kind of blockchain is mostly used inside businesses where only a small number of employees are part of the blockchain network. Organizations and companies who wish to use bitcoin only for purposes that are internal are among the most suitable applicants. The key difference between both types of platforms is that whereas private has limitations to certain types of viewers, public is extremely accessible. In addition, because only one person is liable for maintaining the network, a blockchain that is private is more centralized. Samples of private platforms are the Corda, the fabric of Hyperledger, Hyperledger Sawtooth, and Hyperledger Corda.

c) **Blockchain under Consortium methods :** Consortium blockchains, also known as federated blockchains, tend to be suitable for businesses which need blockchains that are private as well as public. This form involves multiple central leaders, or more precisely, various groups which provide access to chosen nodes for the goals of consuming, composing, and inspecting the blockchain. The decentralized nature is maintained since control does not become reinforced to a single authority. Examples of those platforms are the IBM Corporation Food Trust as well as the Energy Web Foundation.

**IS CRYPTOCURRENCY SAFE?**

When compared to equities and government bonds, bitcoin has brought up questions regarding the reliability and stability of transactions. The need for volatility and adaptability in large scale asset classes are significant characteristics of this type of asset. Basically, trading in digital currencies serves as a based on risk behavior due to which the asset class's value can vary considerably and particularly subject to scams or various

forms of misconduct.

Cryptocurrency has been gaining lot of mainstream adaptions in all countries, but many aspects of cryptocurrency remain unregulated – or navigating towards regulations. With questions around regulations which makes cryptocurrency significantly volatile.

Legal Protections with cryptocurrency payments is not very comprehensive. For instance, you might always be responsible for fraudulent purchases made against your name or association and you might not be able to recover the money.

Cryptocurrency Scams are very common and exposed to security threats and ransomware with compromised personal information. In case of cyberattack you might be asked to pay in cryptocurrency.

Most of the cryptocurrency transactions are performed on the blockchain, which is most secure, safe and no editable. Due to this nature of technology transactions performed on the blockchain are not reversible. To extent this is most prominent feature of blockchain technology to keep the transactions secure.

Owing huge losses for investors resulting from deception, malware, risks, and fluctuation, bitcoins have developed an image for being hazardous assets. While the ledger system and its fundamental crypto are often safe. Despite conventional currencies, which get backing by governments or economic individuals, bitcoins cannot be backed by the corporate or individual entities. In the USA, the European continent, and Asia in particular, bitcoin is still allowed. Bitcoin is characterized as legal property throughout the region of the Asia-Pacific via the payments act of Japan.
The country's cryptocurrency exchanges are required to gather customer information and information regarding wire transfers. According to reports, India is developing a framework for cryptocurrencies, but until it is implemented, cryptocurrencies are not yet forbidden.

**TYPE OF CRYPTOCURRENCIES AND MARKET CAPITALIZATIONS**

Because blockchain technology is open source, any software developer can use its original source code to build new things. The developers have already done it. The number of cryptocurrencies is thought to exceed 20,000.

Here are some of the top cryptocurrencies among the list

- Bitcoin (CRYPTO: BTC)
- Ethereum (CRYPTO: ETH)
- Tether (CRYPTO: USDT)
- Binance Coin (CRYPTO: BNB)
- USD Coin (CRYPTO: USDC)
- XRP (CRYPTO: XRP)
- Terra (CRYPTO: LUNA)
- Solana (CRYPTO:SOL)
- Cardano (CRYPTO: ADA)
- Avalanche (CRYPTO: AVAX)

Market capitalization of different cryptocurrencies as highlighted:

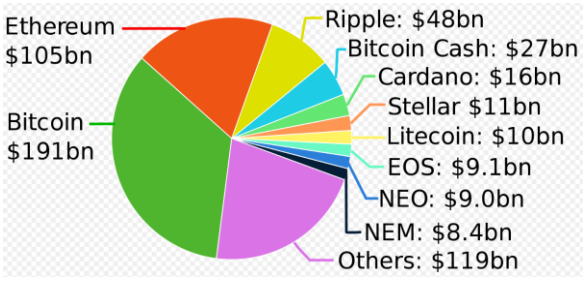



**Figure** 3: Market capitalizations of cryptocurrencies
**Sources: https://en.wikipedia.org/wiki/List_of_cryptocurrencies**

**HOW TO PURCHASE CRYPTOCURRENCIES SAFELY?**

To purchase cryptocurrencies securely, there are three steps involved:

**1. Choose the trading platform**

- The initial move is selecting a platform for trading. Usually, you have a choice to utilize a conventional broker or an exchange for digital currencies.
- **Regular brokers:** They include virtual brokers that handle the acquisition and disposal of securities, bonds, and ETFs, which in addition to methods to purchase and sell cryptocurrency. These firms provide an online trading interface and offer reduced rates for trading.
- **Crypto Exchanges** There have been more than 500 cryptocurrency trading platforms which function similarly as stock transfers, enabling traders to buy or sell digital currencies such as Bitcoin, Ethereum, or Tether, and other. These kinds of platforms function on online platforms such as smart phones or using workstation amenities in an identical way that e-brokers do, generating asset-based payments.

Before selecting a selecting trading platform, always compare their fees, security features, storage and withdrawal options.

**2. Adding money to your account for trading**

After choosing the trading platform, the next phase is to set up the account so you can start trading. Many bitcoin exchanges enable users to buy digital currencies using conventional currencies such as the American Dollar, the British Pound, and Euro utilizing credit or debit card transactions.
Various card issuers also prevent the virtual currency bitcoin purchases since considered insecure purchasing coin using credit card .

Due to the unprecedented volatility of digital currencies, it wouldn't be recommended to go into credit or risk paying expensive payment card fees.
In addition, certain systems will accept wire transfers and ACH transfers. Each platform has its own set of authorized payment methods and deposit and withdrawal processing timeframes. Fees are also a vital issue. These may include transaction fees for deposits and withdrawals, as well as trading expenses. You should investigate the various costs charged by various platforms.

**3. Making a digital currency purchase**

Users can buy, sell, and hold cryptocurrencies through well-known payment systems like PayPal, Cash App, and Venmo App. Cryptocurrency is kept in a digital wallet. There are numerous distinct wallet manufacturers. To make trading simpler, cryptocurrency exchanges could include a wallet on their sites.

**HOW TO STORE CRYPTOCURRENCY(Muru)**

Cryptocurrency storage requires a wallet. A cryptocurrency wallet is a piece of hardware or software that stores all of your digital assets, private keys, and public wallet addresses in one location.
And there several storage methods that can be followed up for crypto wallet.

- Cryptocurrency Storage at an Exchange
- Cold Storage for Cryptocurrency
- Keeping Bitcoin in a Hot Wallet
- Keeping Bitcoin in a Paper Wallet

| Fact | Exchange | Cold | Hot | Paper |
|---|---|---|---|---|
| How does it work? | Your cryptocurrency is stored by a third party, such as a cryptocurrency exchange. | Offline crypto storage hardware | Online cryptocurrency storage application | Private cryptographic keys are physically stored. |
| Advantages | The most straightforward and easiest option | Maximum degree of protection | Simplicity and usage. | Portable bitcoin storing free |
| Disadvantage | The potential danger of entrusting crypto to an outside organization | Gadget price and discomfort | The privacy risk of retaining bitcoins publicly | Trouble and the risk of losing a person's money. |
| Cost | Free | 50 to 150$ | Free | Free |

**WHAT CAN WE PURCHASE USING CRYPTOCURRENCY?**

Cryptocurrency has gone mainstream and with large adaption across various industries it has opened various opportunities for individuals to purchase goods and services using cryptocurrency.

Usage in Technology and e-commerce platform: With innovation at the center of technology various companies have used blockchain technology to sell products and goods. Companies like Microsoft, AT&T and Tesla are adapters to enable the use of bitcoin to purchase goods.

Media and communication, cryptocurrency media outlets accept cryptocurrency.

Insurance companies have slowly transitioned with adaption of cryptocurrency with acceptance of payments in cryptocurrency. For instance, the Swiss insurer AXA stated in April 2021[10] that it has started taking bitcoin as a form of payment for all its insurance lines, except for life insurance (owing to regulatory concerns).
Auto insurance "pay-per-mile" distributor, Metro mile also accepts bitcoin for premium payments.

**BITCOINS CRIME AND CRYPTOCURRENCY SCAM**
However, cryptocurrency criminality has been on rising. Hackers may set up fake exchangers or use the identity of legitimate virtual currency merchants to deceive consumers into providing over money. Another kind of cryptocurrency scam involves deceptive pitches for bitcoin-based individual plans for retiring.
. Among the cryptocurrency frauds are:

- **Bogus websites**: Fraud websites with fake evaluations and bitcoins jargon that promise enormous, guaranteed develops as long as you keep trying to invest.

**e**.g., The well-known play-to-earn game Axie Infinity was breached in July 2022. The attack is thought to have been caused via a fraudulent job offer and was connected to Lazarus, a well-known cybercrime organization.
The network was taken over by hackers, who made off with $600 million. $30 million was eventually recovered by the US authorities, and Sky Mavis paid out players' losses.

- **Virtual Ponzi schemes**: Cybercriminals trading in virtual currencies provide fake investment possibilities and fraudulent returns by paying former investors with funds from fresh investors.
-

E.g., Ponzi scheme that was promoted as a cryptocurrency worth investing in is the OneCoin Crypto Scam. It was run by Ruja Ignatova from Bulgaria, also known as the Cryptoqueen, who became one of the most famous scammers. Her tale reads like a movie script because it is so absurd.

She disappeared in 2017 after defrauding investors of $4 billion, never to be seen again. She is one of the largest cryptocurrency scammers, and she is currently on the FBI's most wanted list with $100,000 reward to help find her.

- **Romance Scams:** According to an increase in online dating scams that the FBI is warning against, scammers are luring people they meet through dating apps or social media to invest in or trade virtual currencies.
- **"Celebrity" endorsements:** Online scammers pose as wealthy or well-known figures, promising to increase your investment in a virtual currency while really stealing what you contribute. They may even use messaging apps or chat forums to disseminate rumors about a well-known businessperson endorsing a specific cryptocurrency. The crooks sell their stake after convincing investors to buy and raising the price, causing the currency's value to decline.

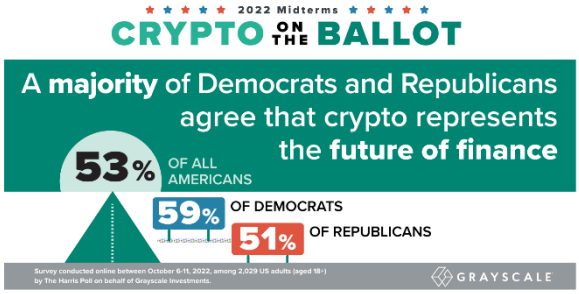
e.g., **SQUID token scam** was promoted as a token that would give access to a play-to-earn game and was modeled on the popular Netflix TV show Squid Game. The relationship gave the token the appearance of being trustworthy even if it wasn't related to Squid Game. The TV show's followers rushed to buy it.
People were tripling and even doubling their initial investments as a result of the token's sharp increase in value. They discovered, however, that they were unable to trade their SQUID tokens.
The $3.36 million in SQUID token investments made by the public vanished all at once. The token practically lost all of its value in a matter of minutes.
As you can see, there are numerous scams within the cryptocurrency ecosystem. Unfortunately, anyone can experience it. Do your homework to try to avoid them and carefully invest your funds.

**FUTURE OF CRYPTOCURRENCY**

Bitcoins are going to be a great phenomenon. To start making investments, you'll require a trustworthy crypto exchange, such as Wazir and on which you are able to purchase, sell, and trade cryptocurrency such as Bitcoin, Ethereum, Tron, and more. The accounting firm Deloitte, a total of 2300 US businesses may have adopted bitcoins as a way of payment from late 2020, rendering it a popular asset for everyday people to gain access to.

The price volatility of cryptocurrencies sold on open markets makes proper price monitoring necessary for investing. For instance, the value of Bitcoin has fluctuated sharply, rising to almost $65,000 in November 2021 before falling to slightly more than $20,000 a year and a half later. Because of this, many people think of cryptocurrency as a passing trend or speculative bubble.

More than half of Americans (53%) agree, according to a Grayscale survey, that "cryptocurrencies are the future of finance," including 59% of Democrats and 51% of Republicans. Democrats and Republicans agree that cryptocurrency regulation is necessary and that the topic is one that is becoming more and more important. Additionally, Americans view cryptocurrencies as a way to promote economic justice.




No one can predict the future of AI technology as it has been continuously evolving from many years

**REFERENCES:**

[1]. Tom Polansek (May 02 2016), "CME, ICE prepare pricing data that could boost bitcoin" Reuters, https://www.reuters.com/article/us-cme-group-bitcoin-idUSKCN0XT1G1/
[2]. Jake Frankenfield (Aug 29 2023), "Cryptocurrency Explained with Pros and Cons for Investment" https://www.investopedia.com/terms/c/cryptocurrency.asp
[3]. (Mar 27 2020), "Data Validation and Verification Using Blockchain in a Clinical Trial for Breast Cancer" Journal of Medical Internet Research - Data Validation and Verification Using Blockchain in a Clinical Trial for Breast Cancer: Regulatory Sandbox (jmir.org)
[4]. (2021), "A beginner's guide to cryptocurrency" Money Control, https://www.moneycontrol.com/msite/wazirx-cryptocontrol-articles/a-beginners-guide-to-cryptocurrency-article/
[5]. https://usa.kaspersky.com/resource-center/definitions/what-is-cryptocurrency
[6]. https://economictimes.indiatimes.com/tech/technology/global-consensus-emerging-on-regulating-crypto-assets-fm-nirmala-sitharaman/articleshow/103536418.cms
[7]. Newegg. "Newegg Is Now Accepting Bitcoin
[8]. AT&T. "AT&T Now Accepts BitPay."
[9]. BitPay. "Microsoft Chooses BitPay to Power Bitcoin Payments."
[10]. Coindesk. "Chicago Sun-Times Becomes First Major US Newspaper to Accept Bitcoin."
[11]. AXA. "New Payment Option: Bitcoin."
[12]. Wikipedia."List of cryptocurrencies" https://en.wikipedia.org/wiki/List_of_cryptocurrencies
[13]. PYMNTS.com. "Auto Insurer Metromile to Allow Bitcoin Payments, Payouts."
[14]. Andrea Knezovic (Apr 13 2023), "15 Biggest Crypto Scams in History + Famous Scammers" Udonis, https://www.blog.udonis.co/blockchain/crypto-scams/
[15]. https://www.nerdwallet.com/author/andy-rosen
[16]. https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/how-to-store-cryptocurrency/

**First A. Prashant Awasthi**, has achieved Master of Science from Symbiosis Institute of Computer Studies and Research (SICSR), Pune India. Mr. Prashant holds 16+ years of IT work experience in the area of Cloud Computing, DevOps, Java, Unix, Linux and Windows platforms. Mr. Prashant has achieved multiple certifications related to Cloud, Terraform and ITIL practices. Mr. Prashant works with one of the leading IT organizations.

**Second B. Murugaiyan Dhandapani** graduated with a bachelor's degree in engineering from the Anna University-afflicted Sri Ramakrishan College of Engineering in Tamil Nadu, India. Murugaiyan had eight or more years of expertise working in the field of cloud architecture, migration, and middleware and currently works by one of the top IT companies and holds numerous certifications in the areas of cloud computing.

.

******