International Journal of Innovation and Scientific Research
ISSN 2336-0046 Vol. 77 No. 1 Feb. 2025, pp. 116-128

http://www.ijisr.issr-journals.org/

The Evolution of Cryptocurrency: From Bitcoin to Advanced Blockchain Solutions

Ayushi Gupta and Anamika Gupta

Shaheed Sukhdev College of Business Studies, University of Delhi, Delhi, India

ABSTRACT: Cryptocurrencies have gained extreme popularity in recent years. With the advent of Blockchain technology and Smart Contracts, the need for third parties or intermediaries for regulation and management has been eliminated. This has resulted in the growing adoption of digital currency and decentralized applications based on them. This article talks about the evolution of cryptocurrency and its advancements since the idea was introduced in 1983 by David Chaum. It also states about the cryptographic principles, several layers in the Blockchain technology, the smart contracts written in Solidity on Ethereum platform, and Decentralized Applications based on them. Some of the popular cryptocurrencies including Bitcoin and other Alternate Coins are also mentioned. However, there exist several legal and regulatory issues which are associated with the use of cryptocurrencies. These issues must be taken care of before moving towards the complete acceptance of these digital currencies. Hence, such issues are also highlighted in this study. Further, cryptocurrencies have found many applications including cross-border transactions, decentralized financial systems, and supply chain tracking, which are also discussed. Finally, the history and current status of cryptocurrency in India has been explored and the platforms where investors can buy and sell them are mentioned. This paper will serve as a guide for understanding the key concept of cryptocurrency, while also highlighting its practical applications. Further, the research community can study user behaviour and market ecosystems in different cryptocurrency platforms.

KEYWORDS: Cryptocurrency, Blockchain Technology, Bitcoin, Smart Contracts, DApps.

1 INTRODUCTION

Currency is one of the most important inventions of homosapiens which has served as the basis for all economic exchange from the beginning of trade. Originally emerging as a system of barter, it has evolved into an extraordinary electronic currency called cryptocurrency. This journey began with early attempts at digital currencies, like David Chaum's eCash in the 1990s [1], which laid the groundwork for future development. The introduction of Bitcoin by the pseudonymous Satoshi Nakamoto, revolutionized the concept with its decentralized peer-to-peer network and a fixed supply of 21 million coins [2]. Since Bitcoin's inception, the cryptocurrency market has seen extensive growth, with numerous cryptocurrencies now offering unique features and use cases. The technology behind these cryptocurrencies, particularly blockchain, holds significant potential to disrupt many other industries apart from the monetary market. As cryptocurrencies become more widely accepted, both by the public and institutional investors, the market is likely to experience significant growth and development. Major financial institutions, including banks and investment firms, are beginning to recognize cryptocurrencies as legitimate assets [3]. Beyond investment and payment methods, cryptocurrencies are being utilized in various industries, from entertainment to healthcare. The expanding number of use cases is likely to attract more users, further driving market growth.

1.1 WHAT IS CRYPTOCURRENCY?

Cryptocurrency is a form of digital or virtual currency that relies on cryptography to ensure security [4]. Unlike traditional currencies issued by governments and central banks, cryptocurrencies operate on a decentralized system powered by blockchain technology. Fig. 1 illustrates the architectures of both centralized and decentralized systems. In the centralized architecture, a central authority manages data or money exchange, whereas in decentralized systems, all nodes function as peers. This decentralized nature means that no single entity has control over the entire network, making cryptocurrencies theoretically immune to government interference or manipulation.

In traditional systems, a central authority provides authorization and trust for transactions. However, this leads to delays and the transactions become highly traceable. On the other hand, cryptocurrencies are based on a decentralized network for processing transactions, which leads to faster exchanges and maintains privacy [5].

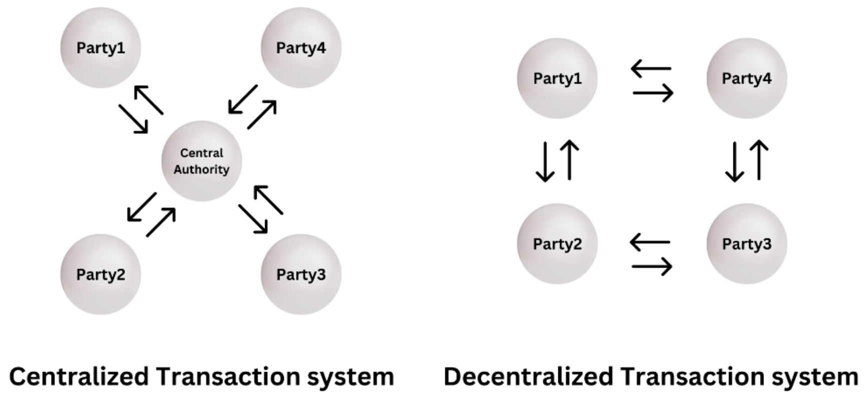

Fig. 1. Network Architectures

1.2 Cryptography And Security

The term "crypto" is derived from the ancient Greek word "kryptos", which means "hidden" or "secret". Cryptography is the field that uses secure methods to share information so that only authorized users can access it and interception by third parties can be prevented [4]. The message to be transmitted, referred to as plaintext, is encoded or encrypted using a secret key to produce an encoded message, known as ciphertext. Upon receipt, the ciphertext is decrypted—either with the same key or a different one—to reveal the original plaintext. Fig. 2 illustrates the concept of cryptography.

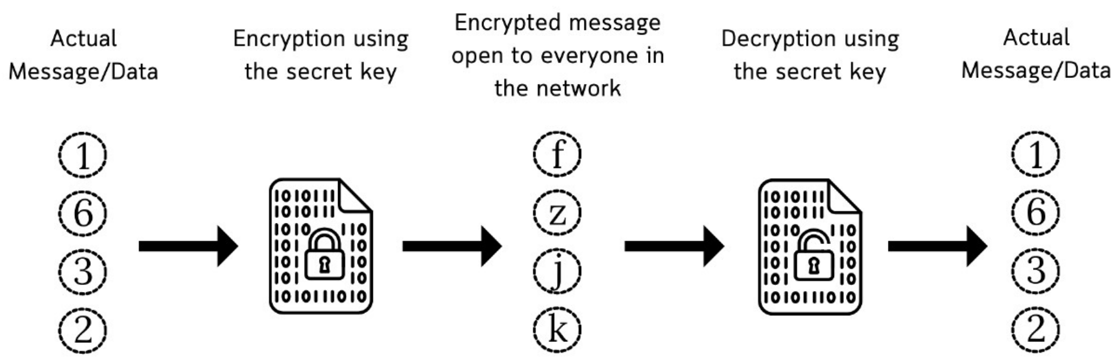

Fig. 2. The Process of Cryptography

In the context of blockchain and cryptocurrencies, cryptographic techniques serve two primary functions: securing transactions and controlling the creation of new coins. Every transaction within a cryptocurrency network is protected using cryptographic algorithms that ensure the authenticity and integrity of the data. In these transactions, there are two important components: public and private keys. The public key is like an address that can be shared openly with others to receive funds, similar to sharing an email address. The private key grants the owner the authority to authorize transactions. The private key must be kept secret because anyone with access to it can control the associated funds. A new transaction is signed with the sender's private key, creating a digital signature, which can be verified by anyone using the corresponding public key. This assurance makes cryptocurrencies secure and trustworthy. The most commonly used algorithm in blockchain technology is SHA-256 which stands for Secure Hash Algorithm, employing a 256 bit code to encrypt the message [6].

1.3 Blockchain Technology

Most cryptocurrencies rely on blockchain technology, which is a shared digital ledger where every transaction is recorded across a decentralized network of computers i.e., each participant maintains a copy of the ledger [7]. Whenever a new transaction occurs, it is added to everyone's ledger, and each block in the chain holds multiple transactions. Fig. 3 shows a blockchain prototype highlighting the contents of a block. Each block in the blockchain acts as a container for transaction details and consists of three key elements: transactional data representing the actual details of the transactions, a unique hash value computed using cryptographic methods on the entire block contents, and the hash value of the preceding block, which links each block to the one before it. Apart from these, each block contains a block number, indicating its position in the chain, a timestamp value, and a nonce value that can be adjusted to generate a hash that meets the network's difficulty target. This nonce value is crucial for the process of mining and validating new blocks.

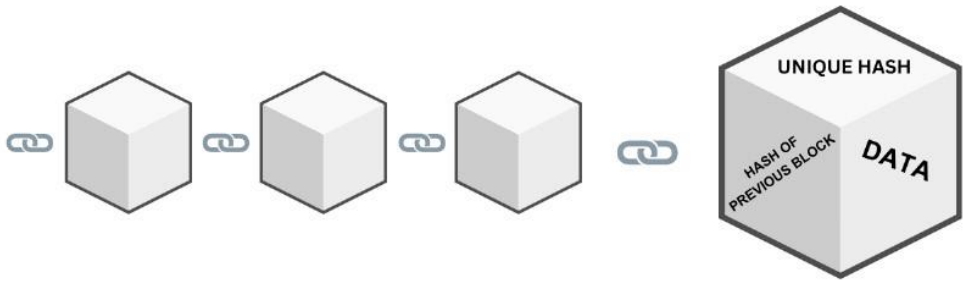

Fig. 3. Blockchain Prototype

Blockchain architecture is typically organized into multiple layers, each with a specific function that contributes to the overall operation of the blockchain system [8]. Fig. 4 shows the several blockchain layers, which are also explained next.

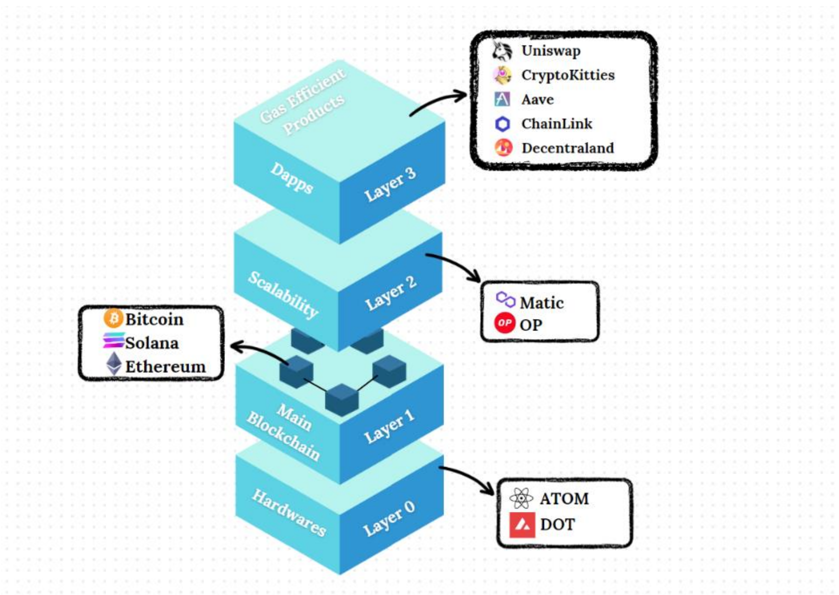

Fig. 4. Layers Representation

- **Layer 0 (Infrastructure Layer):** This layer forms the foundation of the blockchain infrastructure, encompassing the underlying hardware, data transmission protocols, and topology of the network. It facilitates peer-to-peer communication.
- **Layer 1 (Consensus Layer):** This layer is responsible for managing the consensus mechanism which defines the agreement on whether a transaction is valid or not across the network. It comprises protocols like Proof of Work (PoW) and Proof of Stake (PoS), to ensure agreement among network participants and securing the blockchain.
- **Layer 2 (Data Layer):** This layer manages and stores all the historical transaction data as well as the current state of the distributed ledger on the blockchain network.
- **Layer 3 (Application Layer):** This layer provides direct interaction with the end-users through user interfaces. It comprises Decentralized applications (DApps) and smart contracts. DApps are built by developers on this layer to leverage the blockchain's capabilities to provide various services, such as financial transactions and supply chain tracking.

2 THE ADVANCEMENT OF CRYPTOCURRENCY

Cryptocurrencies come from a multidisciplinary field involving cryptography, computer science, and economics. It has transformed the financial market by revolutionary innovations, controversies, and rapid growth. Some of the key milestones that have influenced the evolution of digital currencies are mentioned below.

2.1 PRECURSORS AND EARLY CONCEPTS

- **The vision of David Chaum:** David Chaum was a cryptographer who pictured a digital currency that would allow secure transactions without the need of central authorities. His paper, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups", laid the foundation for cryptographic protocols [1]. He introduced the concept of "blinding", which allowed for secure digital transactions. This idea influenced subsequent projects like EGold and Bit Gold based on cryptographic principles, which allowed the creation of digital tokens.

2.2 THE BIRTH OF BITCOIN (2008-2010)

- **Satoshi Nakamoto's Whitepaper:** In 2008, an anonymous person or group using the pseudonym Satoshi Nakamoto published the whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [2]. This innovative document explained how a decentralized digital currency works.
- **Scarcity:** Nakamoto capped the total supply of bitcoins at 21 million, simulating the scarcity of precious metals like gold.
- **Proof of Work (PoW):** PoW is the consensus mechanism used in Bitcoin Blockchain in which miners validate transactions by solving complex mathematical puzzles. They compete to add blocks to the blockchain, which are validated and verified, ensuring security and decentralization.

2.3 ALTCOINS AND DIVERSE BLOCKCHAINS

- **Altcoins Emerge:** Alternative cryptocurrencies (altcoins) emerged after Bitcoin's success. Litecoin (2011) introduced faster block generation, while Namecoin (2011) explored decentralized domain registration [9].
- **Ethereum and Smart Contracts:** Vitalik Buterin's Ethereum (2015) revolutionized the Blockchain domain by introducing smart contracts [10]. Smart contracts are self-executing programs written by developers to create decentralized applications (DApps) beyond simple transactions.

2.4 REGULATION AND INSTITUTIONAL ADOPTION

- **Legal Challenges:** Cryptocurrencies have faced regulatory challenges worldwide. Some countries accepted and supported them, while others banned or restricted their use with strict measures.
- **Institutional Involvement:** Bitcoin futures contracts were introduced which allowed investors to buy or sell Bitcoins at a fixed price on a specific future date. This was a significant step toward institutional acceptance [11]. Traditional financial institutions like banks and insurance companies, hedge funds, and corporations started looking into cryptocurrencies as a new type of investment.

2.5 Challenges and Future Prospects

- **Scalability:** As adoption is growing, multiple economies will start recognizing it as an official medium of value exchange. As a result, transaction volumes will increase, and maintaining fast and low-cost transactions becomes challenging, leading to slower processing times and higher fees.
- **Environmental Impact:** The PoW consensus protocol consumes loads of energy for every transaction which raises environmental concerns. Proof-of-Stake (PoS) or other consensus mechanisms that offer greener alternatives can be employed for mining and validating blocks [12].
- **DeFi and Beyond:** Decentralized Finance (DeFi) platforms [13], Non-Fungible Tokens (NFTs) [14], and Web3 innovations [15] continue to shape the crypto landscape.

The evolution of cryptocurrencies is an ongoing saga — one that intertwines technology, economics, and human ambition. The further sections delve into cryptocurrency applications such as Smart Contracts and Decentralized Application (DApps) deployed on the Ethereum blockchain, list some popular cryptocurrencies and legal issues associated with them and mention some of the top platforms for buying and selling cryptocurrencies.

3 Cryptocurrency Applications

Cryptocurrencies have found applications across various industries, driven by their unique characteristics such as decentralization, transparency, and security. Below are some key applications of cryptocurrencies:

1. **Store of Value:** Traditional currencies can be influenced by inflation and other market factors. However, the limited supply of Bitcoin and its decentralized nature lead to maintaining its value over time. Hence, Bitcoin is often referred to as ”digital gold” due to its characteristics as a store of value. As per recent research, these qualities of Bitcoin positions it as a feasible alternative to traditional stores of value like gold [16], [17].

2. **Payment Systems:** Through cryptocurrencies, cross-border transactions have become fast, secure, and cost-effective. Traditional banking systems involve intermediaries and higher fees, while cryptocurrencies like Bitcoin and Ether facilitate peer-to-peer transactions with minimal costs. This has been especially helpful in areas where people don’t have easy access to traditional banking services. This can also help people in underserved regions to take part in the global economy [18].

3. **DeFi:** Ethereum provides a platform where people can lend, borrow, and trade directly with each other. This has created a new financial system that does not rely on traditional banks and is more open and accessible. These decentralized financial platforms on Ethereum are making it easier for everyone to join and offering new types of financial services that are available to people all over the world [19], [20].

4. **Smart Contracts and DApps:** The smart contract functionality in Ethereum allows for the development of various DApps which provide automated and trustless agreements between the participants [21]. Based on some predefined conditions, the contracts self-execute and the need for intermediaries is eliminated.

5. **Supply Chain Management:** Supply chain can be made more transparent and efficient using Blockchain technology with cryptocurrencies. Since all the transactions are recorded permanently, it becomes easier to trace them and committing fraud becomes hard, which increases trust in the supply chain [22].

6. **NFTs:** NFTs represent ownership of unique digital items, such as art or virtual real estate. By using blockchain to prove ownership of these digital assets, NFTs have created new opportunities for creators and collectors. Cryptocurrencies are heavily used through NFTs especially on platforms like Ethereum. Studies show that the use of NFTs are expanding into gaming and virtual worlds [23].

The following subsections provide a detailed explanation of Smart Contracts, followed by an example written in the Solidity programming language used for writing smart contracts. After that, DApps are discussed in depth. Since Smart Contracts and DApps operate on Ethereum, the subsections also cover the Ethereum Virtual Machine (EVM).

3.1 Smart Contracts

Smart contracts are codes which are deployed on a blockchain to provide agreement between multiple parties. These contracts are designed to automatically enforce the terms and conditions of the agreement when specific predetermined rules are met [24]. Hence, the need for intermediaries or third parties to enforce the terms of the agreement is eliminated.

For instance, let's say F is a florist who sells flowers and S is a shopkeeper interested in purchasing some of F's flowers. F agrees to send the temperature maintained fresh flowers to S after receiving payment. However, there is a risk that F might send wilted flowers to S, or S might deny making the payment after receiving the fresh flowers. Both parties could face losses due to the lack of trust in the transaction. In this scenario, a smart contract could be written to automate the transaction. The contract would ensure that the fresh flowers are delivered to S as soon as the payment is made, preventing any potential disputes. Fig. 5 showcases such a smart contract between the two parties.

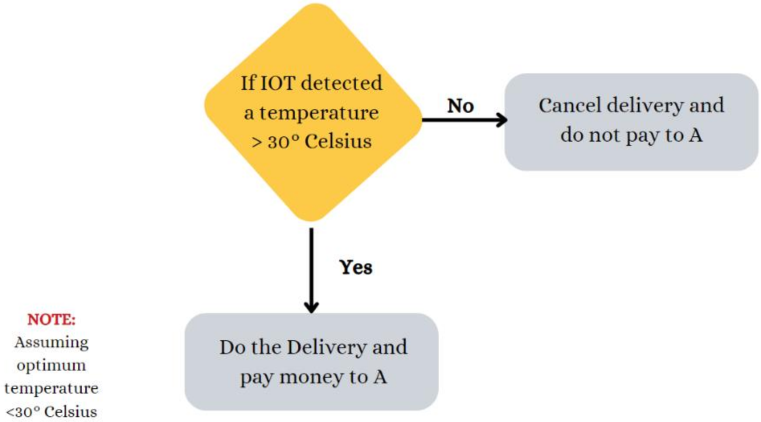

Fig. 5. A Smart Contract between two Parties

3.2 SOLIDITY

Smart contracts are scripted using the high-level object-oriented programming language known as Solidity [25]. Coding the smart contract in established languages such as Python, JavaScript, or C++ requires the use of numerous add-ons, making the process arduous and less efficient. While it is feasible to utilize these languages for contract scripting, they were not specifically engineered for this purpose. In contrast, Solidity was purpose-built for scripting smart contracts, offering a more effective and streamlined approach. For the example shown in Fig. 5, a smart contract written in solidity is shown below in Fig. 6. The statements beginning with '//' represent comments for understanding the code.

```
pragma solidity ^0.8.0;

contract FlowerDelivery {
    address payable public florist; // Address of the Florist (F)
    address public shopkeeper; // Address of the shopkeeper (S)
    uint public price; // Price of the flowers
    uint public temperature; // Temperature of the container

    bool public isTemperatureMaintained;
    bool public isPaymentMade;

    function checkTemperature() external {
        //fetch temperature from IoT device
        if(temperature < 30) {}
            isTemperatureMaintained = true;
        }
        else {
            isTemperatureMaintained = false;
        }
    }
    // Function for the shopkeeper to pay for the flowers
    function payForFlowers() external payable {
            //make payment to florist
            isPaymentMade = True;
    }

    // Function for the florist to confirm the delivery of the flowers
    function confirmDelivery() external {
        if(isTemperatureMaintained == true && isPaymentMade == false) {}
                //transfer price to Florist
                isPaymentMade = true;
            }
        }
    }

    // Function for the shopkeeper to receive flowers
    function receiveFlowers() external view returns (string memory) {
        if(isTemperatureMaintained == true) {
            //transfer price to Florist
            isPaymentMade = true;
        }
        else {
            // cancel delivery
            isPaymentMade = false;
        }
    }
}
```

Fig. 6. An example of a Smart Contract in Solidity

3.3 DECENTRALIZED APPLICATIONS (DAPPS)

A DApp is a software application developed by both established firms and independent developers, that operates on a decentralized blockchain network [26]. DApps differ from traditional applications in several key ways. The key features and characteristics of DApps are mentioned below.

1. **Decentralization:** DApps run on a decentralized network of nodes rather than centralized servers. This structure enhances transparency and reduces the risk of failure since there is no single entity that controls the entire application.

2. **User Interface:** DApps provide user interfaces that allows users to engage with the DApp without needing deep technical knowledge of blockchain technology.
3. **Smart Contracts:** Smart contracts are a fundamental component of DApps which facilitate and automate transactions on the blockchain.
4. **User Types:** The DApp ecosystem includes various user types. DApp users are general consumers who interact with the DApp through its user interface. Smart Contract users are technical users who engage directly with the smart contracts. Finally, Coin/Token users are individuals interested in the financial aspects of the DApp, such as trading tokens or coins associated with the application.
5. **Interoperability:** DApps often connect with different blockchain platforms, which gives them more flexibility and the ability to share resources. Blockchain bridges and standard tools make this easier by allowing developers to move their applications between various platforms smoothly.

Fig. 7 illustrates the architecture of a DApp. Ethereum Virtual Machine (EVM) is responsible for executing the logic defined in the smart contracts. Providers such as Moralis, MetaMask, Alchemy, Infura act as intermediaries, enabling interaction with the blockchain, providing the frontend to execute smart contract functions and retrieve data. Web Server hosts the frontend of the DApp, which is accessible to users via a web browser. Users' requests are processed by the web server, which communicates with the blockchain network via the providers, enabling interaction with the decentralized EVM.

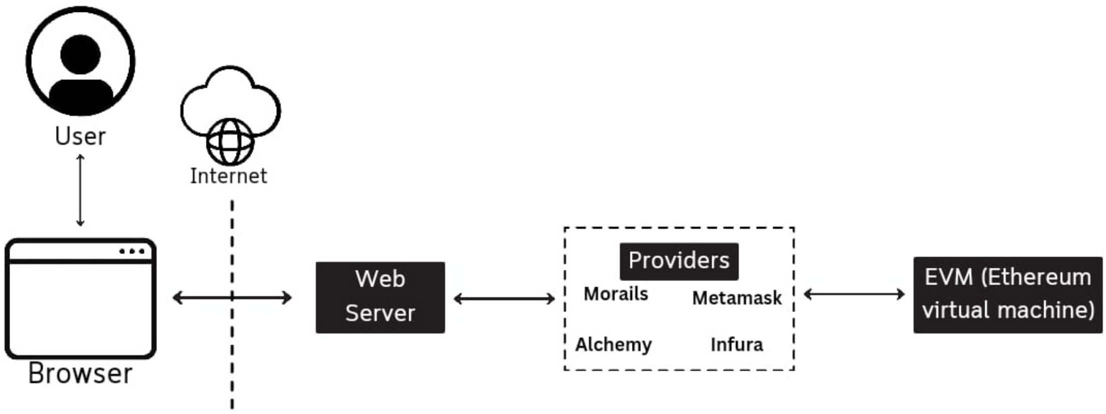

Fig. 7. DApp Architecture

3.3.1 EXAMPLES OF POPULAR DAPPS

1. **Uniswap:** Uniswap is a decentralized exchange (DEX) that allows users to trade cryptocurrencies without the need for a central authority. It operates on the Ethereum blockchain and uses an automated market-making system to facilitate trades [27].
2. **CryptoKitties:** CryptoKitties is a blockchain-based game that enables players to breed, collect, and trade virtual cats. Each CryptoKitty is a unique NFT on the Ethereum blockchain, representing an early and popular example of blockchain gaming [28].
3. **Aave:** Aave is a decentralized lending platform based on smart contracts that allows users to lend and borrow cryptocurrencies without intermediaries [29].
4. **Chainlink:** Chainlink is a decentralized oracle network hosted on the Ethereum platform that enables smart contracts to securely interact with real-world data [30].
5. **Decentraland:** Decentraland is a virtual reality game platform built on Ethereum where users can create, experience, and monetize content and applications such as purchasing virtual land and building upon it [31], [32].

3.4 EVM AND NON-EVM BASED COINS

The Ethereum Virtual Machine (EVM) serves as the fundamental processing unit of the Ethereum network, required for the execution of smart contracts [33]. It allows developers to test, deploy, and run smart contracts in a secure and isolated environment. The EVM interprets the bytecode of smart contracts and protects them against cyber threats maintaining the network's integrity. In contrast, "non-EVM" refers to blockchain networks or platforms that do not rely on the EVM for executing smart contracts. Non-EVM platforms facilitate smart contract operations by employing their own proprietary virtual machines, interpreters, or execution environments. Examples of non-EVM platforms include Polkadot, Solana, and Cardano.

4 POPULAR CRYPTOCURRENCIES

Cryptocurrencies have been used in several applications facilitating secure transactions. Some of the most well-known cryptocurrencies are listed in Table 1 along with their features, the layers they work upon, their applications and limitations.

Tableau 1. Some Popular Cryptocurrencies

Cryptocurrency	Features/ Advantages	Layers	Limitations	Applications
Bitcoin	- Limited Supply of 21 million Bitcoins - Highly secured by Blockchain - Based on PoW protocol - Online Gaming - Widely recognized and accepted	Layer 1	- Slow transaction speed - High transaction fees	- Bitcoin ATMs - Charitable Donations - Online Gaming
Solana (SOL) [34]	- Fast transaction speeds - Scalability - Proof-of-History and Proof-of-Stake protocols	Layer 1 with Layer 2 solutions	Relatively new with less adoption	- Photo Finish Live - Helio: Shopify × Solana Pay plugin
Ethereum (ETH)	- Smart Contracts for DApps and NFTs - Faster transactions than Bitcoin - Proof-of-Stake protocol - Unlimited supply	Layer 1 with Layer 2 scaling solutions	- Higher transaction fees - Scalability Issues	Platform for DeFi and NFTs
Ripple (XRP) [35]	- Quick and secure international payments - Low transaction fees	Layer 1 with enterprise solutions	Centralized nature compared to others	- Modulr - MoneyMatch
Litecoin (LTC)	- Faster and cheaper than Bitcoin - Low transaction fees	Layer 1	Less adoption compared to Bitcoin and Ethereum	- Litecoin Core - Electrum-LTC
Dogecoin [36] (DOGE)	- Simple and easy to use - Faster transactions than Bitcoin - Strong and active community	Layer 1	- Lacks Institutional Support - Scalability issues - Inflationary Supply	- Dogecoin Wallets - Dogecoin Trading Platforms

5 LEGAL ISSUES

Several legal challenges come with cryptocurrencies due to their decentralized nature, anonymity, and lack of established legal frameworks. These issues must be understood and addressed for a secure cryptocurrency ecosystem [37]. Some of the key issues are mentioned below.

1. Cryptocurrencies can hide the identities of those involved, and thus are attractive for illegal activities. They have been used in serious crimes like money laundering, drug trafficking, and weapons trading, which is a major concern. In 2013, authorities shut down the dark web marketplace ”Silk Road,” where Bitcoin was heavily used for illegal transactions like drug dealing [38].
2. There is no central governing authority in a cryptocurrency ecosystem, such as a government or central bank, which makes regulation difficult. The taxation process also becomes complicated.
3. There are no well-defined legal frameworks for cryptocurrencies, which causes problems with taxes, legal disputes, and cybersecurity. This makes it hard to protect investors and users.
4. The value of cryptocurrencies are highly volatile, since they are heavily dependent on market demand and supply instead of concrete assets. Hence, both the regulatory bodies and users are at risk, which makes these assets less stable and reliable.
5. In cases like fraud and inheritance disputes, problems are faced when providing concrete legal evidence since there is anonymity and decentralization in cryptocurrency transactions.
6. There is a lack of clear legal guidelines on digital inheritance. Hence, families often face challenges in accessing deceased individuals’ cryptocurrency holdings due to the lack of necessary information and access protocols.

7. High-profile breaches, such as those affecting Mt. Gox and Bitfinex [39], [40], highlights the vulnerability of cryptocurrency platforms. They are highly targeted by cybercriminals, which leads to substantial financial losses.

6 HISTORY OF CRYPTOCURRENCY AND ITS CURRENT STATUS IN INDIA

Cryptocurrency has had an interesting journey in India, with significant developments and regulatory changes. A complete overview of its history and current status is mentioned below.

- **Introduction (2009-2013):** In 2009, the first cryptocurrency, Bitcoin, was introduced. Further, in 2010, the first commercial Bitcoin transaction took place, with the first exchange taking place in 2013.
- **Initial Regulatory Concerns (2013-2018):**

○ 2013: The Reserve Bank of India (RBI) issued a circular that warned users about the potential risks associated with cryptocurrencies [41].

○ 2017: RBI reiterated its concerns, emphasizing the risks of virtual currencies.

○ 2018: RBI issued a circular prohibiting banks and financial institutions from dealing in virtual currencies.

- **Supreme Court Intervention (2020):** The Supreme Court of India struck down the 2018 RBI circular, declaring it unconstitutional.
- **Regulatory Framework:** The Indian government has been working on creating a regulatory framework for cryptocurrencies. The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021, aims to establish a favorable environment for digital currencies issued by the RBI [42]. As of now, cryptocurrencies are not illegal in India, but there is no comprehensive regulatory framework governing them.
- **Adoption and Usage:** India ranks first in the Global Crypto Adoption Index 2023, indicating a high level of grassroots adoption [43]. As per the market research report, the Indian cryptocurrency market is expected to grow by 7.37% from 301.68 million dollars in 2024 to 532.86 billion dollars in 2032 [44].
- **Digital Rupee:** The RBI has expressed interest in exploring the concept of a central bank digital currency (CBDC), known as the Digital Rupee, which aims to integrate digital currencies into the financial system while ensuring regulatory compliance and stability [45].
- **Government Stance:** The government acknowledges the need for international collaboration to regulate cryptocurrencies effectively [46]. The Ministry of Finance is actively involved in shaping the policy ecosystem for crypto assets.

7 PLATFORMS TO BUY AND SELL CRYPTOCURRENCIES

Platforms for buying and selling cryptocurrencies provide users with the ability to trade digital assets in a secure and efficient manner. These platforms, also known as cryptocurrency exchanges, offer a range of features from simple buy/sell options for beginners to advanced trading tools for experienced users. Some of the most popular platforms are listed in Table 2. This will aid in the broader adoption of cryptocurrencies by making it easier for individuals to enter the market and manage their digital assets.

Tableau 2. Popular Cryptocurrency Platforms

Platform	URL	Pros	Cons
Coinbase	https://www.coinbase.com	Easy to use, good selection of tokens, high security	High fees, user doesn't control private keys, slow to adopt new cryptocurrencies
Uphold	https://www.uphold.com	Simple pricing, supports many tokens, desktop and mobile apps	Not as easy to use, some reports of poor customer service
Kraken	https://www.kraken.com	Long-running exchange, high security, large variety of tokens	Difficult to use, issues with 2FA, reports of poor customer service
Gemini	https://www.gemini.com	Easy app interface, large exchange by assets, supports major assets	No specific cons mentioned
Bitstamp	https://www.bitstamp.net	Long-running, 70+ tokens, low fees	Staking features not available to all, limited staking rewards
eToro	https://www.etoro.com	Global trading options, copy other traders, low minimums	Limited US options, not available in all states, fewer tokens
Bitcoin IRA	https://www.bitcoinira.com	Invest in crypto within an IRA, earn interest tax-free, high security	High fees, high minimums, fewer tokens
Crypto.com	https://www.crypto.com	Many supported tokens, weekly interest on savings, debit card available	Complex fees, no desktop support, limited customer service

8 Conclusion

The rise of cryptocurrency, from a small idea to a widely accepted financial tool, has been both significant and complicated. This chapter has looked at the basics of cryptocurrencies, starting with what they are and how they work. Cryptography and blockchain technology are the core of cryptocurrencies, making them secure, transparent, and decentralized, which is different from traditional financial systems. The evolution of cryptocurrencies, from early theoretical concepts and the groundbreaking launch of Bitcoin to the emergence of alternative coins (altcoins) and diverse blockchain platforms is also discussed. The chapter also explored the details of smart contracts, Solidity programming, and decentralized applications (DApps), which are creating new financial systems, especially on platforms like Ethereum. This was followed by EVM and non-EVM based coins, showing the variety of technologies within the world of cryptocurrencies.

As cryptocurrencies have become more popular, they have faced big challenges, like government regulations and the need for clear legal rules. Looking at the history and current situation of cryptocurrency in India provides an insight into how different places are dealing with these challenges. Some of the popular cryptocurrencies and the platforms where one can buy and sell them are also highlighted.

In conclusion, while cryptocurrencies offer many opportunities, they also bring challenges that need to be carefully thought through by developers, regulators, and users. With the growing use of blockchain-based technologies, it seems likely that decentralized finance and digital currencies will become even more important in the global economy.

References

[1] D. Chaum, «Blind signatures for untraceable payments,» Advances in cryptology, vol. 82, pp. 199–203, 1983.

[2] S. Nakamoto, «Bitcoin: A peer-to-peer electronic cash system,» Bitcoin.org, 2008. Available at: https://bitcoin.org/bitcoin.pdf.

[3] S. J. S. Krishna, A. Panda, and P. Sindhuja, «Cryptocurrency adoption and its influence on traditional financial markets,» dynamics, vol. 8, p. 11, 2023.

[4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 2018.

[5] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and cryptocurrency technologies. Princeton University Press, 2016.

[6] W. Penard and T. Van Werkhoven, «On the secure hash algorithm family,» Cryptography in context, pp. 1–18, 2008.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, «An overview of blockchain technology: Architecture, consensus, and future trends,» in 2017 IEEE international congress on big data (BigData congress), pp. 557–564, IEEE, 2017.
[8] C. Wang, H. Jiang, J. Zeng, Y. Min, Q. Huang, and Z. Zuo, «A review of blockchain layered architecture and technology application research,» Wuhan University Journal of Natural Sciences, vol. 26, no. 5, p. 14, 2021.
[9] M. Haferkorn and J. M. Quintana Diaz, «Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin,» in Enterprise Applications and Services in the Finance Industry: 7th International Workshop, FinanceCom 2014, Sydney, Australia, December 2014, Revised Papers 7, pp. 106–120, Springer, 2015.
[10] V. Buterin, «Ethereum: The world computer,» Ethereum.org, 2013. Available at: https://ethereum.org/en/whitepaper/.
[11] S. Corbet, B. Lucey, M. Peat, and S. Vigne, «Bitcoin futures—what use are they?,» Economics Letters, vol. 172, pp. 23–27, 2018.
[12] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, «Performance analysis and comparison of pow, pos and dag based blockchains,» Digital Communications and Networks, vol. 6, no. 4, pp. 480–485, 2020.
[13] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, «Sok: Decentralized finance (defi),» in Proceedings of the 4th ACM Conference on Advances in Financial Technologies, pp. 30–46, 2022.
[14] B. Hammi, S. Zeadally, and A. J. Perez, «Non-fungible tokens: a review,» IEEE Internet of Things Magazine, vol. 6, no. 1, pp. 46–50, 2023.
[15] P. P. Ray, «Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions,» Internet of Things and Cyber-Physical Systems, vol. 3, pp. 213–248, 2023.
[16] T. N. Rotta and E. Paran´a, «Bitcoin as a digital commodity,» New Political Economy, vol. 27, no. 6, pp. 1046–1061, 2022.
[17] N. Popper, Digital gold: The untold story of Bitcoin. Penguin UK, 2015.
[18] N. Taleb, «Prospective applications of blockchain and bitcoin cryptocurrency technology,» TEM Journal, vol. 8, no. 1, pp. 48–55, 2019.
[19] H. Teng, W. Tian, H. Wang, and Z. Yang, «Applications of the decentralized finance (defi) on the ethereum,» in 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), pp. 573–578, IEEE, 2022.
[20] I. Makarov and A. Schoar, «Cryptocurrencies and decentralized finance (defi),» Brookings Papers on Economic Activity, vol. 2022, no. 1, pp. 141–215, 2022.
[21] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, «An overview on smart contracts: Challenges, advances and platforms,» Future Generation Computer Systems, vol. 105, pp. 475–491, 2020.
[22] H. Min, «Blockchain technology for enhancing supply chain resilience,» Business Horizons, vol. 62, no. 1, pp. 35–45, 2019.
[23] W. Rehman, H. e Zainab, J. Imran, and N. Z. Bawany, «Nfts: Applications and challenges,» in 2021 22nd International Arab Conference on Information Technology (ACIT), pp. 1–7, IEEE, 2021.
[24] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, «Blockchain smart contracts: Applications, challenges, and future trends,» Peer-to-peer Networking and Applications, vol. 14, pp. 2901–2925, 2021.
[25] C. Dannen and C. Dannen, «Solidity programming,» Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners, pp. 69–88, 2017.
[26] C. Dai, «Dex: A dapp for the decentralized marketplace,» Blockchain and Crypt Currency, vol. 95, 2020.
[27] A. A. Aigner and G. Dhaliwal, «Uniswap: Impermanent loss and risk profile of a liquidity provider,» arXiv preprint arXiv: 2106.14404, 2021.
[28] A. Serada, T. Sihvonen, and J. T. Harviainen, «Cryptokitties and the new ludic economy: How blockchain introduces value, ownership, and scarcity in digital gaming,» Games and Culture, vol. 16, no. 4, pp. 457–480, 2021.
[29] Z. Ao, L. W. Cong, G. Horvath, and L. Zhang, «Is decentralized finance actually decentralized? a social network analysis of the aave protocol on the ethereum blockchain,» arXiv preprint arXiv: 2206.08401, 2022.
[30] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz, et al., «Chainlink 2.0: Next steps in the evolution of decentralized oracle networks,» Chainlink Labs, vol. 1, pp. 1–136, 2021.
[31] B. Guidi and A. Michienzi, «Social games and blockchain: exploring the metaverse of decentraland,» in 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 199–204, IEEE, 2022.
[32] C. Goanta, «Selling land in decentraland: The regime of non-fungible tokens on the ethereum blockchain under the digital content directive,» Disruptive technology, legal innovation, and the future of real estate, pp. 139–154, 2020.
[33] G. Wood et al., «Ethereum: A secure decentralised generalised transaction ledger,» Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.
[34] A. Yakovenko, «Solana: A new architecture for a high performance blockchain v0. 8.13,» Whitepaper, 2018.
[35] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, «Ripple: Overview and outlook,» in Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings 8, pp. 163–180, Springer, 2015.
[36] A. Nani, «The doge worth 88 billion dollars: A case study of dogecoin,» Convergence, vol. 28, no. 6, pp. 1719–1736, 2022.

[37] A. Aziz, N. A. M. Noor, and O. Mashhour, «The money of the future: A study of the legal challenges facing cryptocurrencies,» BiLD Law Journal, vol. 7, no. 1, pp. 21–33, 2022.

[38] M. C. Van Hout and T. Bingham, «Silk road, the virtual drug marketplace: A single case study of user experiences,» International Journal of Drug Policy, vol. 24, no. 5, pp. 385–391, 2013.

[39] A. Tsang, «Bitcoin plunges after hacking of exchange in hong kong,» The New York Times, 2016.

[40] J. Boyd, «The mt. gox bitcoin debacle: An update,» 2015. Available at: https://spectrum. ieee.org/the-mt-gox-bitcoin-debacle-an-update.

[41] M. R. Aslam, «The future of cryptocurrencies and its legalisation in india,» 2023. Available at: https://economictimes.indiatimes.com/markets/cryptocurrency/the-future-of-cryptocurrencies-and-its-legalisation-in-india/articleshow/104081432.cms?from=mdr.

[42] D. S. Thakur, R. A. Varma, and D. M. Hake, «Regulation of cryptocurrency in india: Issues and challenges,» Journal of Positive School Psychology, vol. 6, pp. 8921–8929, 2022.

[43] «Global crypto adoption index 2023,» 2024. Available at: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/.

[44] «India cryptocurrency market assessment, by type [bitcoin, ethereum, tether, ripple, others], by component [hardware, software], by process [mining, transaction], by end-user [trading, retail and e-commerce, banking, government, others], by region, opportunities and forecast,» 2024. Available at: https://www.marketsandata.com/industry-reports/india-cryptocurrency-market.

[45] Moneycontrol, «The e-rupee is on the way as rbi gears up for a pilot launch of its own digital currency,» 2022. Available at: https://www.moneycontrol.com/news/business/central-bank-digital-currency-aimed-at-complementing-current-forms-of-money-rbi-9291291.html.

[46] S. D. Damodaran A., Vanguri Sruthi, «Crypto assets: Regulatory choices for consumer and investor protection,» 2024. Available at: https://icrier.org/pdf/CryptoAssets.pdf.