DLINE JOURNALS

Information Security Education Journal (ISEJ)

Print ISSN: 2349-8161
Online ISSN: 2349-817X

ISEJ 2024;11 (2)
https://doi.org/10.6025/ISEJ/2024/11/2/52-59

A Brief Review of Blockchain Technology and Cryptocurrency Education

Prathima D
Computer Science Department
Jain College, Vasvi campus
VV Puram, Bangalore
Pratima-279@yahoo.in

ABSTRACT

Blockchain is a record-keeping technology designed to make it impossible to hack the system or forge the data stored on the blockchain, making it secure and immutable. It's a distributed ledger technology (DLT), a digital record-keeping system for simultaneously recording transactions and related data in multiple places.A digital currency is one in which transactions are verified, and records are maintained by a decentralised system using cryptography rather than a centralised authority."Decentralised cryptocurrencies such as bitcoin now provide an outlet for personal wealth that is beyond restriction and confiscation" · "As bitcoin gains ground, more companies have started accepting the cryptocurrency" ·

Received: 2 June 2024
Revised: 5 September 2024
Accepted: 16 September 2024

Keywords: Blockchain, Crypto currency, Recorded Transactions, Bitcoin

1. Introduction

A blockchain can be described as a compilation of assets, such as properties, telephone numbers, and unique items, or it may be considered intangible. It must maintain records or accessible logs that are distributed among involved parties. Each transaction that is included is initially validated by all participants in that transaction. The blockchain is a distributed database of records of all executed transactions or digital events shared among participating parties. The majority of the system's participants verify each transaction.

It contains every single record of each transaction. Bitcoin is the most popular cryptocurrency and an example of blockchain technology. Blockchain Technology came to light when a person or group named Satoshi Nakamoto published a white paper on "*BitCoin: A peer-to-peer electronic cash system*" in 2008.Digital currencies, such as the decentralised Bitcoin or Ethereum or peer-to-peer digital money, use blockchain technology (Rajput 2019).

• One of the popularuses of Blockchain is Bitcoin. Bitcoin is a cryptocurrency used to exchange digital assets online. It uses cryptographic proof instead of third-party trust for two parties to execute transactions over the Internet. Each transaction is protected through a digital signature.

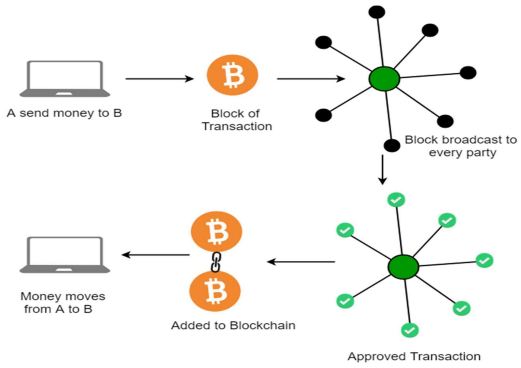

Figure 1. Blockchain process

• Bitcoin blockchain stores transaction details such as sender, receiver, and bitcoin amount.

Through the utilisation of blockchain technology, numerous nodes within the network confirm a transaction at the same time. Anyone with a computer can connect to the network and verify transactions. Several devices endorse the transaction, recorded as a code block distributed among multiple devices. Each new transaction is incorporated into a sequence (thus, blockchain) to preserve a historical log on the DLT (thus distributed ledger), effectively reducing the chances of hacking. (Habib, 2022).

• A blockchain is a highly secure, communal chain of data. It helps business networks exchange assets, store information, and record transactions. These digital ledgers use consensus and permanent record-keeping to make processes more efficient, trustworthy, and safe for all involved parties.

Blockchain security is a comprehensive risk management system for a blockchain network. It uses cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and fraud.

A blockchain is a distributed ledger with an enlarging list of files or records, also called blocks, that are safely interlinked using hash technology.

Hashing in blockchain converts input data into a fixed-size output using a specific algorithm. It establishes data integrity and avoids fraudulent transactions. At the core segment of this process are hash functions, which help create different digital fingerprints for data. The output, known as a hash value, is unique to the input data. The hash value will differ even if the input data is altered slightly.

1. Smart contracts are computer programs that run on blockchain technology and dynamically execute the terms of an agreement when certain conditions are satisfied. These conditions are coded/converted into the contract, and once the conditions are satisfied, the contract is executed without intermediaries or human intervention.The Applications of blockchain technology include Finance, Supply Chain Management, Healthcare and Voting Systems.

2. Challenges

Despite its potential, blockchain technology faces several challenges.

• Scalability

• Energy Consumption

• Regulatory and Legal Issues

· Energy Consumption

· Regulatory and Legal Issues

3. Overview

Cryptocurrencies are digital or virtual currencies that use cryptography for security. Bitcoin was the first cryptocurrency, and since then, thousands of alternatives (altcoins) have emerged.

Bitcoin (BTC): Introduced in 2009, Bitcoin is the first and most well-known cryptocurrency. It remains the largest by market capitalisation. Bitcoin Blockchain is currently among the largest and most widely recognised public blockchains. It was introduced by Satoshi Nakamoto in 2008 as an alternative to the traditional banking system. The primary objective was to decentralise the banking sector and facilitate peer-to-peer transfers of a digital currency known as Bitcoin. It employs cryptographic methods to govern cryptocurrency, verifying and establishing a historical transaction chain over time. Key components of a Bitcoin transaction address include the private key, Bitcoin software, and wallet software [Baboshkin 2022) 19]. Unlike traditional currencies, they exist in a virtual format; no physical or digital coins are exchanged. Bitcoin users possess keys that signify their ownership rights within the network. They utilise these keys to unlock and authorise transactions. Value is transferred by giving it to another key holder. Typically, keys are stored in a digital wallet on user devices. The " mining " process is essential to Bitcoin, as it is a computationally intensive method that validates and confirms transactions. Miners are rewarded approximately every 10 minutes [Jabbar, R. 2022). The challenge of double-spending transactions has been a concern in Bitcoin, which has been addressed (Pagnotta, E.S) in digital currency.

Ethereum (ETH): This cryptocurrency introduced smart contracts, allowing for the creation of decentralised applications (DApps). It is the second-largest cryptocurrency by market cap. Ethereum is a public blockchain platform created by a developer named Vitalik Buterin in late 2013. It features an EVM (Ethereum Virtual Machine) operating system that facilitates the execution of smart contracts on the nodes that participate in the network. Smart contracts are coded in Solidity, a Turing-complete programming language. Ethereum operates as an open-source and decentralised public platform, enabling anyone to develop and launch decentralised applications. It employs a proof-of-work consensus mechanism known as the Dagger Hashimoto algorithm. Ether is the cryptocurrency associated with Ethereum and can be ·
exchanged between Ethereum accounts. A Merkle tree is a hierarchical hash tree data structure that organises the transactions within a block. It utilises the SHA-256 hashing algorithm to produce hashes. (Salem, 2022) Altcoins: This category includes a wide variety of cryptocurrencies with different features and use cases, such as Ripple (XRP), Litecoin (LTC), and Cardano (ADA).

Hyperledger is an open-source, enterprise-grade framework for creating blockchain solutions, which was introduced in 2016. It comprises various projects tailored to meet distinct blockchain requirements and solutions. Notable projects include Burrow, Composer, Fabric, and Indy. Hyperledger Fabric is an operational platform, while other projects are still incubating. Fabric employs distributed ledger technology and supports smart contract capabilities. Users can select from various consensus mechanisms, including PBFT, Kafka, Solo, etc. It also features membership services designed for developing permissioned blockchains. (Agrawal, D. 2022) One of the open-source blockchain options offered by Hyperledger is known as Hyperledger Fabric, which aims to establish a decentralised environment. It consists of a committed peer, a client, a certificate authority, an ordering service, and an endorsing peer. Furthermore, these components interact through channels created to facilitate transactions securely and privately, segregating different application domains. Regarding privacy, an element with limited network access cannot access a chain from a committed peer linked to the channel. To improve a node's data capacity and increase scalability, a unique individual for each channel allows for the sharing of various transactions and data stored across different committed nodes.(Sammeta, N.; 2022)

Multichain is an alternative platform designed to create and implement private blockchains. It serves as a do-it-yourself solution for financial institutions aiming to develop decentralised applications for their offerings. Instead of utilizing a proof-of-work consensus model, Multichain selects a miner from a pool of authorized miners in a round-robin manner. In Multichain, there

are no fees for transactions or rewards for mining. (Bouachir, O.; 2020).

4. Adoption and Impact

Cryptocurrencies have gained popularity as investment assets, payment methods, and enablers of decentralised finance (DeFi).

·Investment

·Payments
·DeFi

Challenges

The cryptocurrency space faces significant challenges, particularly regarding security, regulation, and volatility.

·Security

·Regulation:

·Ethical Considerations in Blockchain Technology and Cryptocurrency

4.1.Privacy and Anonymity

Data Privacy

· **Public Ledger:** Blockchain's transparency means that transaction data is publicly available, while personal IDs are not directly linked to transactions.

· **GDPR Compliance**: It is a conflict with the General Data Protection Regulation (GDPR)

· **Anonymity:** Cryptocurrencies like Bitcoin offer a degree of pseudonymity, which can be corrupted.

· **Ethical Dilemma:** Balancing the misuse of privacy benefits by malicious actors poses a significant ethical challenge.

4.2. Security

Cybersecurity

· **Vulnerabilities:** Despite blockchain's robust security, vulnerabilities in smart contracts, exchanges, and wallets can be exploited, leading to significant financial losses.

· **Hacks and Thefts:** High-profile hacks, such as the Mt. Gox and DAO incidents

Consumer Protection

· **Scams and Frauds**: The rise of Initial Coin Offerings (ICOs) and other crypto investments has led to numerous scams and fraudulent schemes, raising questions about the ethical obligation to protect investors.

· **Education and Awareness**: The ethical responsibility is to educate users about the risks and safe practices in handling cryptocurrencies.

4.3. Environmental Impact

Energy Consumption

· **Proof of Work (PoW)**: Blockchain networks like Bitcoin use PoW consensus mechanisms, which are highly energy-intensive. This raises ethical concerns about the environmental sustainability of such systems.

·**Climate Change**: prompting calls for more environmentally friendly alternatives like Proof of

Stake (PoS)

4.4. Regulatory Compliance
Legal and Regulatory Challenges

· **Regulatory Uncertainty:** The lack of clear regulatory frameworks for blockchain and cryptocurrencies can lead to ethical dilemmas as companies and users navigate a complex legal landscape.

· **Compliance and Innovation:** There is an ethical tension between ensuring regulatory compliance to protect consumers and fostering innovation in the blockchain space.

4.5. Taxation and Financial Regulation
· **Tax Evasion:** Cryptocurrencies can be used to evade taxes, raising ethical issues about fair contribution to public finances.

·**Anti-Money Laundering (AML):** Ensuring compliance with AML regulations is crucial to preventing cryptocurrency misuse for illicit activities.

5. Social Implications

5.1. Financial Inclusion
·Access to Financial Services: Blockchain technology has the strength to improve financial decisions by providing access to financial services for unbanked and underbanked populations.

·**Digital Divide:** There is an ethical concern about exacerbating the digital divide, as access to blockchain technology and cryptocurrencies requires a certain level of digital literacy and internet connectivity.

5.2. Decentralization and Power Dynamics
·**Decentralization**: While blockchain promotes decentralisation, it also shifts power dynamics, potentially disrupting traditional financial and governance structures.

·**Ethical Governance**: The decentralised nature of blockchain raises questions about accountability.

6. Problem Statement in Blockchain and Cryptocurrency

Several critical issues, including technical, regulatory, environmental, and social challenges, impede the adoption and integration of blockchain technology and cryptocurrencies.

Key Issues
Scalability and Performance
·**Problem**:face significant scalability issues. The ability to process transactions quickly and efficiently is limited, leading to high transaction fees and slow processing times.

·**Impact**: Scalability limitations hinder the ability of blockchain to support high-volume applications, such as global financial transactions and large-scale enterprise use cases.

Security Vulnerabilities
·**Problem**: Despite the inherent security features of blockchain, vulnerabilities in smart contracts, wallets, and exchanges present significant risks. Hacks and fraud have resulted in substantial financial losses and undermined trust in the technology.

·**Impact:** Security breaches can deter individuals and institutions from adopting blockchain and cryptocurrencies, limiting their growth and acceptance.

Regulatory Uncertainty
. **Problem:** The regulatory landscape for blockchain and cryptocurrencies is fragmented and

Environmental Impacts

· **Problem**: POW consensus mechanisms have significant environmental implications, particularly in Bitcoin mining. This raises concerns about the sustainability of blockchain technology.

· **Impact**: High energy consumption contributes to climate change and environmental degradation, prompting calls.

Privacy and Anonymity Concerns

· **Problem**: Blockchain's transparency can conflict with privacy requirements, as transaction data is publicly accessible. Additionally, the pseudonymous nature of cryptocurrencies can be exploited for illegal activities.

· **Impact**: Balancing transparency with privacy is challenging, and misuse of illicit activities can attract regulatory scrutiny and public distrust.

User Experience and Accessibility

·**Problem**: The complexity of blockchain technology and the user experience associated with cryptocurrency transactions can be daunting for non-technical users.

· **Impact**: Poor user experience and accessibility issues can limit mainstream adoption and the inclusivity of blockchain-based solutions.

Interoperability

· **Problem**: Different blockchain platforms often operate in silos, lacking interoperability with other systems and blockchains.

·**Impact**: The lack of interoperability hinders the seamless exchange of data and assets across different blockchain networks, limiting the potential for integrated solutions.

Economic and Social Implications

· **Problem**: The rise of cryptocurrencies has economic and social implications, including the potential for financial instability, inequality, and the impact on traditional financial systems.

· **Impact**: These implications necessitate carefully considering how cryptocurrencies affect broader economic and social structures, ensuring that benefits are maximised while mitigating negative effects.

Attacks on blockchain technology and cryptocurrency

While offering robust security features, blockchain technology and cryptocurrency are not impervious to attacks. Here are some of the notable attack vectors:

51% Attack

A 51% attack happens when a single entity or group controls over 50% of the network's mining hash rate.

Double-Spending Attack

Double-spending involves spending the same cryptocurrency more than once, including:

· **Race Attack**: The attacker sends two conflicting transactions in quick succession.

·**Finney Attack**: A mined block with a transaction is withheld until a new transaction is broadcasted.

·**Vector76 Attack**: A combination of race and Finney attacks exploiting network latency.

Phishing and Social Engineering

Phishing attacks deceive users into revealing private keys or credentials through fake websites, emails, or messages. This can lead to unauthorised access to wallets and funds.

Malware and Ransomware

Malware can be used to:
·Steal private keys from infected devices.

·Hijack computing power for mining (cryptojacking).

·Encrypt user files and demand cryptocurrency payments for decryption (ransomware).

7. Smart Contract Vulnerabilities

Smart contracts are susceptible to bugs and vulnerabilities. Common issues include:
·Re-entrancy Attack: This attack exploits the ability to call back into the same contract before the previous function execution is completed, often leading to fund drains.

·Integer Overflow/Underflow: Bugs that result from numerical calculations exceeding or falling below their defined limit, potentially causing unintended contract behaviour.

·Front-Running: Attackers exploiting the transaction order to benefit from pending transactions.

7.1. Solutions on blockchain technology and cryptocurrency

Various solutions and best practices can be implemented to mitigate the risks and vulnerabilities associated with blockchain technology and cryptocurrency. Here are some of the key strategies. The strategies include Enhanced Consensus Mechanisms, Smart Contract Security, Advanced Cryptographic Techniques, Decentralization and Network Robustness, User Education and Awareness, Regulatory Compliance and Standards, Scalability Solutions, Incident Response and Recovery, Privacy Enhancements andCollaboration and Research.

8. Conclusion on Blockchain Technology and Cryptocurrency

Blockchain technology and cryptocurrency represent transformative advancements with the potential to revolutionise various industries by providing decentralised, secure, and transparent systems. However, their widespread adoption comes with significant challenges and vulnerabilities.

Nazanin Moosavi covered various details, including block formations, protocol layers, consensus mechanisms, classifications of blockchain, obstacles faced, the value derived from blockchain technology, and their applications, which are thoroughly explained. Ultimately, this survey article presents a comprehensive examination of the fundamentals and structure of blockchain and its utilisation across multiple sectors, which we consider to be the highlight of this review.The future of blockchain technology and cryptocurrency is promising, with potential applications extending beyond finance to healthcare, supply chain, voting, and more. Continued innovation, collaboration, and adherence to best practices are essential to overcoming current challenges and unlocking the full potential of these technologies. As the ecosystem matures, the balance between decentralisation, security, scalability, and regulatory compliance will be crucial in shaping the trajectory of blockchain and cryptocurrency in future years.

References

[1] Rajput, S., Singh, A., Khurana, S., Bansal, T., Shreshtha, S. (2019). Blockchain technology and cryptocurrencies. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 909-912). IEEE. https://doi.org/10.1109/AICAI.2019.8701371

[2] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet 14*(11) 341. https://doi.org/10.3390/fi14110341

[3] Baboshkin, P., Mikhaylov, A., Shaikh, Z. A. (2022). Sustainable cryptocurrency growth impossible? Impact of network power demand on Bitcoin price. *Finans. Žhurnal Financ. J.*, 116-130. Available at: https://ideas.repec.org/a/fru/finjrn/220308p116-130.html

[4] Jabbar, R., Dhib, E., ben Said, A., Krichen, M., Fetais, N., Zaidan, E., Barkaoui, K. (2022). Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access, 10*, 20995-210310.

[5] Pagnotta, E. S. (2022). Decentralizing money: Bitcoin prices and blockchain security. *Review of Financial Studies, 35*, 866-907.

[6] Salem, H., Mazzara, M., Saleh, H., Husami, R., Hattab, S. M. (2022). Development of a blockchain-based ad listing application. In *Proceedings of the International Conference on Advanced Information Networking and Applications* (p. 1-7). Springer. https://doi.org/10.1007/978-3-030-67238-6_1

[7] Agrawal, D., Minocha, S., Namasudra, S., Gandomi, A. H. (2022). A robust drug recall supply chain management system using the Hyperledger blockchain ecosystem. *Computers in Biology and Medicine, 140* 105100.

[8] Sammeta, N., Parthiban, L. (2022). Hyperledger blockchain-enabled secure medical record management with deep learning-based diagnosis model. *Complex Intelligent Systems 8* 625-640.

[9] Boucher, O., Aloqaily, M., Tseng, L., Boukerche, A. (2020). Blockchain and fog computing for cyber-physical systems: The case of smart industry. *Computer 53*(6) 36-45.

[10] Astier, J. Y., Zhukov, I., Murashov, O. (2017). Smart building management systems and the Internet of Things. *Bezopasnost informacionnyh tehnology 2*(3) 2017.

[11] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings of the 2nd International Conference on Open and Big Data (OBD)* (p. 25-30). IEEE.

[12] Barinova, A., Zapechnikov, S. (2017). On the techniques and tools for privacy-preserving smart contracts. *Bezopasnost informacionnyh tehnology 2*(2) 2017.

[13] Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security 2013*(11) 5-8.

[14] Burgess, K., Colangelo, J. (2015). The promise of Bitcoin and the blockchain. *Consumers' Research*.

[15] Moosavi, N., Taherdoost, H., Mohamed, N., Madanchian, M., Farhaoui, Y., Khan, I. U. (2024). Blockchain technology, structure, and applications: A survey. In *Proceedings of the International Conference on Industry Sciences and Computer Science Innovation Blockchain Technology, Structure, and Applications: A Survey* (p. 645-658). Procedia Computer Science, 237.