

Blockchain and Bitcoin: Technical Foundations, Operating Mechanisms, and Security and Economic Challenges

Djafar Hamza

Ferhat Abbas University Setif 1, Algeria

Email: hamzadjafar@gmail.com

Meriem Bencheikh

Ferhat Abbas University Setif 1, Algeria

Email: bencheikh.meryem@gmail.com

Abstract

This study aims to highlight the role of blockchain technology in building a decentralised digital system, explain the issuance and operation of Bitcoin as the first application of blockchain, and examine decentralisation, cryptography, mining, and the challenges associated with them. The study found that blockchain constitutes an integrated technological system that combines mining and cryptography to provide security and trust in Bitcoin transactions. However, sharp price fluctuations limit its use as a medium of exchange and increase the risks associated with investing in it.

Keywords: blockchain, Bitcoin, decentralisation, mining

JEL classification: O33, G18

Introduction

Blockchain is one of the most prominent digital innovations because it provides security, transparency, and decentralisation in the recording and exchange of information. It first emerged as the foundation of Bitcoin, which represented its first practical application and paved the way for digital financial systems without traditional intermediaries. As it developed, its applications expanded to include finance, supply chains, healthcare, and smart contracts, thereby enhancing the efficiency and reliability of systems, facilitating information tracking and verification, and reducing manipulation and data loss.

Research problem: Although Bitcoin is the first successful and widely adopted application of blockchain technology, the adoption of this cryptocurrency raises questions about the effectiveness of blockchain in achieving security, transparency, and decentralisation in digital financial transactions. Hence, the research problem may be formulated as follows:

How does blockchain technology contribute to protecting the Bitcoin network and ensuring the sustainability of its transactions in light of economic and security challenges?

¹ Received: December 09, 2025; Accepted: July 10, 2026; Published: August 15, 2026



The following subquestions arise from the research problem:

- How does Bitcoin operate through blockchain, and which mechanisms ensure the continuity and reliability of transactions?
- What role does mining play in protecting the Bitcoin network and enhancing its security?
- What are the principal challenges facing blockchain and Bitcoin?

Research hypothesis: To address the research problem, the following hypothesis was formulated:

The decentralised architecture, cryptography, and mining mechanism of the blockchain network contribute to protecting Bitcoin and enhancing the reliability and sustainability of its transactions.

Research objectives: The study seeks to achieve the following objectives:

- To identify blockchain, the history of its emergence, and its operating mechanism;
- To examine blockchain applications, advantages, and challenges;
- To discuss Bitcoin and determine how it is issued;
- To identify the Bitcoin mining mechanism, its benefits, and the challenges associated with it.

Methodology: To achieve the intended objectives of this study, a descriptive-analytical approach was adopted by collecting and analysing data to understand the various aspects of the research topic.

The Concept and Characteristics of Blockchain

Historical Context of the Emergence of Blockchain

The fundamental ideas underlying blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 he presented the paper “The Part-Time Parliament” on consensus among unreliable computers, which was published in 1998. In 1991, the idea of using a signed chain of information to protect digital documents from alteration emerged. These ideas were subsequently brought together in the 2008 paper “Bitcoin: A Peer-to-Peer Electronic Cash System”, published by Satoshi Nakamoto. The Bitcoin network then appeared in 2009 as the first practical application of blockchain technology (Yaga & Mell, 2018, p. 2).

Definition of Blockchain

Blockchain is a digital ledger that records and verifies transactions transparently and in a tamper-resistant manner. What distinguishes this ledger is that it is not stored in one location but distributed across a large number of computers known as nodes (Rainstorm, 2023, p. 10).

It is also a type of database that stores information in interconnected blocks, each containing a set of transactions. The chain is distributed across several computers, making it extremely difficult to modify or delete recorded data (Jameson, 2024).

Thus, blockchain may be defined as a distributed, encrypted digital database that serves as a permanent, secure ledger for transactions and the data recorded within it.

Characteristics of Blockchain

- Decentralisation: There is no central authority controlling the storage, verification, and processing of data; responsibility is distributed among all network participants.
- Trust and transparency: Blockchain enables participants to view recorded information, thereby enhancing transparency and trust among them.
- Verification and security: It enables recorded transactions to be verified and protected through encryption, reducing the possibility of manipulation or unauthorised alteration.
- Multiple applications: Its uses extend from finance to numerous sectors, including supply chains, where it is used to track products and verify their origins.

- Immutability: Transactions are recorded within interconnected blocks, making their modification or deletion extremely difficult and enhancing the integrity and credibility of records (Rainstorm, 2023, p. 13).

Operating Mechanism of Blockchain Technology

As its name suggests, a blockchain is simply a chain of blocks, each representing a set of transactions. Its distinguishing feature is that every block is linked to the preceding and subsequent blocks, creating a tightly connected sequential structure. The technology operates as follows:

Block creation and transaction recording: When a new transaction occurs, it is recorded in a new block that includes several transactions and is verified by network participants. Each block generally contains the following elements (Fédération Wallonie, 2022, p. 4):

- Index: Identifies the block's position in the chain.
- Timestamp: Identifies the date and time at which the block was added.
- Data: Includes details of the transaction, such as the sender and recipient, and the amount.
- Hash: Converts the data into a fixed string of characters. Each block is linked to the hash of the previous block, making alteration of any block almost impossible and ensuring the security and reliability of the information.
- Previous block hash: Ensures the interconnection between blocks.
- Nonce: A random number used to generate a new hash.

Transaction recording: Once a transaction is initiated, the nodes in the network temporarily record it in a new block pending verification. Each block contains a set of transactions, after which the blocks are linked in chronological order to form an interconnected and unbreakable chain. This process preserves information and transactions in a permanent ledger and maintains the continuity of the transaction history (Rainstorm, 2023, p. 15).

Block encryption: Before a block is added to the chain, it is assigned an encrypted code known as a hash, a unique signature that identifies the block's content and distinguishes it from other blocks. This code is generated by solving complex mathematical problems. Each block contains its own hash and the hash of the previous block. This interconnection makes data alteration practically impossible. Any attempt to alter a block changes all subsequent hashes and requires all blocks to be mined again, which demands enormous amounts of energy and resources.

Mining and transaction verification: The process of validating transactions and adding them to new blocks is called mining. A miner uses substantial computing power to test a vast number of nonce values until a hash satisfying the required conditions is obtained, that is, until complex mathematical equations are solved. When a miner succeeds:

- The new block is added to the chain.
- The miner receives a reward, usually in the form of cryptocurrency such as Bitcoin.

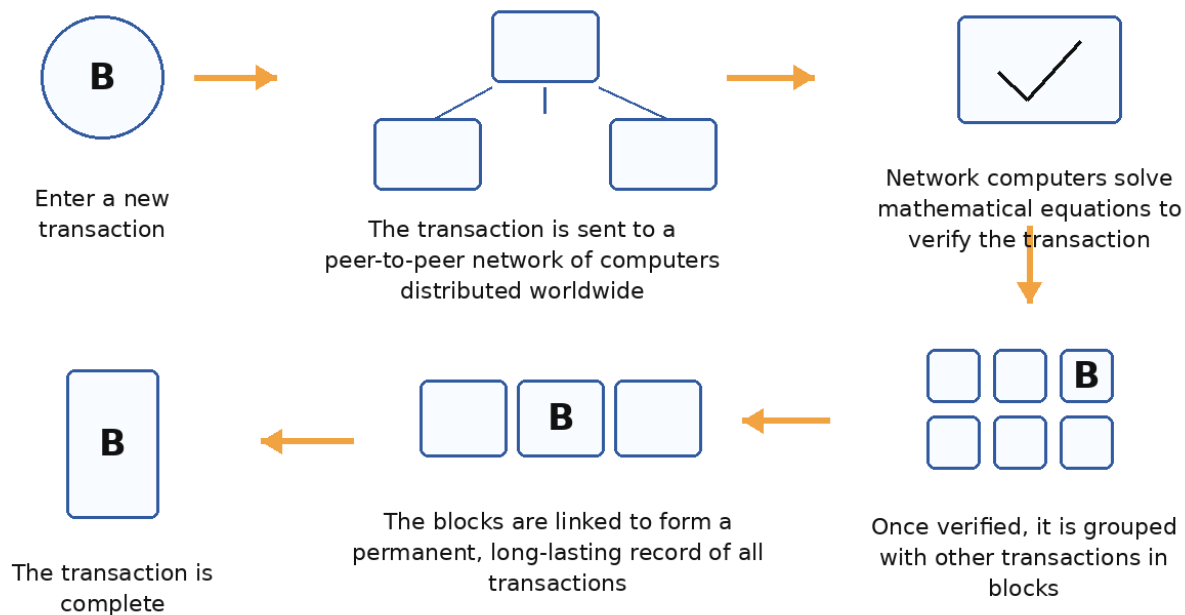
Mining therefore provides an incentive mechanism that ensures the network continues to operate and be maintained; however, it also consumes large amounts of computing power and electricity (Fédération Wallonie, 2022, p. 8).

Adding the block to the chain and updating the ledger: Once the equations have been solved and verified, the new block is permanently added to the chain, and all network participants (nodes) receive a copy of the ledger containing all transactions since the network's creation. Each block is linked to the previous block, forming a sequential chain, which makes altering any block difficult because all subsequent blocks would have to be rebuilt. The operating mechanism of blockchain technology is illustrated in the following figure.

Figure

Blockchain Operating Mechanism

1



Note. Prepared by the researchers using Microsoft Visio.

The figure above illustrates the stages of a transaction on a blockchain network. The process begins with the entry of a transaction and its broadcast across the peer-to-peer network, after which its validity and freedom from double spending are verified. It is then grouped with other transactions into a new block, which is added to the blockchain, thereby creating a permanent and transparent record. Finally, the transaction becomes immutable and irreversible, enhancing security and trust in the network.

Decentralised Architecture and Cryptographic Mechanisms in the Blockchain Network

Blockchain differs from centralised systems because it relies on a decentralised peer-to-peer network in which nodes retain copies of the chain and collectively verify new blocks. This structure ensures the following:

- Continuity: The failure of a single node does not stop the network.
- Security: The absence of a central point reduces the risk of attacks.
- Transparency: Recorded information is available to participants.

Blockchain also relies on asymmetric cryptography, using a public key to verify transactions and a private key to sign them and prove ownership, thereby protecting them from forgery and impersonation. Blockchain thus constitutes an integrated system of decentralisation, mining, and cryptography that achieves security and trust.

Blockchain Applications and Advantages

Blockchain Applications

Blockchain technology initially emerged as a means of protecting digital records from manipulation. With the emergence and spread of Bitcoin, the technology expanded into multiple fields and began serving different sectors through wide-ranging applications, including the following (Becher, 2026):

- Banking: Blockchain is used for currency exchange, loan security, and payment processing, while transactions are recorded immutably. This reduces fraud, accelerates settlement, and lowers transfer costs.

- Smart contracts: Self-executing protocols programmed according to specific conditions, intended to reduce errors, automate processes, and eliminate intermediaries.
- Cybersecurity: Blockchain provides advanced protection for data and assets through encryption, decentralisation, and the immutability of the ledger. It is used in banking, healthcare, the Internet of Things, and other sectors.
- Healthcare: It is used to protect and encrypt patient data and medical records, facilitate the secure exchange of these records, and automate processes such as insurance claims and treatment monitoring.
- Supply chains: They enable the tracking of goods and shipments from production to delivery, improving transparency and quality and reducing the number of intermediaries.
- Non-fungible tokens (NFTs): These represent unique digital assets and establish ownership on the blockchain; they are used particularly in digital art and electronic games.
- Insurance: It helps track claims, reduce fraud, enhance transparency, automate procedures, and reduce paper-based transactions.
- Retail: It contributes to tracking products and verifying their origin and ethical production practices through quick-response codes and the Internet of Things.
- Real estate: It is used to record property ownership and transaction histories, simplify verification and document exchange, and reduce costs by limiting reliance on intermediaries.
- Government: It can facilitate voting processes, reduce fraud, and enhance transparency and trust in electoral systems.

Blockchain represents a technological revolution that is not limited to cryptocurrencies but extends to various economic and social fields. The essence of this technology lies in the following (Fédération Wallonie, 2022):

- Decentralised transaction management.
- Security based on cryptography.
- Transparency that enhances trust.

Advantages of Blockchain

The blockchain system possesses several distinguishing advantages, most notably the following (Annappa et al., 2022, pp. 50–51):

- Transparency: Blockchain enables participating parties to view data, enhancing the clarity and traceability of transactions.
- Availability: The multiplicity of nodes ensures service continuity and data availability, so the failure of a single node does not stop the system.
- Reliability: It enables the secure, reliable storage and transfer of valuable assets, such as money and contracts.
- Trust: Blockchain protects against manipulation, fraud, and cybercrime; trust derives from its technical architecture rather than a central authority.
- Security: It relies on cryptography and mechanisms for inter-node cooperation to protect data and transactions and strengthen system security.
- Cost reduction: It helps reduce the costs of transferring and storing value by simplifying and automating processes in comparison with traditional systems.
- Efficiency: It improves process efficiency by making data available to the right parties at the right time, particularly in supply chains.

Challenges Facing Blockchain Technology

Although this emerging technology is considered resistant to manipulation, it is not without limitations. The principal challenges currently facing blockchain technology are as follows (Becher, 2026):

- Transaction limitations: Some blockchain networks struggle to process large numbers of transactions rapidly and efficiently, resulting in network congestion, higher transaction fees, and limited adoption.
- Energy consumption: The proof-of-work mechanism consumes significant energy due to its high computational requirements. Consequently, alternative mechanisms such as the less energy-intensive proof-of-stake model are increasingly being adopted.
- Scalability problems: Requiring each node to retain a copy of the chain and process transactions slows and congests the network, particularly during peak periods. This has prompted the development of solutions such as Layer 2 and sharding.
- Regulatory challenges: Governments and regulatory bodies continue to struggle to adapt legal frameworks to the decentralised nature of blockchain, perpetuating legal and regulatory uncertainty.

Bitcoin as the First Practical Application of Blockchain

Bitcoin is the first practical application of blockchain technology and the first decentralised digital currency. It was created by an unidentified person or group using a pseudonym. It is among the best-known and most widely adopted digital currencies and is called “digital gold” because of the value it has acquired in global markets.

History of Bitcoin

In 2008, Satoshi Nakamoto published a research paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System”, marking the beginning of cryptocurrencies and a new phase of digital financial innovation.

Bitcoin first appeared in 2009, when Nakamoto mined the first block in the Bitcoin blockchain, known as the Genesis Block. This block is regarded as the “big bang” of the digital currency world. The first block contained an encrypted message stating, “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”, which has been interpreted as direct criticism of the traditional banking system (Rainstorm, 2023, p. 6). In the same year, Satoshi mined the first block and received a reward of 50 bitcoins, thereby establishing Bitcoin as a decentralised electronic cash system. The first Bitcoin transfer occurred when Satoshi gave 10 bitcoins to the American programmer Hal Finney. Thereafter, Bitcoin circulated more extensively online and was accepted for payments and transaction settlement (Al-Kouh, 2024, p. 1318). In 2010, cryptocurrencies witnessed their first real-world Bitcoin transaction when a digital currency holder named Laszlo Hanyecz purchased two pizzas for 10,000 bitcoins. This transaction is highly symbolic in Bitcoin’s history and reflects the currency’s changing value over time (Rainstorm, 2023, p. 6).

As Bitcoin developed, its popularity increased and demand for it as an investment instrument grew substantially in what became known as the “digital gold rush”. This encouraged mining and trading and created a need for further innovation.

In 2011, Litecoin emerged as the first alternative cryptocurrency, offering faster transaction execution and using a different algorithm.

In 2013, the cryptocurrency market witnessed the collapse of Mt. Gox, one of the largest Bitcoin trading platforms. This caused major losses for investors and raised concerns regarding platform security and the need to strengthen user protection (Rainstorm, 2023, p. 6).

Security Factors in the Bitcoin System

The principal factors that provide Bitcoin with this high level of protection and security include the following (Al-Halwani, 2018, p. 50, adapted):

- Decentralised architecture: There is no single central point that can be targeted, making the Bitcoin network more resistant to attacks.

- Independence from any central authority: No single government or institution controls the system, preventing the imposition of alterations or the creation of a “back door”.
- Wide network distribution: The Bitcoin network is distributed across thousands of devices worldwide, and nodes retain copies of the database, making the records difficult to control or manipulate.
- Interconnection of blocks and transaction chains: Each block is connected to its previous blocks; therefore, changing any information requires altering all subsequent blocks.
- Volume of data requiring alteration: Changing the ledger would require rebuilding more than 500,000 blocks, while a new block is produced approximately every 10 minutes, making manipulation extremely difficult.
- Technical complexity and the high cost of intrusion: Mining requires advanced equipment, substantial energy, and effective cooling systems, increasing the cost of manipulating the network.
- Required computing power: Block production requires enormous computing capabilities beyond those of ordinary computers, making network manipulation extremely costly and complex.

Bitcoin Mining and Issuance Mechanism

Bitcoin is a cryptocurrency based on blockchain technology and is produced through mining, which requires powerful computing equipment and substantial energy consumption, raising concerns about its environmental impact (Rainstorm, 2023, p. 22). Mining involves adding new blocks and issuing Bitcoin units by testing different nonce values until a hash that satisfies the network's conditions is found. This process requires considerable computing power and proceeds as follows:

Approximately every 10 minutes, miners obtain the data needed to create a new block and search for the appropriate nonce value to produce a valid hash. When one miner succeeds, the block is added to the chain and the miner receives a reward and transaction fees, while the others continue trying.

The block is then sent to all nodes for independent verification. Once its validity has been confirmed, the transaction ledger is updated, and the new block is added, ensuring the network's continued operation (Wilson, 2025).

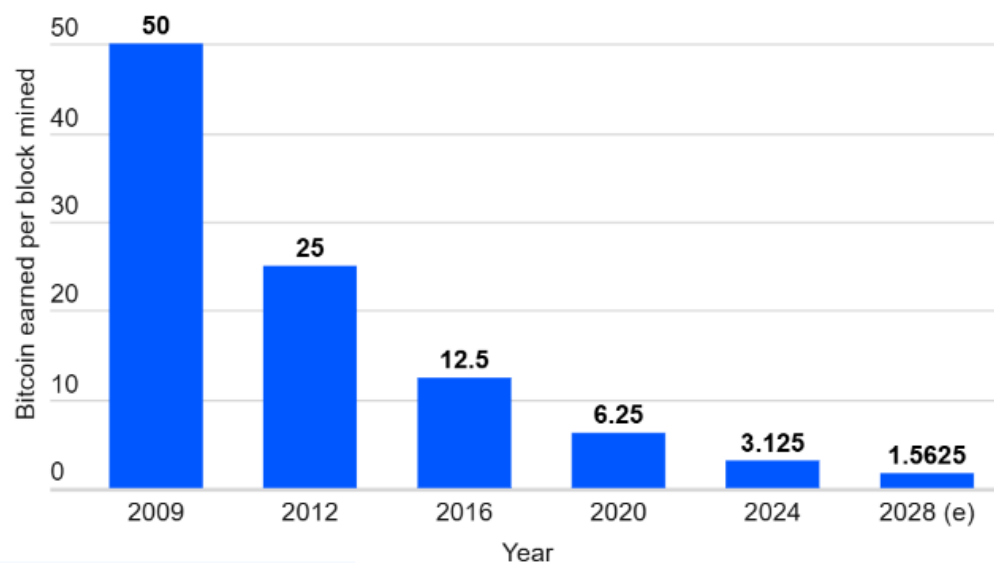
Bitcoin Mining Rewards and Their Calculation

When Bitcoin was created in 2009, the reward for mining a new block was 50 bitcoins. This reward is halved after every 210,000 blocks, or approximately every four years. It fell to 25 bitcoins in 2012 and then to 12.5 bitcoins in 2016. By 2140, the year in which the final Bitcoin unit is expected to be mined, the block reward is expected to become extremely small. This gradual reduction is known as Bitcoin halving (Wilson, 2025). Bitcoin halving refers to reducing the block reward by half every 210,000 blocks, or approximately every four years. This reduces the rate at which new Bitcoin units are issued and increases their scarcity. Bitcoin issuance is capped at 21 million units. When this limit is reached in approximately 2140, miners will rely on transaction fees as a source of income for mining operations (Wilson, 2025). The following figure shows Bitcoin mining rewards over time.

Figure

Bitcoin Mining Rewards Over Time

2



Note. Prepared by the researchers using Microsoft Excel.

Benefits and Challenges of Bitcoin Mining

Benefits of Bitcoin mining: Bitcoin mining provides several important benefits to individual miners and the Bitcoin network as a whole, most notably the following (Sherrard-Bewhay, 2025):

- Network security: Bitcoin mining helps verify transactions and prevent double spending, thereby maintaining the blockchain's integrity and security.
- Transaction verification: Mining ensures that transactions are valid and comply with network rules, thereby enhancing trust in the system.
- Creation of new bitcoins: Mining is the mechanism by which new Bitcoin units are issued and added to the circulating supply while maintaining their scarcity.
- Support for the decentralised network: Miners help strengthen the Bitcoin network's decentralisation and distinguish it from centralised financial systems.
- Potential profitability: Miners can earn financial returns through rewards in newly issued bitcoins when they successfully mine blocks.

Risks and Challenges Facing Mining

Bitcoin mining is not free from risks and challenges, most notably the following (Sherrard-Bewhay, 2025):

- Regulatory uncertainty: Ongoing changes to the laws governing Bitcoin mining may affect mining operations.
- Security risks: Miners face risks of hacking and theft that may result in the loss of coins or equipment.
- Environmental impact: High energy consumption raises environmental concerns and complicates balancing profitability and sustainability.
- Market volatility: Substantial fluctuations in Bitcoin's price may adversely affect mining profitability.
- Competition: Bitcoin mining is highly competitive, making it difficult for new miners to enter the field, as large operations have more efficient equipment and benefit from lower electricity costs.

Methods and Tools

The methods and tools used must be presented accurately, clearly, and concisely, enabling other researchers to replicate the study or verify its findings. Where necessary, particularly in complex cases, these methods may be illustrated using a diagram, table, or graph to simplify them.

Study Findings

The study yielded the following findings and recommendations:

- Blockchain is a promising technology for developing financial and commercial systems because it provides decentralisation, transparency, security, and reliability.
- The decentralised architecture contributes to network continuity and protects transactions without the need for a central intermediary.
- Blockchain relies on the integration of mining, peer-to-peer networks, and cryptography to ensure transaction security.
- Bitcoin is the first practical application of blockchain and the first decentralised digital currency; however, its mining requires high energy consumption, raising environmental concerns.
- Mining contributes to transaction verification and protects the network from manipulation, thereby enhancing trust in it.
- Despite Bitcoin's attractiveness as an investment, it faces challenges associated with the absence of central oversight, price volatility, and illegal uses.

Recommendations

- Establish clear legal frameworks to regulate cryptocurrency trading and limit its use in illegal transactions.
- Enhance financial awareness of Bitcoin's risks, particularly its volatility, digital fraud, and the lack of centralised protection.

Conclusion

In conclusion, blockchain technology represents a significant transformation in digital systems by providing transparency, reliability, and decentralisation in the management of data and transactions. Bitcoin is its most prominent application, enabling the secure trading of digital assets outside traditional financial systems and providing a means to preserve value and address certain economic challenges.

References

- Al-Halwani, M. (2018). *Blockchain, cryptocurrencies, and international financial law* [In Arabic]. Al-Halwani Academy.
- Al-Kouh, M. A. B. O. (2024). The nature of smart contracts [In Arabic]. *Journal of the Faculty of Sharia and Law*.
- Annappa, B., et al. (2022). *Blockchain technology and applications*. CRC Press.
- Baker, B. (2025, June 12). *Bitcoin mining: A beginner's guide to how it works*. Bankrate. <https://www.bankrate.com/investing/what-is-bitcoin-mining/>
- Becher, B. (2026, January 15). *Blockchain: What it is, how it works, why it matters*. Built In. <https://builtin.com/blockchain>
- Fédération Wallonie. (2022, December). *Introduction au blockchain*. Bruxelles.
- Hayes, A. (2025, December 25). *Blockchain facts: What it is, how it works, and how it can be used*. Investopedia. <https://www.investopedia.com/terms/b/blockchain.asp>
- Jameson, C. (2024). *Blockchain et affaires avec des actifs numériques pour les débutants*. Digital World.
- Rainstorm, L. Z. (2023). *Cryptocurrency 101: Everything you need to know about digital currencies and blockchain technology*. Shuttle Systems.
- Reddy, D. N., & Pathipati, H. (2024). *Cryptocurrency and blockchain technologies*. Leilani Katie Publication.
- Sherrard-Bewhay, J. (2025, February 25). *What is Bitcoin mining and how does it work?* Bankless Times. <https://www.banklesstimes.com/cryptocurrency/bitcoin/mining/>
- Wilson, S. (2025, January 16). *What is Bitcoin mining?* CoinFlip. <https://coinflip.tech/blog/bitcoin-mining-101>
- Yaga, D., & Mell, P. (2018). *Blockchain technology overview*. National Institute of Standards and Technology.