

Distributed Ledger Technology Through Blockchain Networks and Consensus Mechanisms

Luis Eduardo Muñoz Guerrero

Facultad de Ingenierías, Universidad Tecnológica de Pereira, Pereira, Risaralda, Colombia

ORCID: <https://orcid.org/0000-0002-9414-6187>

lemunozg@utp.edu.co

ABSTRACT

Blockchain technology has emerged as one of the most significant innovations in the field of computer science and information technology in recent decades. This document presents a comprehensive analysis of the fundamentals, characteristics, applications, and challenges of blockchain technology. The basic concepts that underpin this technology are explored, including its decentralized architecture, consensus mechanisms, and cryptographic properties. Additionally, various applications of blockchain beyond cryptocurrencies are examined, covering sectors such as supply chain, healthcare, finance, and public administration. The main objective of this work is to provide a comprehensive understanding of blockchain and its potential to transform multiple industries. Both the advantages and current limitations of this technology are discussed, as well as future perspectives for its development and adoption.

Keywords: Blockchain, Cryptocurrencies, Decentralization, Distributed Technology, Computer Security, Cryptography, Consensus Mechanisms.

1. INTRODUCTION

In today's digital era, secure and efficient data management has become a fundamental challenge for organizations and individuals. Blockchain technology represents an innovative solution to this challenge, offering a distributed ledger system that promises to revolutionize the way we store, share, and verify information. Blockchain initially emerged as the underlying technology of Bitcoin, the first decentralized cryptocurrency, but its potential extends far beyond financial applications.

The importance of blockchain lies in its ability to create immutable and transparent records without the need for a central authority. This fundamental characteristic has profound implications for numerous sectors of the economy and society. In a world where trust in traditional institutions has been questioned, blockchain offers an alternative mechanism to establish trust through technology and mathematics rather than relying solely on intermediaries.

This document aims to provide a comprehensive view of blockchain technology, exploring its technical foundations, practical applications, and the challenges it faces. Through this analysis, we seek to contribute to the understanding of this emerging technology and its potential to transform various aspects of our digital society. The structure of this paper is organized as follows: Section 2 discusses the fundamental concepts of blockchain technology, Section 3 examines its main characteristics, Section 4 explores various applications across different industries, Section 5 analyzes the challenges and limitations, Section 6 presents future perspectives, and Section 7 concludes the paper.

2. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Blockchain, or chain of blocks, is essentially a distributed database that maintains a continuous and growing record of transactions or data. The fundamental structure of blockchain consists of a series of chronologically linked blocks, where each block contains a set of transactions or information. Each block is connected to the previous block through a cryptographic hash, thus forming an immutable chain of records. This architecture ensures that once data is recorded, it becomes extremely difficult to alter retroactively without detection by the network.

A typical block in a blockchain contains several essential components. First, there is the block header, which includes important metadata such as the timestamp, the hash of the previous block, and a special number called nonce that is used in the mining process. Second, there is the block body, which contains the actual transactions or data being recorded. Each transaction within the block is verified and validated before being included. The block header also contains a Merkle root, which is a hash of all the transactions in the block, providing an efficient way to verify the integrity of the data.

The concept of hash is fundamental to understanding blockchain. A hash is a mathematical function that takes an input of any size and produces a fixed-size output. This output is unique for each specific input, which means that even a minimal change in the input data will produce a completely different hash. This property is crucial for the security and immutability of blockchain. Common hash functions used in blockchain include SHA-256, which is used by Bitcoin, and Keccak-256, which is used by Ethereum.

One of the most distinctive characteristics of blockchain is its decentralized nature. Unlike traditional databases

that are controlled by a central entity, a blockchain is maintained by a network of geographically distributed nodes. Each node in the network maintains a complete or partial copy of the blockchain, which eliminates the single point of failure that characterizes centralized systems. This distributed architecture is what gives blockchain its resilience and resistance to censorship. Decentralization offers several significant advantages. First, it increases system resilience, as the network can continue functioning even if some nodes fail or are attacked. Second, it reduces dependence on intermediaries, which can decrease costs and increase efficiency. Third, it distributes power and control among multiple participants, which can promote greater equity and transparency. However, decentralization also presents challenges. Coordination among multiple nodes requires sophisticated consensus mechanisms, which can be computationally expensive. Additionally, decision-making in a decentralized system can be slower and more complex than in a traditional centralized system. Consensus mechanisms are protocols that allow nodes in a blockchain network to agree on the current state of the blockchain. These mechanisms are essential for maintaining the integrity and consistency of the blockchain in a decentralized environment where there is

no central authority. The best-known consensus mechanism is Proof of Work, used by Bitcoin. In this system, miners compete to solve complex mathematical problems, and the first to find the solution has the right to add the next block to the chain. This process requires a significant amount of computational power and energy, which provides security by making attacks economically unfeasible. Another important mechanism is Proof of Stake, where validators are selected to create new blocks based on the amount of cryptocurrency they own and are willing to stake. This method is considerably more energy-efficient than Proof of Work, although it presents its own challenges in terms of security and decentralization. There are also other consensus mechanisms such as Delegated Proof of Stake, where token holders vote for a limited number of delegates who validate transactions, and Practical Byzantine Fault Tolerance, which is designed to work in environments where nodes may fail or act maliciously. The choice of the appropriate consensus mechanism depends on the specific requirements of the blockchain application in question, including considerations of security, scalability, and energy efficiency.

Table 1: Comparison of Major Consensus Mechanisms

Consensus Mechanism	Energy Efficiency	Transaction Speed	Decentralization Level	Security Model
Proof of Work	Low	Slow (7-15 TPS)	High	Computational power
Proof of Stake	High	Medium (15-30 TPS)	Medium-High	Economic stake
Delegated Proof of Stake	Very High	Fast (1000+ TPS)	Medium	Voting + stake
Practical Byzantine Fault Tolerance	High	Fast (1000-3500 TPS)	Low-Medium	Voting consensus

Table 1. Comparative analysis of different consensus mechanisms used in blockchain networks.

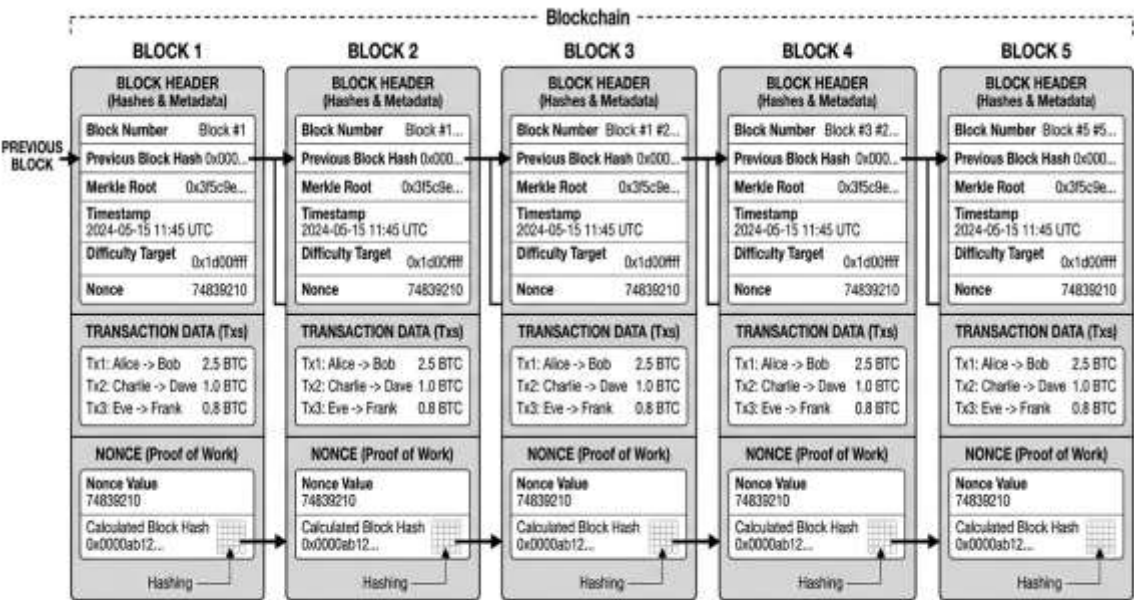


Figure 1. Illustration of blockchain structure showing blocks linked through cryptographic hashes.**3. MAIN CHARACTERISTICS OF BLOCKCHAIN**

Immutability is one of the most valuable properties of blockchain. Once a block has been added to the chain and confirmed by the network, it is extremely difficult, if not impossible, to modify or delete the information contained in that block. This characteristic is achieved through the combination of cryptographic hash functions and the linked chain structure. When someone attempts to modify an old block, the hash of that block would change, which would invalidate all subsequent blocks in the chain. For such a modification to be accepted by the network, the attacker would have to recalculate all subsequent blocks faster than the rest of the network is adding new blocks, which is practically impossible in a large and active network.

Immutability has important applications in areas where record integrity is crucial, such as in financial audits, medical records, and legal documentation. For instance, in financial auditing, the immutable nature of blockchain ensures that transaction records cannot be tampered with after the fact, providing auditors with a reliable source of truth. In the legal domain, smart contracts stored on blockchain can execute automatically when predefined conditions are met, and the record of execution is permanently stored. However, immutability also poses challenges, especially in relation to privacy regulations such as the General Data Protection Regulation (GDPR) in Europe, which includes a "right to be forgotten" that may require the ability to delete certain personal data.

Blockchain offers an unprecedented level of transparency. In a public blockchain, all transactions are visible to all network participants. Anyone can verify transactions and track the movement of assets through the chain. This transparency can increase trust and accountability in systems where it has traditionally been difficult to verify the authenticity of transactions. The transparency of blockchain is particularly valuable in scenarios where multiple parties need to trust the same data but do not necessarily trust each other. By making all transactions visible and verifiable, blockchain eliminates the need for a trusted third party to maintain the integrity of the records.

Traceability is particularly valuable in supply chain applications, where it is important to track the origin and movement of products. With blockchain, each step in a

product's journey can be recorded immutably, allowing consumers and regulators to verify the authenticity and origin of products. For example, in the diamond industry, blockchain is being used to track diamonds from mine to market, helping to ensure that they are not conflict diamonds. In the food industry, blockchain can track food products from farm to table, making it easier to identify the source of contamination in case of a food safety incident. However, total transparency may not be desirable in all contexts. In some cases, transaction privacy is important, which has led to the development of private blockchains and advanced cryptographic techniques that allow transactions to be verified without revealing all details.

Blockchain security is based on solid cryptographic principles. Cryptographic hash functions ensure that data cannot be altered without detection. Public key cryptography allows users to control their digital assets securely without needing to reveal sensitive information. Each user on a blockchain has a key pair: a public key, which functions as an address to which others can send transactions, and a private key, which is used to sign transactions and prove ownership of assets. The security of the system depends on users keeping their private keys secure. If a private key is lost, the associated assets become permanently inaccessible. If a private key is stolen, the thief can transfer the assets to their own control.

Although blockchain is generally very secure, it is not completely invulnerable. The 51% attack is a theoretical vulnerability where a malicious actor controls the majority of the network's computational power or stake, depending on the consensus mechanism. With this control, the attacker could potentially reverse transactions, double-spend coins, or prevent new transactions from being confirmed. However, such attacks are extremely costly and difficult to execute on large and established blockchains like Bitcoin or Ethereum. The cost of acquiring enough computational power or stake to execute a 51% attack on these networks would be prohibitively expensive, and the attack would likely cause the value of the cryptocurrency to plummet, making the attack economically irrational. Smaller blockchains with less computational power or stake securing them are more vulnerable to such attacks.

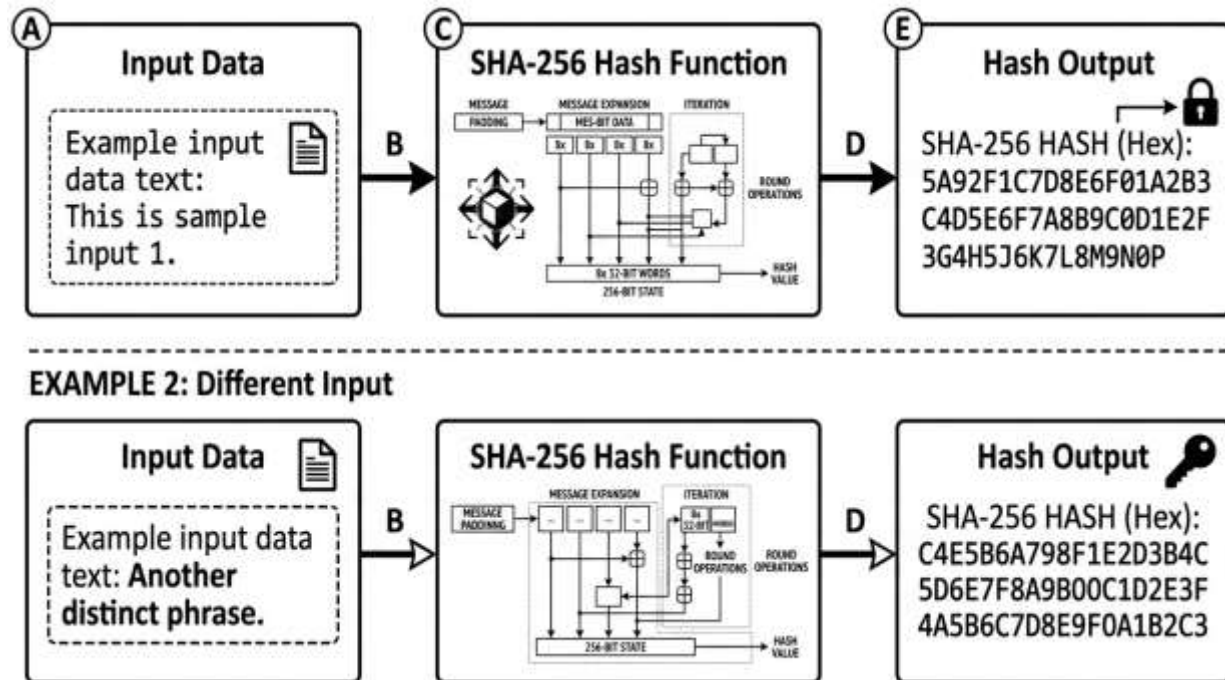


Figure 2. Cryptographic hash function process demonstrating how input data is transformed into fixed-size output.

4. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

The most well-known application of blockchain is cryptocurrencies. Bitcoin, created in 2009 by an anonymous person or group using the pseudonym Satoshi Nakamoto, was the first successful implementation of a decentralized digital currency. Since then, thousands of cryptocurrencies have been created, each with unique characteristics and purposes. Cryptocurrencies enable peer-to-peer transactions without the need for traditional financial intermediaries such as banks. This disintermediation can reduce transaction costs and increase the speed of transactions, particularly for cross-border payments. Bitcoin operates on a public blockchain where all transactions are transparent and verifiable by anyone.

Beyond simple cryptocurrencies, blockchain is being used to create more complex financial systems. Decentralized finance, commonly known as DeFi, uses smart contracts on blockchain platforms like Ethereum to replicate traditional financial services such as loans, exchanges, and insurance, but in a decentralized manner and without intermediaries. DeFi applications allow users to lend and borrow cryptocurrencies, trade assets on decentralized exchanges, and earn interest on their holdings through liquidity provision. The total value locked in DeFi protocols has grown significantly in recent years, demonstrating the increasing adoption of these decentralized financial services. However, DeFi also faces challenges including smart contract vulnerabilities, regulatory uncertainty, and scalability issues.

Traditional banks and financial institutions are also exploring blockchain to improve the efficiency of their operations. International transfers, which can traditionally take days and be expensive due to the involvement of multiple intermediary banks, can be performed in minutes with significantly reduced costs using blockchain. Several major banks have formed consortiums to develop blockchain-based systems for interbank transfers and settlements. For example, Ripple has developed a blockchain-based payment protocol that enables real-time cross-border payments. Central banks around the world are also exploring the possibility of issuing central bank digital currencies (CBDCs) using blockchain technology, which could provide the benefits of digital payments while maintaining central bank control over monetary policy.

Supply chain management is another area where blockchain is proving to be very valuable. The ability to track products from their origin to the final consumer in a transparent and immutable manner can help combat counterfeiting, improve efficiency, and increase consumer trust. Companies in industries such as food, pharmaceuticals, and luxury goods are implementing blockchain solutions to verify the authenticity of their products. For example, Walmart has implemented a blockchain-based system to track the origin of food products, which has reduced the time needed to trace the source of contaminated food from days to seconds. This rapid traceability is crucial in responding to food safety incidents and can help prevent widespread illness.

In the pharmaceutical industry, blockchain is being used to combat the problem of counterfeit drugs, which is estimated to be a multi-billion dollar problem globally.

By tracking drugs from manufacturer to patient through the supply chain on a blockchain, it becomes much more difficult for counterfeit drugs to enter the legitimate supply chain. The transparency provided by blockchain can also help ensure that products are produced ethically and sustainably. For instance, blockchain can be used to verify that products are made without child labor or that they meet environmental sustainability standards, allowing consumers to make more informed purchasing decisions based on their values.

In the healthcare sector, blockchain offers solutions to some of the most persistent challenges related to medical record management. Medical records stored on blockchain can be accessible to patients and authorized providers, while maintaining the privacy and security of sensitive information. Patients can have greater control over their medical data, deciding who can access it and for what purposes. This patient-centric approach to medical records is a significant departure from traditional systems where medical records are controlled by healthcare providers and patients have limited access to their own data.

Interoperability between different healthcare systems is an important problem that blockchain can help solve. Currently, medical records are often siloed in different healthcare systems that cannot easily communicate with each other. With blockchain, medical records can be securely shared between different institutions, improving continuity of care and reducing duplication of tests and procedures. This interoperability can lead to better health outcomes and reduced healthcare costs. Additionally, blockchain can be used in clinical trials to ensure the integrity of trial data and to provide transparency in the

reporting of trial results, which can help address concerns about publication bias and data manipulation in medical research.

Digital identity management is another promising application of blockchain. Blockchain-based identity systems can give individuals greater control over their personal information, allowing them to selectively share verified data without revealing unnecessary information. This concept, known as self-sovereign identity, puts individuals in control of their digital identities rather than relying on centralized identity providers. With a blockchain-based identity system, individuals can prove their identity or specific attributes about themselves without revealing all of their personal information. For example, someone could prove they are over 18 years old without revealing their exact date of birth.

In the realm of electronic voting, blockchain offers the possibility of creating voting systems that are both secure and transparent. Votes recorded on blockchain would be immutable and verifiable, potentially increasing trust in electoral processes. Blockchain-based voting could also make voting more accessible by enabling secure remote voting, which could increase voter participation. However, implementing blockchain-based voting systems presents significant technical and usability challenges that are still being addressed. Concerns include ensuring voter privacy while maintaining vote verifiability, protecting against coercion, and making the system accessible to all voters regardless of their technical sophistication. Several pilot projects have been conducted to test blockchain voting in various contexts, but widespread adoption has been limited due to these challenges.

Table 2: Blockchain Applications Across Different Industries

Industry Sector	Use Case	Key Benefits	Implementation Status
Finance	Cryptocurrencies & DeFi	Reduced costs, faster transactions	Mature
Supply Chain	Product tracking & authentication	Transparency, anti-counterfeiting	Growing
Healthcare	Medical records management	Interoperability, patient control	Pilot stage
Government	Digital identity & voting	Security, transparency	Experimental
Real Estate	Property records & smart contracts	Reduced fraud, efficiency	Early adoption
Energy	Peer-to-peer energy trading	Decentralization, efficiency	Pilot stage

Table 2. Overview of blockchain applications in various industry sectors with their current implementation status.

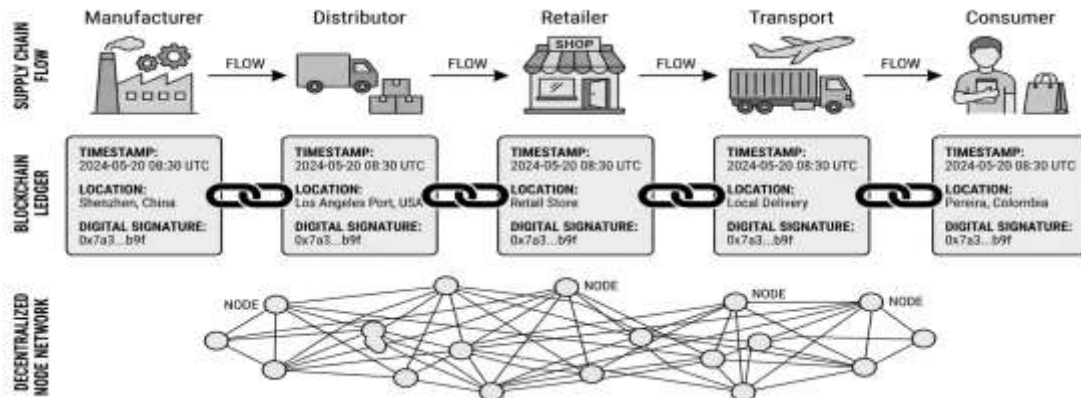


Figure 3. Blockchain-based supply chain tracking system showing product journey from manufacturer to consumer.

5. CHALLENGES AND LIMITATIONS

One of the most significant challenges facing blockchain is scalability. Public blockchains like Bitcoin and Ethereum have limitations in terms of the number of transactions they can process per second. Bitcoin, for example, can process approximately 7 transactions per second, while Ethereum can process around 15-30 transactions per second. In contrast, traditional payment systems like Visa can handle thousands of transactions per second. This limitation is partly due to the need for each node in the network to process and store all transactions. As the blockchain grows, storage and processing requirements increase, which can make it more difficult for individuals to participate as full nodes. This can lead to centralization, as only entities with significant resources can afford to run full nodes.

Several solutions are being developed to address the scalability problem. Second-layer solutions, such as the Lightning Network for Bitcoin, allow transactions to be conducted off-chain and only settled on the main blockchain periodically, significantly increasing transaction throughput. Sharding is another approach being explored, particularly by Ethereum, where the blockchain is divided into smaller segments called shards that can be processed in parallel. Each shard processes its own transactions and smart contracts, and the results are periodically synchronized with the main chain. Other approaches include increasing block size, which allows more transactions per block, and using more efficient consensus mechanisms that require less computational overhead.

The energy consumption of some blockchains, particularly those using Proof of Work, has been the subject of considerable criticism. Bitcoin mining, for example, consumes an amount of electricity comparable to the consumption of some small countries. This high energy consumption has significant environmental implications, especially if the electricity comes from non-renewable sources. The energy-intensive nature of Proof of Work has led to concerns about the sustainability of blockchain technology and its contribution to climate change. Critics argue that the environmental cost of blockchain, particularly for applications like cryptocurrency, may outweigh its benefits.

The transition to more energy-efficient consensus mechanisms, such as Proof of Stake, is one of the ways the industry is addressing this problem. Ethereum completed its transition from Proof of Work to Proof of Stake in September 2022, in an event known as The Merge. This transition reduced Ethereum's energy consumption by approximately 99.95 percent, demonstrating that blockchain can be made much more energy-efficient. However, it is important to note that this transition primarily addressed energy consumption without significantly increasing transaction throughput on the base layer. Other blockchains have been designed

from the start to use energy-efficient consensus mechanisms. However, Proof of Stake has its own challenges, including concerns about centralization, as those with more stake have more influence over the network, and the nothing at stake problem, where validators have little to lose by validating multiple competing chains.

The decentralized and often transnational nature of blockchain presents unique regulatory challenges. Governments and regulators around the world are struggling with how to regulate cryptocurrencies and other blockchain applications in a way that protects consumers without stifling innovation. The pseudonymous nature of many blockchain transactions has raised concerns about their use for illicit activities, such as money laundering, tax evasion, and financing of terrorism. These concerns have led some countries to impose strict regulations or even bans on cryptocurrencies. For example, China has banned cryptocurrency trading and mining, while other countries have taken a more permissive approach.

At the same time, other countries are adopting a more favorable approach, seeing blockchain as an opportunity for economic innovation and competitiveness. Some jurisdictions, such as Switzerland and Singapore, have developed regulatory frameworks that aim to provide clarity for blockchain businesses while protecting consumers. The lack of a clear and consistent regulatory framework at the international level creates uncertainty for companies and developers working with blockchain. Harmonization of regulations across different jurisdictions will be important for the future development of the technology. There are also questions about how existing laws apply to blockchain, such as securities laws, data protection laws, and contract laws.

Despite its potential, blockchain remains a complex technology that can be difficult to understand and use for the average user. Managing private keys, for example, requires a level of responsibility and technical knowledge that many users do not possess. The loss of a private key means permanent loss of access to associated assets, and there is no customer service to call to recover lost keys. This is fundamentally different from traditional financial systems where passwords can be reset and accounts can be recovered. The irreversibility of blockchain transactions is another usability challenge. Once a transaction is confirmed on the blockchain, it cannot be reversed, even if it was sent to the wrong address by mistake.

For blockchain to achieve mass adoption, user interfaces must be simplified and processes must be more intuitive. Better educational tools are needed to help people understand how blockchain works and how they can benefit from it. Wallet applications need to be designed with better user experience, including features like address books to prevent sending to wrong addresses, and

clear warnings about the irreversibility of transactions. Some solutions being explored include social recovery mechanisms, where users can designate trusted contacts who can help recover access to their accounts, and multi-

signature wallets, where multiple keys are required to authorize transactions, providing a balance between security and recoverability.

Table 3: Advantages and Challenges of Blockchain Technology

Aspect	Advantages	Challenges/Limitations
Scalability	Distributed processing	Limited TPS, growing storage requirements
Security	Cryptographic protection, immutability	51% attacks on small networks, key management
Energy	PoS mechanisms are efficient	PoW consumes significant electricity
Transparency	All transactions visible and verifiable	Privacy concerns, regulatory compliance
Decentralization	No single point of failure	Slower decision-making, coordination complexity
Cost	Reduced intermediary fees	High initial implementation costs
Usability	Programmable smart contracts	Complex for average users, steep learning curve

Table 3. Comparative analysis of the main advantages and corresponding challenges faced by blockchain technology.

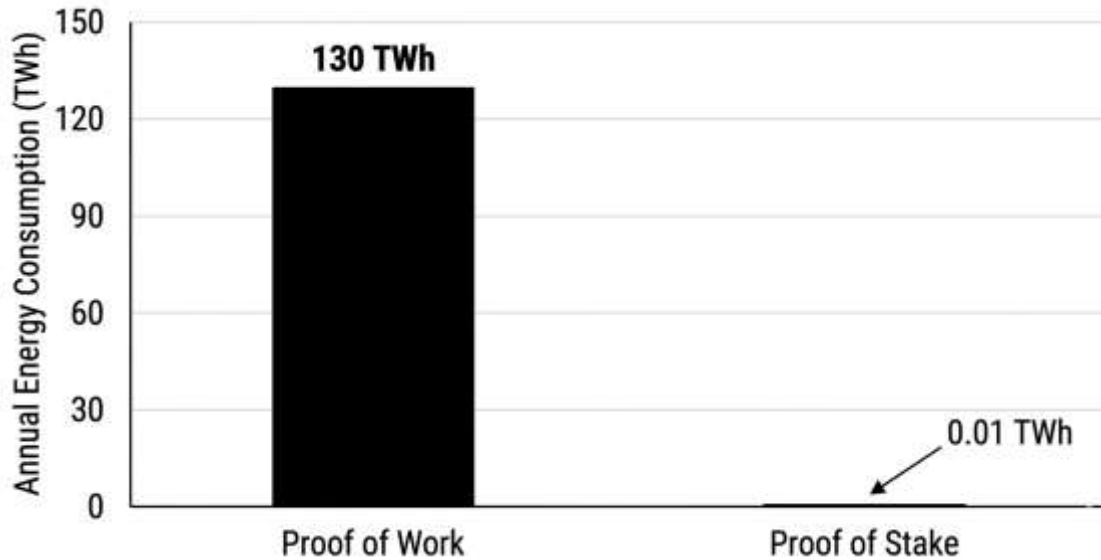


Figure 4. Energy consumption comparison between Proof of Work and Proof of Stake consensus mechanisms.

6. FUTURE PERSPECTIVES

The future of blockchain is promising but uncertain. As the technology matures, we are likely to see greater integration of blockchain into existing systems and the development of new applications that we have not yet imagined. Interoperability between different blockchains will become increasingly important, allowing different networks to communicate and share information efficiently. Currently, most blockchains operate in isolation, unable to directly interact with each other. Cross-chain bridges and interoperability protocols are being developed to address this limitation, enabling assets and data to move between different blockchains. This interoperability could unlock new use cases and increase the overall utility of blockchain technology.

The convergence of blockchain with other emerging technologies such as artificial intelligence, the Internet of Things, and quantum computing could open new possibilities. For example, IoT devices could use blockchain to communicate and conduct transactions autonomously and securely. Smart cities could use blockchain to manage infrastructure, energy distribution,

and public services in a transparent and efficient manner. Artificial intelligence could be combined with blockchain to create decentralized AI systems where data and models are shared securely among multiple parties. Supply chains could become fully automated with IoT sensors recording data on blockchain and smart contracts automatically executing based on that data.

However, there are also potential threats. Quantum computing, when fully developed, could break the current cryptographic algorithms on which blockchain is based. Most blockchain systems rely on cryptographic algorithms like ECDSA (Elliptic Curve Digital Signature Algorithm) for digital signatures, which are vulnerable to Shor's algorithm on quantum computers. Hash functions like SHA-256, while more resistant, would have their security reduced by Grover's algorithm, though they would still maintain significant security margins. The blockchain community is working on developing quantum-resistant cryptography to address this future threat. Post-quantum cryptographic algorithms are being researched and standardized, and some blockchain

projects are already beginning to implement quantum-resistant features.

Institutional adoption of blockchain is growing, with more companies and governments exploring and implementing blockchain solutions. Major corporations in various industries are investing in blockchain research and development. Financial institutions are exploring blockchain for clearing and settlement, trade finance, and digital asset custody. Governments are exploring blockchain for land registries, identity management, and public records. This institutional adoption could accelerate the development of standards and best practices, facilitating broader adoption. However, institutional adoption also raises questions about the balance between the decentralized ideals of blockchain and the centralized nature of many institutions.

The development of central bank digital currencies (CBDCs) represents a significant trend in the evolution of blockchain and digital currencies. Many central banks around the world are researching or piloting CBDCs, which would be digital versions of their national currencies. CBDCs could provide the benefits of digital payments, such as faster transactions and lower costs, while maintaining central bank control over monetary policy. However, the design of CBDCs raises important questions about privacy, financial inclusion, and the role of commercial banks in the financial system. Some CBDC designs use blockchain or distributed ledger technology, while others use centralized databases.

7. CONCLUSION

Blockchain represents a significant technological innovation with the potential to transform numerous aspects of our digital society. Its fundamental characteristics of decentralization, immutability, transparency, and cryptographic security offer solutions to problems that have been difficult to solve with traditional technologies. Throughout this document, we have explored the technical foundations of blockchain, its main characteristics, and its various applications in sectors ranging from finance to healthcare and supply chain management. We have also examined the significant challenges facing the technology, including scalability issues, energy consumption, regulation, and usability.

It is important to recognize that blockchain is not a universal solution for all problems. There are use cases where traditional or centralized databases are more appropriate and efficient. The key is to identify scenarios where the unique properties of blockchain provide real value. Blockchain is most valuable in situations where multiple parties need to share data but do not fully trust each other, where transparency and auditability are important, and where disintermediation can provide significant benefits. In other situations, the overhead and complexity of blockchain may not be justified.

As the technology continues to evolve and mature, we are likely to see solutions to many of the current challenges. Research and development in areas such as scalability,

energy efficiency, and usability are advancing rapidly. At the same time, the development of clearer regulatory frameworks will help provide the certainty needed for broader adoption. The blockchain industry is still young, and there is much room for innovation and improvement. New consensus mechanisms, layer-2 solutions, and cross-chain protocols are being developed to address current limitations.

For blockchain to reach its full potential, collaboration between developers, businesses, governments, and users will be necessary. Education and awareness about blockchain will also be crucial for its successful adoption. As more people understand the technology and its benefits, they are more likely to adopt it and contribute to its development. Universities and educational institutions are beginning to offer courses on blockchain, and industry certifications are being developed to standardize knowledge and skills in this field.

In conclusion, blockchain is a transformative technology that is still in its early stages of development and adoption. Although it faces significant challenges, its potential to create more transparent, secure, and efficient systems is undeniable. The future of blockchain will depend on how the technology community, businesses, and regulators work together to overcome these challenges and seize the opportunities that this technology offers. This document has provided an overview of blockchain, but there is much more to explore and learn. As the technology continues to evolve, it will be important to stay updated with the latest developments and continue researching how blockchain can be effectively applied to solve real-world problems. The next decade will be critical in determining whether blockchain lives up to its transformative potential or remains a niche technology with limited applications.

REFERENCES

- [1] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Porto, Portugal, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.
- [2] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, IEEE, 2016, pp. 25–30.
- [3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, May 2015, pp. 104–121, doi: 10.1109/SP.2015.14.
- [4] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, 2014. [Online]. Available: <https://ethereum.org/en/whitepaper/>
- [5] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based

- applications: Current status, classification and open issues," *Telematics Inf.*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.
- [6] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Systems Design Implement. (OSDI)*, USENIX, New Orleans, LA, Feb. 1999, pp. 173–186.
- [7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [8] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "BlockChain technology: Beyond Bitcoin," *Appl. Innov. Rev.*, no. 2, pp. 6–19, 2016.
- [9] A. de Vries, "Bitcoin's growing energy problem," *Joule*, vol. 2, no. 5, pp. 801–805, May 2018, doi: 10.1016/j.joule.2018.04.016.
- [10] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.
- [11] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. 18th Int. Conf. Financial Cryptography Data Security (FC)*, Springer, 2014, pp. 436–454, doi: 10.1007/978-3-662-45472-5_28.
- [12] M. Kouhizadeh and J. Sarkis, "Blockchain practices, potentials, and perspectives in greening supply chains," *Sustainability*, vol. 10, no. 10, p. 3652, Oct. 2018, doi: 10.3390/su10103652.
- [13] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.
- [14] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982, doi: 10.1145/357172.357176.
- [15] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, New York, NY, 2016, pp. 254–269, doi: 10.1145/2976749.2978309.
- [16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Bitcoin.org*, Oct. 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [17] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable off-chain instant payments," *Technical Report*, Jan. 2016. [Online]. Available: <https://lightning.network/lightning-network-paper.pdf>
- [18] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.
- [19] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.
- [20] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
- [21] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014. [Online]. Available: <https://ethereum.github.io/yellowpaper/paper.pdf>
- [22] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," *PLOS ONE*, vol. 11, no. 10, p. e0163477, Oct. 2016, doi: 10.1371/journal.pone.0163477.
- [23] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Honolulu, HI, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
- [24] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, Oct. 2018, doi: 10.1504/IJWGS.2018.095647.
- [25] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops (SPW)*, San Jose, CA, 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.