Unraveling Blockchain: An Exploration in Methods, Security, and Scalability for Cryptocurrencies

Jessica Ali
ODU Student, CS 463

***Abstract*—This report will examine blockchain technology as the foundational system behind cryptocurrencies, focusing on its structure, security, and scalability. We begin by defining major cryptocurrencies such as Bitcoin and Ethereum, then by exploring how blocks are cryptographically linked to ensure data integrity. Additionally, we analyze decentralized maintenance through consensus mechanisms like Proof-of-Work and Proof-of-Stake. Scalability challenges are addressed alongside solutions, including Ethereum 2.0 and the Lightning Network. Furthermore, we explore and discuss the role of cryptographic tools such as mining, digital signatures, and encryption in securing blockchain networks. Such as real-world applications beyond digital currency, supply chain tracking, and voting systems are also considered. We will conclude by reflecting on blockchain's advantages over traditional systems and the challenges that must be addressed for its broader adoption in the coming decade. We delve into the Unraveling of Blockchain through practical metaphors, case studies, and discussion.**

Keywords—Blockchain, Cryptocurrency, Bitcoin, Ethereum, Decentralization, Consensus Mechanisms, Scalability, Security, Cryptography, Real-World Applications

I. Introduction

One can argue that blockchain technology has emerged as a backbone of cryptocurrency systems, arguably revolutionizing how digital assets are stored, transferred, and secured [1],[2]. This report explores foundational components and operational methods of blockchain while delving into key scalability and security issues [2]. Specifically, it addresses 11 critical questions ranging from definitions of cryptocurrencies and blockchain to cryptographic techniques and real-world applications. As industries shift toward digital solutions, understanding the architectural foundation of blockchain becomes increasingly important. Blockchain is not just a tool for currency. However, it represents a broader paradigm for secure decentralized data sharing, which is exceptionally relevant to supply chain integrity, academic credential verification, and intergovernmental. Data exchanges. Therefore, this paper provides readers with the clarity needed to understand blockchain. Design answers a growing demand in a practical world. In a practical sense, Blockchain technology has become a key part of how cryptocurrencies like Bitcoin and Ethereum work, changing how digital money is stored, moved, and protected [1], [2]. This report breaks down the basics of how blockchain functions and closely examines common challenges—like making it scale for more users and keeping it secure [2]. It is built around 11 essential questions, covering everything from blockchain and cryptocurrency to how they work behind the scenes and where they are being used in the real world.

As more industries move toward digital solutions, it's becoming more important to understand how blockchain is built and why it matters. Blockchain is not just about money—it's also being used to help track goods in supply chains, protect academic records, and even share data between governments. This paper will give readers a clear and practical understanding of how blockchain is designed and why it is becoming so important in today's digital world.

II. CRYPTO AND EXAMPLES

Cryptocurrencies are decentralized digital currencies that utilize cryptographic principles to enable secure online financial transactions. Bitcoin, launched in 2009, was the first cryptocurrency to successfully apply these principles on a peer-to-peer network [3]. Ethereum is followed by more capabilities like smart contracts and decentralized applications [4]. Beyond Bitcoin and Ethereum, cryptocurrencies like Ripple focus on bank transfers, while Litecoin offers fast transaction speeds. One relevant case study is El Salvador's adoption of Bitcoin as legal tender in 2021 [4]. One real-life example of how a country tried to use cryptocurrency nationally is what happened in El Salvador. In 2021, the country made history by officially becoming the first to accept Bitcoin as legal money. To help people use it, the government created a digital wallet called Chivo and set up Bitcoin ATMs nationwide so that citizens could send, receive, or withdraw money easily.

This move showed the immense possibilities of using cryptocurrency to improve access to money, especially for people who do not have bank accounts. However, it also revealed some serious challenges. Many people did not fully understand how Bitcoin worked, and there was insufficient education or support to help them use the new system. On top of that, not everyone had the phones or internet needed to use the digital wallet. Some people did not trust the system or found it too confusing, which made adoption slow and unpredictable.

El Salvador's experience reminds us that while national cryptocurrency systems can be innovative, they also need careful planning, good technology, and lots of public education to work well.

Blockchain functions like a shared digital Ledger, recording every transaction made with cryptocurrencies such as Bitcoin or Ethereum. When someone sends or receives these coins, the transaction details, like the sender, receiver, and amount, are grouped with other transactions into a block. That block is then linked to the previous one using cryptographic codes called hashes, forming a chain of blocks. A chain is then stored and constantly updated by many computer nodes worldwide. Each node has a copy of the whole blockchain, and they work together to ensure new transactions are valid before adding them to this chain. Understandably, all changes must be approved by the network and added in a specific, secure way. No one can go back and secretly change transaction history. This makes it difficult to cheat or tamper with, allowing cryptocurrency to work without a central bank or authority. The example in El Salvador underscores the importance of aligning blockchain policy with real-world constraints and user readiness. While blockchain is explained above simply, it is not always the case in real-world practice and acceptance, yet we can consider El Salvador's adoption of Bitcoin as legal tender a success.

III. BLOCKCHAIN FUNDAMENTALS

At the blockchain core, a single blockchain is a digital letter composed of a growing list of records called blocks, each containing transaction data, a timestamp, A cryptographic hash, and a reference to the previous block's hash [5]. The previously explained features ensure blocks are immutable and sequentially linked, forming a secure data chain. Thus, this is where the. The name blockchain. Blockchain structure prevents unauthorized changes. Moreover, it arguably provides a trustworthy historical record reinforced by decentralized validation mechanisms [6]. One such mechanism, or using a Merkel tree(s), allows blockchains to summarize and validate large volumes of transactions efficiently, ensuring data integrity with minimal storage requirements. A mathematical proof system strengthening a trust model as an alteration to even a single bit of transaction data will result in an invalid hash alerting network or networks to potential tampering [5].

To explain more practically, at the blockchain core, blockchain is like a growing stack of digital boxes. Each box or block contains a list of recent transactions, the time they happened, and a special fingerprint called a hash. Each box also carries the fingertips of the box before it! This links them all together like a chain, hence the name. Once a box is added to the stack, it cannot be changed without messing up all the boxes before it. This is like pulling out one piece from a stack in the popular game Jenga. To look at it more mathematically, think of each block in a blockchain as a row in a ledger or a data set. Each block stores a list of transactions—just like a set of values—and includes a unique output called a hash, which is calculated using all the data in that block. This hash works kind of like a checksum or ID number. However, here is the catch: each block also stores the hash from the block before it. So, if you change just one value in one block, it changes that block's hash—and that messes up the connection to the next block, and the next, and so on. That makes blockchain so secure: the entire chain depends on every previous link staying the same. It is like a sequence where each number depends on the one before. Break the pattern, and the whole chain falls apart like knocking over a carefully balanced stack.

To ensure everything stays honest, many people (computers) on the network double-check each new box before it gets added. They use a Merkle tree tool, which summarizes all the information in the box into one neat line that's easy to check. If someone tries to sneak in a fake transaction—even changing just one tiny detail—it would change the box's fingerprint and alert the whole network that something is wrong.

IV. Block creation and Network Maintenance

To explain block creation and network maintenance, blocks are added to a blockchain through consensus mechanisms managed by a decentralized network of nodes [7]. Each node validates transactions and reaches an agreement before a new block is committed to or put in the chain. Unlike traditional centralized systems, blockchain operates on peer-to-peer. Models that distribute authority and eliminate single points of failure [8]. Each node maintains a copy of the entire blockchain, forming a resilient system together [7]. Arguably, it is a resilient system that will automatically reconcile discrepancies—using distributed algorithms [8]. The decentralized nature reduces the impact of node failures and deters collision, as malicious actions require controlling most of the network, such as in a 51% attack [7]. Thinking differently, one can think of a blockchain as a public notebook that anyone can see but no one can erase or secretly change. Whenever someone sends or receives cryptocurrency, it is like writing a new line in the notebook. These lines are grouped into pages called blocks, and once a page is complete, it is stapled to the last one. Forming a chain of pages. Before a new page is added, everyone in the room, such as the network of computers, checks the work to ensure it is correct. Because everyone has a copy of the notebook and watches the process, it is tough for anyone to manipulate the system. This system is how cryptocurrencies are secure and trustworthy without needing a bank to keep their records.

V. scalability and Performance

While blockchain theoretically allows infinite extension of its ledger, its Performance often suffers as chain length increases [9]. Issues such as latency, energy consumption, and limited transaction throughput become more prominent at scale. Various solutions, such as off-chain transactions and sharding, are proposed to address these bottlenecks and enhance scalability while preserving decentralization and security [10]. Ethereum's switch to Proof-of-Stake (PoS) under Ethereum 2.0 is one example of how developers address these scalability challenges [10]. Two solutions, like the Lightning Network and sidechains, also aim to offload transaction volume from the main chain, enabling microtransactions and higher throughput without sacrificing security [10]. A technical comparison can be made between Bitcoin and Ethereum regarding how they handle scalability. Bitcoin uses SegWit and the Lightning Network to enable faster off-chain transactions, while Ethereum has adopted rollups and is transitioning to sharding [9].

While a blockchain can grow forever—like a notebook with unlimited pages—the longer it gets, the harder it becomes to flip through quickly. As more people use it, the system can slow down, use more energy, and struggle to handle many transactions simultaneously. It is like a busy highway where too many cars cause traffic jams. To fix this, developers are finding clever ways to make traffic flow more smoothly. One idea is to move some of the cars onto side roads—this is called off-chain transactions. Another is to divide the road into lanes that can handle different tasks simultaneously, like sharding. Ethereum, for example, is switching to a new system called Proof-of-Stake (PoS) and adding sharding to make things faster and more efficient. Bitcoin takes a different approach. It adds tools like SegWit and the Lightning Network, which work like express lanes to speed up small payments. Ethereum uses rollups, which bundle many transactions into one, like putting many letters into one envelope. These different strategies are like tuning up different types of vehicles to make sure they all run smoothly on the digital road.

VI. consistency and security Measures

To maintain consistency across multiple nodes, blockchain systems utilize consensus algorithms like Proof-of-Work and Proof-of-Stake [11]. These protocols ensure that all participants agree on blocks' order and content despite a central authority's absence. Blockchain's cryptographic structure also prevents tampering and double-spending, strengthening its trustworthiness as a financial infrastructure [12]. These consensus protocols play a critical role in deterring double-spending, which would otherwise undermine the reliability of digital currencies [11]. By design, PoW requires extensive computational resources, creating a cost barrier for fraud, while PoS assigns block creation rights based on the validator's stake, promoting economic responsibility. Another big difference in how blockchains work is how they decide who adds the following block to the chain. Bitcoin uses Proof-of-Work, or PoW, while newer blockchains like Cardano and Ethereum 2.0 use Proof-of-Stake or PoS.

Proof-of-work is like a race where everyone solves challenging math problems. The first one to get the correct answer wins the chance to add a new block and earn a reward. However, this race uses a lot of electricity and powerful computers, which can be expensive and not eco-friendly. On the other hand, proof-of-stake is more like putting your name into a raffle. The more cryptocurrency you "stake" or lock up, the more tickets you get in the drawing. The winner is chosen randomly, but people with more at stake have a better chance. This system does not require as much energy and encourages people to play fair—because if they try to cheat, they risk losing their money. Both systems are designed to keep the network secure but work very differently. PoW is tried and tested, while PoS is newer and more energy-efficient, making it a popular choice for the future of blockchain. Blockchains use a group voting system called consensus algorithms to keep everyone on the same page. It is like a classroom where the students must all agree on the answer before moving on. These rules—like Proof-of-Work (PoW) and Proof-of-Stake (PoS)—make sure that all the computers in the network agree on what order things happen and what belongs in the next block, even though there is no teacher (or central authority) in charge.

Blockchain also uses cryptography, such as a lock and key, to keep records safe. This helps prevent cheating, like someone trying to spend the same money twice (called double-spending). Proof-of-work is like solving a challenging math puzzle that takes a lot of time and electricity—this makes cheating expensive and not worth it. On the other hand, proof-of-stake is like putting down a security deposit: people who want to add the following block have to risk their own money, so they have a reason to play fair. Bitcoin still uses PoW, which is slower but battle-tested. Newer systems like Ethereum 2.0 and Cardano have moved to PoS to save energy and encourage responsible participation. Each method has its trade-offs, but both are designed to keep the system secure and honest.

VII. CRYPTOGRAPHIC PUZZLES AND TECHNIQUES

Blockchain security is the cryptographic puzzle-solving process inherent in mining [13]. Often computationally intensive, these puzzles deter malicious actors by requiring significant resources to manipulate the chain. Cryptographic techniques such as hash functions, public-key cryptography, and digital signatures work together to secure transactions and authenticate users, forming the basis for blockchain's tamper-proof nature [14]. The puzzle difficulty adjusts dynamically based on the network's computing power, ensuring block intervals remain consistent regardless of fluctuations in mining activity. Another important part of blockchain security is elliptic curve cryptography, a fancy way to say that each digital wallet has a special lock and key. The private key is a secret password only the wallet owner knows. Without it, no one can move or spend the cryptocurrency inside that wallet—like only you can unlock your phone with your fingerprint or passcode. This ensures that only the real owner can approve transactions, keeping others from stealing or using the funds.

On top of that, blockchain adds another layer of protection, which is something called mining. You can think of mining as a giant digital competition where computers race to solve difficult math puzzles. These puzzles are so complex that they take a lot of time and electricity to solve, which keeps people from cheating or messing with the system. The first computer to solve the puzzle gets to add the following block of transactions to the chain and earns a reward. This process makes it very expensive and challenging for anyone to fake or change anything, helping keep the system fair and secure for everyone. The puzzles are so tricky that solving them takes time, energy, and computer power, making it hard for anyone to cheat or take over the system [13].To protect each transaction, blockchain uses different cryptographic tools. Hash functions act like digital fingerprints for each block, while public-key cryptography and digital signatures work like secure envelopes and handwritten signatures to prove who sent what. All these tools work together to keep the system safe from tampering [14]. The difficulty of these puzzles adjusts depending on how many players (computers) are trying to solve them. It is like a video game that gets harder when more people play, so its pace stays balanced. On top of that, digital wallets use a special kind of math called elliptic curve cryptography, which ensures that only the valid owner of a wallet can send money from it—like having a private key that only fits your lock.

VIII. REAL-WORLD APPLICATIONS AND ADVANTAGES

Blockchain technology extends beyond cryptocurrencies into supply chain management, healthcare, and digital identity verification. These applications benefit from blockchain's transparency, immutability, and auditability. In healthcare, blockchain ensures tamper-proof medical records are accessible only to authorized personnel, while in real estate, it streamlines property transfers by minimizing paperwork and third-party verification. IBM's Food Trust blockchain platform allows stakeholders in the food supply chain, from farms to retailers, to track products in real-time, improving traceability and reducing the impact of recalls [15]. Walmart has already implemented this to trace mangoes and pork in seconds rather than days. However, in scenarios where participants can rely on a trusted central authority, a conventional database will generally outperform a blockchain in speed and throughput, meaning that distributed ledgers become truly advantageous only when there is no single party that all users trust [16]. This illustrates how blockchain enhances transparency, operational efficiency, and consumer trust in global supply chains. Blockchain is not just for digital money—it is also like a super-secure digital notebook used in supply chains, healthcare, and ID verification. Because everyone can see what is written in the notebook (transparency), and no one can change past entries (immutability), it is great for tracking important information over time. In healthcare, it is like locking medical records in a digital vault that only the right doctors or nurses can open. Real estate cuts out many paperwork and mediators, making it easier to transfer property securely. One real-world example is IBM's Food Trust system. It is like giving every tomato or piece of pork a digital passport that lets companies trace where it has been, from farm to store shelf [15]. Walmart uses this system to track food in seconds instead of days. However, a regular database may work faster and more efficiently when everyone trusts a central party—like a reliable company or agency. Blockchain shines the most when everyone can trust no person or group [16]. That is when its built-in honesty and transparency make a real difference, especially in global supply chains where trust can be hard to come by.

IX. SUMMARY AND REFLECTION

Through this exploration, we understand how blockchain provides a highly secure, decentralized framework for digital interactions. Its strengths lie in its resistance to fraud, consistency without central oversight, and adaptability to various industries [17]. Even though blockchain has many benefits, it still faces significant challenges—like using too much energy, unclear rules from governments, and trouble working with older systems that were not made for it. Tripathi et al. emphasize that the long-term success of blockchain will depend on overcoming fundamental limitations, such as improving scalability and navigating regulatory hurdles, before the technology can reach its full transformative potential [18]. Based on Trpathi et al., one can argue that scalability solutions and evolving governance models will help blockchain technologies remain efficient and inclusive. Its impact on financial inclusion, particularly in regions with limited banking access, highlights the societal value it holds if implemented with ethical foresight. To think in a more practical sense and closer to home, By looking closely at how blockchain works, we see that it is like a digital safety net. In this secure, shared system, people can interact and exchange value without needing a go-between. It is tough against fraud, stays consistent without someone in charge, and can be shaped to fit many industries [17]. However, just like any tool, it is not perfect. Using blockchain can take much energy, and the rules around it—like government regulations—are still unclear. Connecting it with older systems that are not built for this kind of technology can also be tricky. Tripathi et al. points out that for blockchain to grow and succeed long-term, we need to fix these significant issues, especially by making it faster and easier to understand and regulate [18]. One can argue that developers are already working on scaling blockchain and improving decisions across networks[19]. One of its most significant promises is helping people who do not have easy access to banks or secure systems—especially in underserved parts of the world. If built and used wisely, blockchain could help bridge some gaps and make digital systems more fair and open for everyone [19].

X. Conclusion

Blockchain continues to redefine the digital landscape by offering a decentralized approach to data integrity and transaction verification [19]. Its significance in enabling trustless systems marks a paradigm shift in computing and finance. Continued research and development will be essential in addressing its limitations and realizing its full potential across sectors. Its use in establishing decentralized autonomous organizations (DAOs) indicates an evolving corporate structure where rules and decisions are encoded into smart contracts [20]. As integration into IoT, AI, and supply chains progresses, the synergy among these technologies will further amplify blockchain's influence across sectors in the future. All blockchain continues to redefine the digital landscape by offering a decentralized approach to data integrity and transaction verification [19]. Blockchain is important because it lets people do business or share information without needing to trust each other—or a middleman. That is a significant change from how things typically work in banking and technology. However, to make the most of it, developers still need to work out some problems, like making it faster and easier to use. Its use in establishing decentralized autonomous organizations (DAOs) indicates an evolving corporate structure where rules and decisions are encoded into smart contracts [20]. As integration into IoT, AI, and supply chains progresses globally, the communication between these technologies will further amplify blockchain's influence across such sectors in the coming decades. A more important question might be how far integration can go while still making sense to the average user.

Acknowledgments

Thank you to Professor Susan Zehra and Teaching Assistant Jain Li for a wonderful semester.

This template was adapted from those the IEEE provided on their website and downloaded from Scribbr.

References

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, pp. 6–19, 2016.

[2] 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. Congress on Big Data (BigData Congress), 2017, pp. 557–564.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[4] V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform,” 2014.

[5] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain technology overview,” NIST Interagency Report 8202, National Institute of Standards and Technology, Oct. 2018.

[6] B. Shrimali and H. B. Patel, "Blockchain state-of-the-art: architecture, use cases, consensus, challenges, and opportunities," Journal of King Saud University – Computer and Information Sciences, vol. 34, pp. 6793–6807, 2022.

[7] C. Decker and R. Wattenhofer, “Information propagation in the Bitcoin network,” in Proc. IEEE P2P 2013, 2013, pp. 1–10.

[8] D. Vujičić, D. Jagodic, and S. Ranđić, “Blockchain technology, Bitcoin, and Ethereum: A brief overview,” in Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH), 2018, pp. 1–6.

[9] K. Croman et al., “On scaling decentralized blockchains (a position paper),” in Proc. 3rd Workshop on Bitcoin and Blockchain Research (Financial Cryptography 2016 Workshops), 2016, pp. 106–125.

[10] A. Hafid, A. S. Hafid, and M. Samih, “Scaling blockchains: a comprehensive survey,” IEEE Access, vol. 8, pp. 125244–125262, 2020.

[11] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, vol. 107, pp. 841–853, 2020.

[12] Z. Hussein, M. A. Salama, and S. A. El-Rahman, “Evolution of blockchain consensus algorithms: a review on the latest milestones,” Cybersecurity, vol. 6, Art. 30, 2023.

[13] A. A. Aljabr, A. Sharma, and K. Kumar, “Mining process in cryptocurrency using blockchain technology: Bitcoin as a case study,” Journal of Computational and Theoretical Nanoscience, vol. 16, no. 10, pp. 4293–4298, 2019.

[14] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, “On the security and performance of proof-of-work blockchains,” in Proc. 2016 ACM SIGSAC Conf. on Computer and Communications Security (CCS), 2016, pp. 3–16.

[15] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: current status, classification and open issues,” Telematics and Informatics, vol. 36, pp. 55–81, 2019.

[16] K. Wüst and A. Gervais, “Do you need a blockchain?” in Proc. Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 45–54.

[17] J. Golosova and A. Romanovs, “The advantages and disadvantages of the blockchain technology,” in Proc. 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018, pp. 1–6.

[18] G. Tripathi, M. A. Ahad, and G. Casalino, “A comprehensive review of blockchain technology: underlying principles and historical background with future challenges,” Decision Analytics Journal, vol. 9, Art. 100344, 2023.

[19] M. Iansiti and K. R. Lakhani, “The truth about blockchain,” Harvard Business Review, vol. 95, no. 1, pp. 118–127, 2017.

[20] S. Underwood, “Blockchain beyond Bitcoin,” Communications of the ACM, vol. 59, no. 11, pp. 15–17, 2016