Dissertation

Eduardo Oliveira

March 15, 2025

1 Blockchain

1.1 Origins of Blockchain

Blockchain is a decentralized, immutable ledger technology designed to facilitate secure and transparent transactions within distributed networks. Initially conceptualized for the Bitcoin blockchain [4], this technology has since evolved into a multi-purpose infrastructure underpinning various domains, including finance, supply chain management, and digital identity verification.

The development of blockchain, however, did not occur in isolation. The concept of a cryptographically secured chain of blocks predates Bitcoin and draws from earlier research on distributed consensus and cryptographic techniques. A key component in blockchain structures is the Merkle tree, introduced by Ralph Merkle in the 1980s [3]. These trees enable efficient data integrity verification by organizing hashes in a hierarchical structure, which is crucial for maintaining the integrity of blockchain data.

Building on these foundational cryptographic concepts, Stuart Haber and W. Scott Stornetta proposed a method for securely time-stamping digital documents in 1991 [2]. This innovation was significant because it prevented backdating and tampering, laying the groundwork for immutable records. In 1992, Haber, Stornetta, and Bayer further refined this approach by incorporating Merkle trees into their time-stamping system, thereby improving efficiency and strengthening security [1]. These advancements not only contributed to the development of blockchain but also highlighted the potential of decentralized, immutable ledgers for maintaining verifiable records.

The inherent properties of blockchain—decentralization, immutability, transparency, and security—make it particularly well-suited for addressing challenges in scientific reproducibility. By maintaining an auditable and tamper-proof history of research data and workflows, blockchain ensures long-term verifiability and integrity. This application leverages the foundational principles established by early cryptographic and distributed systems research, demonstrating how blockchain can extend beyond financial transactions to support rigorous scientific reproducibility.

1.2 Consensus Mechanisms in Blockchain

Consensus mechanisms are fundamental to blockchain networks, ensuring agreement among distributed nodes without requiring centralized authority. These mechanisms validate transactions and maintain the integrity of the ledger, preventing issues such as double-spending and malicious attacks.

1.2.1 Proof of Work (PoW)

Proof of Work (PoW) was first implemented in Bitcoin [**?**] and remains one of the most well-known consensus mechanisms. PoW requires network participants, known as miners, to solve complex cryptographic puzzles using computational resources. The first miner to find a valid solution can append a new block to the blockchain and receive a block reward. This process ensures security but comes at the cost of significant energy consumption [**?**]. Additionally, the difficulty adjustment mechanism ensures that blocks are produced at a steady rate by modifying the complexity of the puzzle based on the total computational power of the network.

1.2.2 Proof of Stake (PoS)

Proof of Stake (PoS) was introduced as an energy-efficient alternative to PoW [**?**]. Instead of relying on computational work, PoS selects validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Validators are incentivized to act honestly since they risk losing their stake if they attempt to manipulate the system. Variants of PoS, such as Delegated Proof of Stake (DPoS) [**?**], introduce mechanisms where token holders vote for delegates to validate transactions on their behalf, improving efficiency while maintaining decentralization.

1.2.3 Mining and Block Validation

Mining is the process by which transactions are validated and added to a blockchain. In PoW-based systems, miners compete to solve cryptographic puzzles, while in PoS-based systems, validators are selected to propose and confirm blocks based on their stakes. The mining process serves two key purposes: securing the network by making attacks computationally expensive and issuing new tokens as rewards. The incentive structure aligns participant behavior with the network's security goals [**?**].

1.2.4 Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance (BFT) is a property of distributed systems that allows them to function correctly even if some nodes act maliciously or fail [**?**]. Traditional consensus mechanisms, such as Practical Byzantine Fault Tolerance (PBFT) [**?**], require all participants to communicate and reach consensus before a block is finalized. PBFT-based systems provide high efficiency

and finality but require a known set of validators, making them more suitable for permissioned blockchains. Many modern blockchain frameworks, including Hyperledger Iroha, incorporate BFT-based consensus mechanisms to enhance security and reliability.

1.3 Public and Private Blockchains

Blockchains can be classified based on their accessibility and governance models, primarily into public and private blockchains.

1.3.1 Public Blockchains

Public blockchains, such as Bitcoin and Ethereum, are open to anyone, allowing unrestricted participation in the network. These blockchains prioritize decentralization and security at the expense of scalability. Consensus mechanisms in public blockchains typically rely on PoW or PoS, where participants must follow established protocols to validate transactions [**?**]. Public blockchains offer transparency, as all transactions are recorded on a publicly accessible ledger, making them suitable for applications requiring trustless environments.

1.3.2 Private and Permissioned Blockchains

Private blockchains restrict participation to authorized entities, making them suitable for enterprise applications. Hyperledger Fabric and Hyperledger Iroha are examples of permissioned blockchain frameworks designed for regulated environments where identity verification and compliance are critical [**?**]. Private blockchains provide improved scalability and efficiency since they do not require energy-intensive consensus mechanisms like PoW. However, they trade off decentralization, as a governing authority typically oversees the network.

1.4 Hybrid Blockchain Models

Hybrid blockchain models combine aspects of both public and private blockchains. These architectures allow organizations to maintain a private ledger while interacting with public networks for verification and transparency purposes. Such approaches are particularly useful in industries where both privacy and auditability are required, such as supply chain management and financial services [**?**].

1.5 Conclusion

Consensus mechanisms, mining, and fault tolerance strategies are critical in ensuring blockchain security and functionality. The choice between PoW, PoS, and BFT-based approaches impacts the efficiency, decentralization, and security of blockchain networks. Furthermore, the distinction between public, private, and hybrid blockchains influences their applications, with public blockchains

prioritizing trustlessness and private blockchains emphasizing control and efficiency. Understanding these foundational aspects enables the development of blockchain-based solutions tailored to the needs of Open Science and research reproducibility.

Public Key Cryptography in Blockchain

Public key cryptography plays a fundamental role in securing blockchain networks by enabling secure transactions, identity verification, and data integrity without requiring a centralized authority. It forms the foundation for digital signatures, key management, and encryption mechanisms that ensure trust and security in decentralized environments.

Role of Public Key Cryptography in Blockchain

Blockchain networks rely on asymmetric cryptography, also known as public key cryptography, to authenticate and authorize transactions. Each participant in the network possesses a pair of cryptographic keys: a **public key**, which serves as an address that others can use to send transactions, and a **private key**, which is used to sign transactions and prove ownership. When a user initiates a transaction, they generate a **digital signature** using their private key, allowing other participants to verify the authenticity of the transaction without revealing the private key itself.

This mechanism ensures that only the rightful owner of an asset can authorize its transfer, preventing fraud and unauthorized access. Additionally, cryptographic hashing techniques complement public key cryptography by ensuring data integrity and linking transactions in an immutable ledger.

Commonly Used Cryptographic Ciphers and Standards

Several cryptographic ciphers and standards are widely used in blockchain implementations to provide strong security guarantees:

- **RSA (Rivest-Shamir-Adleman):** A traditional public key cryptosystem based on the difficulty of factoring large prime numbers. While RSA is widely used in general cryptographic applications, its key sizes are relatively large compared to modern alternatives, making it less practical for blockchain applications.
- **Elliptic Curve Cryptography (ECC):** A more efficient asymmetric cryptography scheme that provides the same level of security as RSA but with significantly smaller key sizes. This efficiency makes ECC the preferred choice for blockchain applications.
- **ECDSA (Elliptic Curve Digital Signature Algorithm):** A widely adopted digital signature scheme based on ECC, used in Bitcoin and Ethereum to secure transactions.

- **EdDSA (Edwards-curve Digital Signature Algorithm):** A modern alternative to ECDSA, known for its faster signature verification and improved security properties. It is used in newer blockchain protocols like Monero.
- **X25519:** A secure key exchange protocol based on Curve25519, commonly used in cryptographic operations for secure communication in blockchain applications.

Elliptic Curve Cryptography (ECC) in Blockchain

Elliptic Curve Cryptography (ECC) is a type of public key cryptography that leverages the mathematical properties of elliptic curves over finite fields to provide strong security with smaller key sizes. The security of ECC is based on the **Elliptic Curve Discrete Logarithm Problem (ECDLP)**, which is computationally hard to solve.

In blockchain systems, ECC is primarily used for:

1. **Digital Signatures:** ECC enables the creation of compact and secure digital signatures, such as those used in Bitcoin (ECDSA) and newer blockchain protocols (EdDSA).
2. **Key Pair Generation:** Blockchain wallets generate private-public key pairs using elliptic curves, ensuring that users can securely sign and verify transactions.
3. **Scalability and Efficiency:** Due to its small key size and lower computational requirements, ECC allows blockchain networks to process transactions more efficiently while maintaining security.

Bitcoin, for instance, uses the **secp256k1** elliptic curve for key generation and signing, which provides a 256-bit key length offering high security with lower processing overhead compared to traditional cryptographic methods.

Conclusion

Public key cryptography is a cornerstone of blockchain security, enabling authentication, digital signatures, and secure communication. The adoption of ECC and its derivatives, such as ECDSA and EdDSA, has significantly improved the efficiency and scalability of blockchain networks, making them resilient to attacks while minimizing computational and storage costs. Future blockchain advancements may incorporate more advanced cryptographic techniques, including post-quantum cryptography, to further enhance security in decentralized systems.

References

[1] Dave Bayer, Stuart Haber, and W. Scott Stornetta. Improving the Efficiency and Reliability of Digital Time-Stamping. In Renato Capocelli, Alfredo De Santis, and Ugo Vaccaro, editors, *Sequences II*, pages 329–334, New York, NY, 1993. Springer New York.

[2] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *J. Cryptology*, 3(2):99–111, January 1991.

[3] Ralph C. Merkle. A Digital Signature Based on a Conventional Encryption Function. In G. Goos, J. Hartmanis, D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and Carl Pomerance, editors, *Advances in Cryptology — CRYPTO '87*, volume 293, pages 369–378. Springer Berlin Heidelberg, Berlin, Heidelberg, 1988. Series Title: Lecture Notes in Computer Science.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.