The Web3 Revolution

Building the Future of Blockchain, DeFi, and the Metaverse

Hui Gong

Apress®

The Web3 Revolution

Building the Future of Blockchain, DeFi, and the Metaverse

Hui Gong

Apress®

The Web3 Revolution: Building the Future of Blockchain, DeFi, and the Metaverse

Hui Gong
Institute of Finance & Technology
University College London
London, UK

ISBN-13 (pbk): 979-8-8688-0490-8 ISBN-13 (electronic): 979-8-8688-0491-5
https://doi.org/10.1007/979-8-8688-0491-5

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Malini Rajendran
Development Editor: James Markham
Editorial Assistant: Gryffin Winkler

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, Suite 4600, New York, NY 10004-1562, USA. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub. For more detailed information, please visit https://www.apress.com/gp/services/source-code.

If disposing of this product, please recycle the paper

This book is dedicated to my son, Tianyi Gong.

Table of Contents

About the Author

Dr. Hui Gong is the Programme Director of the MSc in Banking and Digital Finance and a Lecturer in Decentralised Finance and Blockchain at UCL Institute of Finance & Technology, where he also leads the Blockchain and DeFi Lab. His academic journey, which includes a PhD from University College London, has been marked by an in-depth exploration of blockchain, cryptocurrencies, Web3, and the transformative power of these technologies. He has collaborated with leading financial institutions such as Credit Suisse, integrating artificial intelligence and blockchain into the core of quantitative finance and fintech innovations.

As the founder of the China-UK Blockchain Association and a former Special Advisor on Fintech and Blockchain for some All-Party Parliamentary Groups, he has actively contributed to both the Sino-British dialogue and policy discussions in these sectors. His extensive work with the UCL Centre for Blockchain Technology (CBT) and Westminster Business School has resulted in numerous publications on topics such as ICOs and Central Bank Digital Currencies (CBDCs). Dr. Gong continues to dedicate his experience and knowledge to advancing financial technology, teaching and sharing his expertise in blockchain, DeFi, Web3, and the metaverse at a crucial time of technological evolution.

Acknowledgments

In the journey of writing this book, my deepest gratitude goes first and foremost to those who have supported me and embraced blockchain technology amidst its many controversies. Having been in this industry for nearly a decade, my passion has thrived on the support of everyone who shares a 'consensus' on the transformative potential of this field.

A special thanks to Professor Harry Thapar, former Head of the School of Finance and Accounting, and Ann Thapar, former Course Leader of MSc Fintech with Business Analytics, at Westminster Business School. Their decision to hire me post my PhD in 2019 allowed me to pioneer courses on blockchain, including topics on tokenisation that were yet to gain full regulatory acceptance. My innovative curricula have been well received by students, enhancing my teaching journey. In 2023, Professor Francesca Medda welcomed me back to the UCL Institute of Finance & Technology, offering me the opportunity to continue educating on Decentralised Finance and Blockchain at UCL. Their forward thinking, coupled with the encouragement and enthusiasm of my students, has been pivotal in my path and instrumental in the creation of this book, which will serve as a resource in my future courses. Additionally, the 4btc Inscription community, which I formed while writing this book, and all its members have provided unwavering support, reinforcing my belief in blockchain's capacity to revolutionise and disrupt finance as a part of the Web3 revolution.

Lastly, I extend my deepest appreciation to my family for their selfless dedication and support. I hope this work not only guides beginners in blockchain and cryptocurrency but also sparks innovative thinking among them. This journey has been challenging, but it's the community of like-minded, consensus-driven individuals that has made it worthwhile. We believed, and therefore we have seen.

Introduction

In the ever-evolving landscape of digital innovation, *The Web3 Revolution* charts a comprehensive journey from the theoretical underpinnings of blockchain technology to its practical applications in today's digital world. This book is crafted not merely as a guide but as a bridge, connecting the intricate mechanisms of decentralisation, cryptography and smart contracts with their real-world implementations that promise to redefine the fabric of our digital society.

As we delve into the complex world of Web3, we explore how these technologies are not just technological advancements but transformative tools that facilitate a shift in power from centralised entities to individuals and communities. Each chapter systematically unfolds, starting from the fundamentals of blockchain technology as exemplified by Bitcoin and Ethereum, moving through the nuances of non-fungible tokens (NFTs), decentralised autonomous organisations (DAOs) and the burgeoning field of decentralised finance (DeFi).

This book aims to serve both novices and seasoned professionals in the tech industry by providing a clear, contextual understanding of how each piece of the Web3 puzzle fits together and why it matters. Through a blend of technical descriptions, industry case studies and real-world scenarios, *The Web3 Revolution* offers readers not just knowledge but a vision of the potential impacts and opportunities that lie ahead in this new digital frontier.

Embark on this journey to demystify the complexities of blockchain and discover the practicalities that make Web3 a revolutionary step towards a more transparent, secure and equitable digital future. Whether you're an entrepreneur, a developer, a builder or simply a tech enthusiast, this book is designed to equip you with a robust understanding of Web3 and Blockchain technology and inspire you to be a part of this transformative wave.

PART I

The Origins and Fundamentals of Blockchain

CHAPTER 1

Decrypting Blockchain Technology

This chapter delves into the foundational aspects of blockchain, exploring its origins, key mechanics and the transformative potential it holds for creating a transparent, efficient and secure digital world. As we unfold the layers of this technology, we invite readers to explore how blockchain is not just reshaping finance but also redefining the boundaries of technology and trust in the modern era.

1.1 What Is Blockchain?

The origin of blockchain technology is closely linked to Bitcoin, tracing back to 2008 when the concept of Bitcoin was first introduced. Bitcoin is not only a cryptocurrency but also runs on an innovative technology known as blockchain. This technology, evolving alongside Bitcoin, has now been widely applied in various fields.

The genesis of Bitcoin dates back to 31 October 2008, when a mysterious individual or team known as Satoshi Nakamoto released a groundbreaking document – the Bitcoin whitepaper.[1] In this whitepaper, Nakamoto proposed a novel concept of digital currency, challenging

H. Gong, *The Web3 Revolution*, https://doi.org/10.1007/979-8-8688-0491-5_1

the existing financial system and revolutionising traditional monetary concepts. Then, on 3 January 2009, the Bitcoin network witnessed a historic moment as the first block, known as block #0, was successfully mined.[2] This block, commonly referred to as the genesis block or the original block, not only marked the official start of the Bitcoin network but also the first practical application of blockchain technology. This innovative application heralded a new era of digital currency and distributed ledger technology, laying the foundation for modern cryptocurrencies and blockchain technology.

As an innovative digital ledger technology, the core of blockchain lies in its ability to store and transfer data in a decentralised, transparent and immutable manner. In a blockchain, data is grouped and stored in structures called 'blocks', which are linked in chronological order, forming a continuously growing chain. Each block contains a series of transaction records and the cryptographic hash of the previous block, ensuring that once data is written to the blockchain, it is nearly impossible to alter or delete, thus preserving the integrity and complete history of data.

Decentralisation is another key characteristic of blockchain. Unlike traditional databases or ledger systems where data is stored in centralised servers or data centres, blockchain data is distributed across the entire network, with each node in the network maintaining a copy of the entire blockchain, shown in Figure 1-1. This distributed data storage significantly reduces the risk of single points of failure and enhances the system's resilience against attacks.

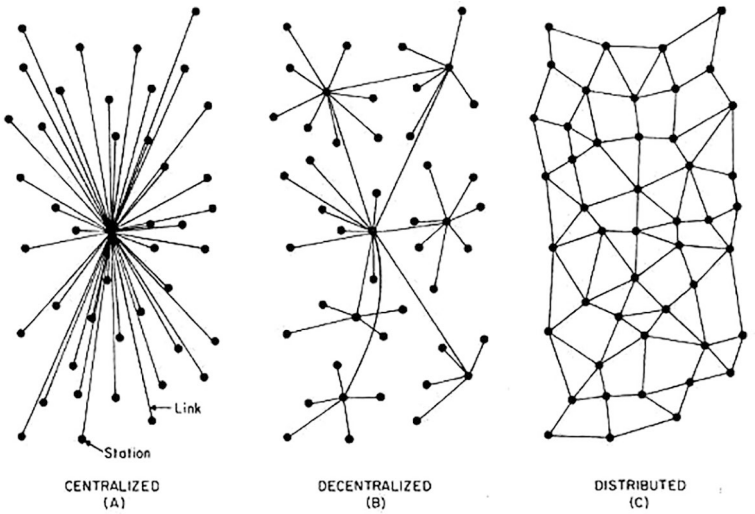

Figure 1-1. *Centralised vs. Decentralised vs. Distributed*
Source: https://berty.tech/blog/decentralized-distributed-centralized

This table provides an overview of the key characteristics and trade-offs associated with each type of system in terms of maintenance, stability, scalability, development and potential for evolution and diversity.

Table 1-1. *Comparison of Centralised vs. Decentralised vs. Distributed*

System Type	Centralised	Decentralised	Distributed
Points of Failure/ Maintenance	Single point of failure, easier to maintain	More points of failure than centralised but finite, harder to maintain	No single point of failure, hardest to maintain
Fault Tolerance/ Stability	Highly unstable if the central point fails	More stable than centralised, can survive central node failures	Very stable, single failures have little impact
Scalability/Max Population	Low scalability	Moderate scalability	Infinite scalability
Ease of Development/ Creation	Fastest to create, follows a single framework	Slower than centralised, need to sort out lower-level details	Slowest, complex resource sharing and communication required
Evolution/ Diversity	Low diversity, evolves slowly	Once infrastructure is in place, can evolve quickly	High potential for evolution once infrastructure is set

Furthermore, the transparency of blockchain technology is one of its defining features. In public blockchains, anyone can view all transaction records and block information, yet the identities of transaction participants remain anonymous or pseudonymous, as illustrated in Figure 1-2. This combination of transparency and privacy makes blockchain an ideal technology choice for sectors such as finance, supply chain management and healthcare.

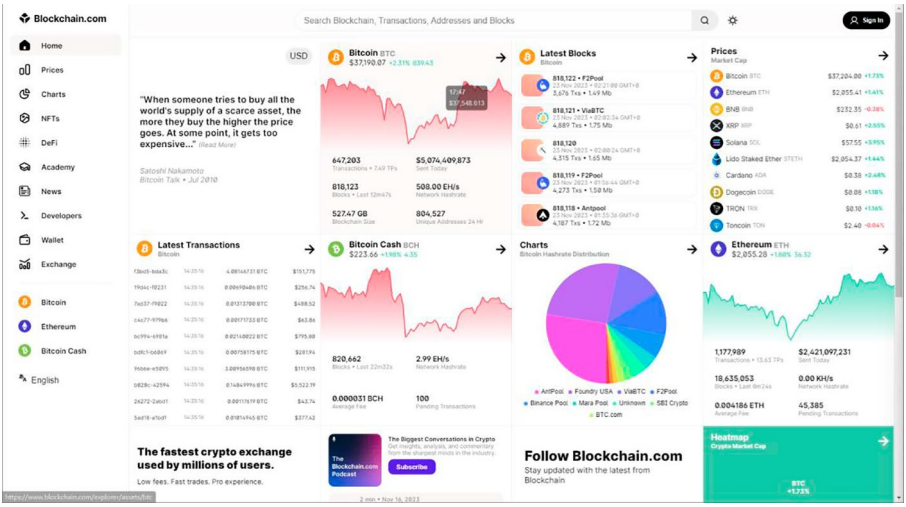

Figure 1-2. *Bitcoin Explorer*
Source: www.blockchain.com/explorer (Accessed: 23 November 2023)

To ensure the accuracy of transactions and the security of the network, blockchain networks typically employ a method known as the 'consensus mechanism' to verify and add new transactions. The most famous consensus mechanism is the proof of work (PoW) used by Bitcoin, where participants (miners) in the network must solve complex computational problems to validate transactions and create new blocks.

Hence, blockchain technology is not only designed to validate transactions and enhance the security of the digital ledger but also to mitigate critical issues such as the double-spending of cryptocurrencies and various fraudulent activities. Blockchain 1.0,[3] the initial iteration of this technology predominantly used in cryptocurrencies like Bitcoin, targets two fundamental problems:

- **Double-Spending Problem**: It uses a combination of peer-to-peer file sharing and public key encryption technologies to prevent the same digital currency unit from being used more than once. This is executed

within a trustless framework where transactions are recorded on a publicly accessible ledger and confirmed by a consensus among participants, thus eliminating the need for a centralised authority.

- **Byzantine Generals' Problem**: This refers to the challenge of achieving consensus in a decentralised network. Blockchain 1.0 addresses this through the proof-of-work (PoW) mechanism, where all participants agree on a verified truth without the need for a trusted intermediary. This is accomplished by miners solving cryptographic puzzles to validate transactions and add new blocks, thereby ensuring network agreement on the ledger's state.[4]

These foundational aspects underpin the robustness of blockchain against potential vulnerabilities and form the basis for its widespread application in various sectors beyond cryptocurrency.

Blockchain 2.0 represents a significant evolution from the original blockchain concept, marked by the integration of smart contracts into blockchain protocols. Pioneered by Ethereum, smart contracts are automated codes that execute when predefined conditions are met, enabling complex transactions beyond simple cryptocurrency exchanges. This advancement fostered the development of decentralised applications (DApps) and decentralised autonomous organisations (DAOs), expanding blockchain's utility into various domains such as governance and digital ownership, exemplified by non-fungible tokens (NFTs).

Blockchain 3.0 extends blockchain's application beyond financial sectors to diverse industries, emphasising sustainability, scalability and enhanced security. It integrates enterprise-level systems with blockchain, enabling industries like healthcare and supply chain management to utilise smart contracts for functions like medical services and logistics. Additionally, Blockchain 3.0 supports interoperability between different

blockchain networks, as seen in Cosmos and Chainlink ecosystems. Technological innovations like proof-of-stake consensus models and Directed Acyclic Graph (DAG) algorithms in this generation of blockchains, exemplified by platforms like Cardano, Solana and Avalanche, address previous limitations by reducing energy consumption and significantly increasing transaction processing speeds.[5]

In summary, blockchain technology offers a novel, more secure and reliable method for digital transactions and data storage through its unique decentralised structure, immutable data recording, transparency and robust consensus mechanism.

Blockchain vs. Internet

The Internet revolutionised the way information is disseminated, enabling rapid, cost-efficient and seamless exchange of knowledge across the globe. However, it falls short in transmitting value due to inherent trust issues and centralisation, often requiring intermediaries for validation.

In contrast, blockchain technology is engineered to transfer value. It does so by providing a decentralised platform where transactions are not only transparent but also immutable, creating an environment where trust is established through cryptographic verification rather than central authorities. Blockchain's capability to transmit value is exemplified by its ability to facilitate the exchange of digital assets, execute smart contracts and ensure the authenticity and integrity of transactions without centralised oversight. This makes blockchain an ideal infrastructure for the digital economy, where value transfer is as critical as information exchange.

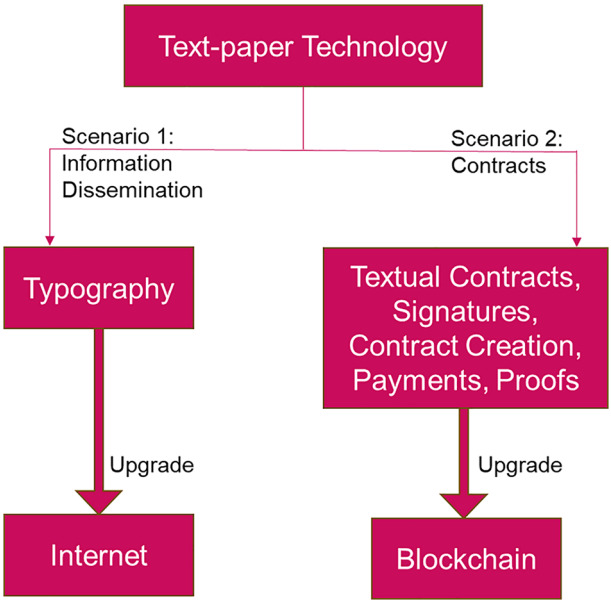

Figure 1-3. *Information vs. Value Transfer*

Figure 1-3 outlines the evolution of technology from text-paper to digital formats. At the top, 'Text-paper technology' serves as the starting point. From there, two paths diverge: one leads to 'Typography', eventually evolving into the 'Internet', symbolising the digital upgrade of text for information dissemination. The other path heads towards 'Textual Contracts, Signatures, Contract Creation, Payments, Proofs', which then lead to 'Blockchain', representing the digitisation of contractual and transactional processes. The diagram suggests that while the Internet evolved as the digital successor of typography for text, blockchain serves a similar role for transactions and contractual agreements.

Blockchain and AI

Blockchain and artificial intelligence (AI) are forging a strategic alliance that not only amplifies their individual strengths but also addresses fundamental societal and economic challenges. Blockchain's architecture,

celebrated for its security and immutability, establishes a bedrock for AI to function in a manner that is both transparent and verifiable, paving the path for 'decentralised AI' systems like SingularityNET. AI, in reciprocation, elevates blockchain's operational efficiency through intelligent optimisation of complex computations. This symbiosis further empowers individuals to take control of their data, facilitating personal data monetisation while disrupting the data monopoly held by tech behemoths. As AI algorithms evolve in complexity, the trust and clarity provided by blockchain become crucial in validating and understanding AI-driven decisions. Although still nascent and ripe with undiscovered possibilities, the convergence of blockchain and strong AI is a testament to their potential in revolutionising both the mechanics of productivity and the infrastructure of production relations, ensuring that AI's expansive capabilities are harnessed within a framework that upholds transparency, accountability and ethical standards.[6]

Figure 1-4. *Image Generated by the ChatGPT DALL·E 3 Model Based on the Preceding Text*
Source: https://chat.openai.com/?model=gpt-4

1.2 How Blockchain Works: Hash Functions, Encryption and Digital Signatures

The working mechanism of blockchain technology relies on two core components: hash functions and encryption technologies.

Hash Functions

Hash functions play a central role in blockchain, particularly in the cryptocurrency domain, where cryptographic hash functions possess key characteristics essential for ensuring security and integrity. The following three properties—collision resistance, hiding, and puzzle friendliness—are specifically critical for cryptographic hash functions used in cryptocurrencies.

- **Collision Resistance**: In cryptography, collision resistance is a key attribute of hash functions, requiring that for a given hash function H, it should be computationally infeasible to find two different inputs x and y such that H(x) = H(y). This means, despite the theoretical existence of such input pairs, finding them in reality is extremely difficult due to computational resource limitations. Collision resistance ensures the uniqueness of transactions in cryptocurrency, guaranteeing each transaction generates a unique hash value. Without collision resistance, attackers could create two different transactions with the same hash value, enabling undetected ledger tampering. In blockchain, as each block's hash value is included in the next block, collision resistance is vital for maintaining the integrity of the chain.

- **Hiding**: The hiding feature of hash functions is important for protecting data privacy in cryptography. A hash function with hiding properties means that even if the hash value is known, it is not possible to determine which specific input value produced it. This feature is typically achieved by combining randomness (like random numbers or salt) with the input data, ensuring even slight input variations result in significantly different outputs, making it impossible to deduce or guess the original data without additional information. In blockchain technology, hiding is extremely important as it ensures the privacy of transaction details while allowing network nodes to verify the validity of transactions without revealing actual data. For instance, Bitcoin's hash function uses hiding to prevent unauthorised access to information about transaction amounts and participant identities. This can be likened to the practice of sealing letters with wax in ancient times or using envelopes to conceal the contents of a letter. Just as a sealed letter ensures that only the intended recipient can access the message, the hiding property in hash functions ensures that sensitive transaction details remain private, while still allowing the network to verify the authenticity of the transaction. Additionally, hiding plays a role in creating cryptocurrency addresses and processing smart contracts, further enhancing the security and privacy protection capabilities of the blockchain network.
- **Puzzle Friendliness**: Puzzle friendliness is a unique property of hash functions in the cryptocurrency domain. It implies that for a given output value,

finding an input value that maps to this output is very difficult. In other words, there is no effective way to predict which input value will produce a specific hash value, unless all possible inputs are tried. In the mining process of cryptocurrencies like Bitcoin, puzzle friendliness is crucial. Miners must try a vast number of different inputs (including transaction information and a random number) to find a hash value that meets the current difficulty target of the network, typically meaning the hash value must be less than a certain number. This process is computationally intensive, and randomness ensures no shortcuts to complete the task, thus guaranteeing network security and the stable issuance of currency.

These features collectively form the cornerstone of hash functions in cryptocurrency, ensuring the security and functionality of the blockchain network.

Encryption

Asymmetric Encryption: Asymmetric encryption is a key technology in blockchain to ensure the security of transactions. In this system, the public key encrypts information into ciphertext for public transmission, while the private key decrypts the ciphertext back into plaintext, accessible only to the holder of the private key, thus ensuring the confidentiality of the information. In blockchain transactions, participants use their private key to digitally sign transactions. The corresponding public key can be used by others to verify the legitimacy of the signature, but not to forge it, thereby ensuring the authenticity and non-repudiation of the transaction.

Merkle Trees: Merkle trees are structures optimised for validating data. They aggregate transaction data through hash functions, where each leaf node contains the hash value of an individual transaction, and

internal nodes contain the hash values of their child nodes. This structure is highly efficient in ensuring data integrity and speeding up information verification, thus working in conjunction with asymmetric encryption to ensure the completeness and validity of data.

Hash Pointers and Data Structures: The hash pointer structure records the hash value of data and pointers to other parts of the data structure. Blockchain uses hash pointers to link each block into a chain, where each block contains the hash value of the previous block, establishing the immutability and historical continuity of the blockchain. This sequential linking maintains a timestamped, orderly record of transactions, providing strong support for the authenticity of data. By linking each block to the hash value of its predecessor, it not only confirms the data's immutability but also establishes a verifiable, sequentially arranged chain of transaction records.

Combining these three elements, blockchain provides a transparent, secure and unalterable environment for transactions, laying the foundation for building trust and value transfer.

Table 1-2 is a comparison table of the cryptographic functions used by Bitcoin (BTC) and Ethereum (ETH).

Table 1-2. *Cryptographic Function for BTC and ETH*

Feature	Bitcoin (BTC)	Ethereum (ETH)
Hash Function	SHA-256	Keccak-256 (variant of SHA-3)
Signature Algorithm	ECDSA (Elliptic Curve Digital Signature Algorithm)	ECDSA (Elliptic Curve Digital Signature Algorithm)

This table illustrates the differences and similarities in the cryptographic functions employed by both Bitcoin and Ethereum. While both use the ECDSA algorithm for digital signatures, they differ in their choice of hash functions, with Bitcoin using SHA-256 and Ethereum using Keccak-256.

Digital Signatures

Digital signatures play a crucial role in blockchain, ensuring the security and authentication of transactions. The digital signature mechanism includes generating a key pair (public and private keys), the signing process and the verification process. The private key is used to sign messages, while the public key allows anyone to verify the authenticity of the signature. Digital signatures not only ensure that only the signer can generate the signature but also bind the signature to a specific document, ensuring that the signature cannot be used to indicate approval or endorsement of a different document. The design goal of this mechanism is to meet two main properties, very similar to the analogy of handwritten signatures:

1. **Uniqueness**: Only you can generate your signature, but anyone who sees it can verify its validity. This is achieved by using the private key to sign messages, and the private key is confidential and accessible only to the owner of the key.
2. **Binding**: The signature is bound to a specific document, so it cannot be used to indicate agreement or endorsement of a different document. In other words, the signature is a verification of a specific transaction or message and cannot be misused or repurposed for other content.

The digital signature scheme includes the following three algorithms:

- **Key Generation**: This method takes a key size parameter and generates a pair of keys. The private key (secret key) is kept confidential and used to sign messages; the public key (public verification key) is public, and anyone can use it to verify the signature.