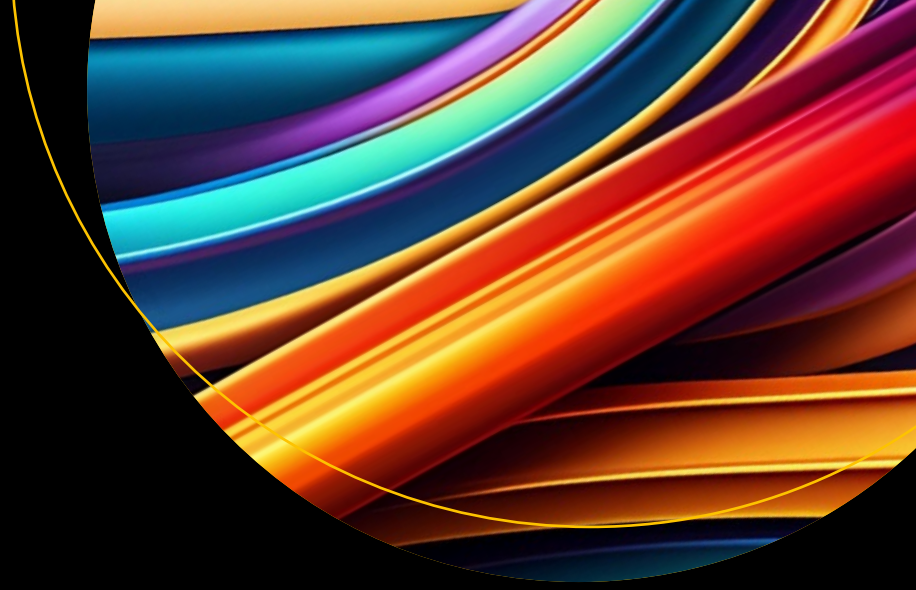

Blockchain Essentials

Core Concepts and Implementations

Ramchandra Sharad Mangrulkar
Pallavi Vijay Chavan

Apress®

Blockchain Essentials

Ramchandra Sharad Mangrulkar • Pallavi Vijay Chavan

Blockchain Essentials

Core Concepts and Implementations

Apress®

Ramchandra Sharad Mangrulkar
Mumbai, Maharashtra, India

Pallavi Vijay Chavan
Mumbai, Maharashtra, India

ISBN-13 (pbk): 978-1-4842-9974-6 ISBN-13 (electronic): 978-1-4842-9975-3
https://doi.org/10.1007/978-1-4842-9975-3

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Smriti Srivastava
Development Editor: Laura Berendson
Coordinating Editor: Shaul Elson

Cover designed by eStudioCalamar

Cover image by Sketchepedia@freepik.com

Distributed to the book trade worldwide by Apress Media, LLC, 1 New York Plaza, New York, NY 10004, U.S.A. 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 (https://github.com/Apress). For more detailed information, please visit https://www.apress.com/gp/services/source-code.

Paper in this product is recyclable

To our cherished daughter, Mansi:
Your unwavering support, encouragement, and constant sympathy were invaluable during the creation of this book. Without you, it would have been completed in half the time.

Contents

About the Authors

Dr. Ramchandra Mangrulkar is a Professor in the Department of Information Technology in the Dwarkadas J. Sanghvi College of Engineering in Mumbai, India. He holds various memberships in professional organizations such as IEEE, ISTE, ACM, and IACSIT. He completed his Doctor of Philosophy (Ph.D.) in Computer Science and Engineering from S.G.B. Amravati University in Maharashtra and Master of Technology (MTech) in Computer Science and Engineering from the National Institute of Technology, Rourkela. Dr. Mangrulkar is proficient in several technologies and tools, including Microsoft's Power BI, Power Automate, Power Query, and Power Virtual Agents, Google's Dialog Flow, and Overleaf. With over 22 years of combined teaching and administrative experience, Dr. Mangrulkar has established himself as a knowledgeable and skilled professional in his field. He has also obtained certifications like Certified Network Security Specialist International CyberSecurity Institute (ICSI) – Certified Network Security Specialist (CNSS) from ICSI, UK. Dr. Mangrulkar has an extensive publication record, with 95 publications including refereed/peer-reviewed international journal publications, book chapters with international publishers (including ones indexed in Scopus), and international conference publications.

Dr. Pallavi Vijay Chavan is Associate Professor at Ramrao Adik Institute of Technology, D. Y. Patil "Deemed-to-be-University," Navi Mumbai, MH, India. She has been in academia for the past 17 years working in the area of computing theory, data science, and network security. In her academic journey, she has published research in data science and security with reputable publishers such as Springer, Elsevier, CRC Press, and Inderscience. She has published 2 books, over 7 book chapters, more than 10 international journal papers, and over 30 international conference papers. Presently she serves as advisor to five Ph.D. research scholars in related fields. She completed her Ph.D. at Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, MH, India, in 2017. In 2003,

she earned the first merit position at Nagpur University for a B.E. in Computer Engineering. She is the recipient of research grants from University Grants Commission (UGC), Council of Scientific & Industrial Research (CSIR), and University of Mumbai. She serves as a reviewer for Elsevier and Inderscience journals. Her motto is "Teaching is a mission."

About the Technical Reviewer

Dr. Parikshit Mahalle is a senior member of the Institute of Electrical and Electronics Engineers and Professor, Dean of Research and Development and -Chair of the Department of Artificial Intelligence and Data Science at Vishwakarma Institute of Information Technology, Pune, India. He completed his Ph.D. at Aalborg University, Denmark, and continued as a postdoctoral researcher at Communication, Media & Information Technologies, Copenhagen, Denmark. He has over 23 years of teaching and research experience. He is a former member of the Board of Studies in Computer Engineering and former chairman of the Department of Information Technology at Savitribai Phule Pune University and various universities and autonomous colleges throughout India. He owns 15 patents, has published over 200 research studies and papers (2950+ Google Scholar, 1550+ H index-25 and Scopus citations, 438 H index-8, Web of Science, and H index-10 citations), and has authored/edited 56 books with Springer, CRC Press, Cambridge University Press, and others. He is editor in chief for IGI Global's *International Journal of Rough Sets and Data Analysis* and Inderscience's *International Journal of Grid and Utility Computing*, is a member of the editorial review board for IGI Global's *International Journal of Ambient Computing and Intelligence*, and serves as a reviewer for various reputable journals and conferences. His research interests include machine learning, data science, algorithms, Internet of Things, identity management, and security. He currently advises eight Ph.D. students in the areas of IoT and machine learning, and six students have successfully defended their Ph.D. under his supervision from Savitribai Phule Pune University. He is also the recipient of the Best Faculty Award by Sinhgad Institutes and Cognizant Technology Solutions. He has delivered over 200 lectures at the national and international levels.

Preface

Blockchain has become the buzzword of the day. Developers are focusing on more user-friendly applications with the help of blockchain, achieving decentralization and a trustless environment without third-party involvement. This includes diverse concepts and tools that play major roles in developing crypto-based applications in various programming languages. The distributed ledger and smart contracts involved reveal the importance of blockchain in creating immutable and transparent, cryptographically secure record-keeping of transactions. The programming approach helps to shed light on the core concepts of blockchain and relevant applications in easy steps. This helps to motivate learners to become part of the solution to most of the applications demanding trustless and independent autonomous systems. The identification and examination of blockchain technology beyond cryptocurrency will help to investigate alternative solutions using many blockchain-supportive tools.

The main purpose of this book is to present the difficult concepts of blockchain technology in very accessible and easy-to-understand language using a programming approach so that learners can easily grasp the key concepts arising from the emerging notion of blockchain technology. Another purpose of this book is to make available the experience of academia and industry to the target audience through hands-on programming.

This book presents the concepts of blockchain technology in a concise manner with clear and easy examples using trending blockchain programming languages. The book fills a gap of address issues surrounding the practical implementation of blockchain concepts using case studies. The book also highlights the usefulness of blockchain technology beyond its current applications.

Mumbai, India
September 2023

Ramchandra Sharad Mangrulkar
Pallavi Vijay Chavan

Acknowledgements

We extend our sincere gratitude to the dedicated contributors and accomplished researchers in the field of blockchain for their invaluable contributions and pioneering work.

Introduction to Blockchain

1

Readers of this book are likely to have some knowledge and basic idea about the enormous potential of the trending, decentralizing, and trustworthy technology called blockchain. This technology represents an innovation in the digital ecosystem that has significantly impacted trusted computing activities, resulting in an enhanced level of protection from cyber security threats.

This chapter lays out the fundamentals of blockchain technology, presenting its theoretical background, historical milestones, and present growth trends. Further, the conceptual view of a block in blockchain and the types of blockchain are described. The chapter discusses the basic skill set and libraries required to start doing "blockchain programming," which is a key objective of this book. The chapter ends with a few examples and their implementation in Python.

1.1 Prerequisites

The prerequisites for blockchain technology include:

- Understanding of cryptography: Cryptography is the foundation of blockchain technology. A basic understanding of cryptographic concepts, such as hashing, public-key encryption, and digital signatures, is necessary.
- Distributed systems: Blockchain is a distributed system that runs on multiple nodes. Therefore, it is essential to have a good understanding of distributed systems to build and deploy blockchain applications.
- Data structures and algorithms: Blockchain technology relies on complex data structures such as Merkle trees and algorithms such as consensus algorithms. Understanding of these concepts is crucial for building a robust blockchain system.
- Networking and security: Blockchain technology requires a good understanding of networking protocols, such as TCP/IP, HTTP, and HTTPS. Additionally, a solid understanding of security concepts, such as firewalls, encryption, and authentication, is necessary to develop secure blockchain applications.
- Smart contracts: Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller directly written into lines of code. Knowledge of smart contract programming languages, such as Solidity, is necessary for building decentralized applications.

R. S. Mangrulkar, P. Vijay Chavan, *Blockchain Essentials*,
https://doi.org/10.1007/978-1-4842-9975-3_1

- Business and economics: Blockchain technology is disrupting traditional business models and creating new opportunities. Understanding the economics of blockchain and how it can be applied to business is essential for leveraging its potential.
- Legal and regulatory dimensions: Blockchain technology operates in a regulatory gray area in many countries, and regulations are constantly evolving. Understanding the legal and regulatory environment in which blockchain operates is critical for creating compliant and successful blockchain applications.

1.2 Blockchain Myths

Blockchain is an emerging technology. The following list dispels some of the myths surrounding blockchain:

- Blockchain is the same thing as Bitcoin (or any other cryptocurrency)
  There is a misleading idea that if you learn blockchain technology, you will become a good trader! This is untrue. Blockchain is not equivalent to any cryptocurrency, whether Bitcoin or any other currencies on the market like Altcoins. In fact, blockchain is a technology, whereas Bitcoin is a cryptocurrency that makes use of blockchain technology. Blockchain has many applications outside the crypto world. Blockchain technology provides a full support system for developing cryptocurrencies, whereas Bitcoin is a fundamental application that builds on this emerging blockchain technology.
- Blockchain can solve all security issues
  Blockchain cannot be used to definitively eliminate corruption or fraudulent activities. Blockchain's many applications have been developed by players in the various models governing economies around the world. Blockchain cannot all issues related to security. Solving all societal issues using blockchain is a formidable challenge. Thus, careful consideration needs to be given as to which societal issues should be addressed using blockchain.
- Blockchain is the only possible technology
  Blockchain is not necessarily the best technology for solving your problems; they might be better solved employing technology that does not use blockchain. It is possible that many different existing technologies would yield better results in terms of security without the use of blockchain.
- Blockchain and distributed databases are similar technologies
  Blockchain and distributed databases are different technologies. Blockchain is not a distributed databases. Blockchain is not designed to store and secure data. Blockchain and distributed databases are two different technologies, each with its own merits and demerits and different potential to solve different problems. Both are essential, and one cannot easily replace the other.

1.3 Blockchain and Decentralization

Blockchain technology emerged to solve most of the issues in decentralization. Decentralization refers to the distribution of power or authority away from a single central entity to multiple individuals or groups. In the context of technology, it refers to systems or networks that operate without a central authority controlling them. Figure 1-1 gives an overview of centralized and decentralized systems.

Decentralization is required to address trust issues, that is, the different parties involved do not trust each other, but they should cooperate. The network of different entities such as businesses, individuals, government, private- and public-sector organizations, with their own interests, can come

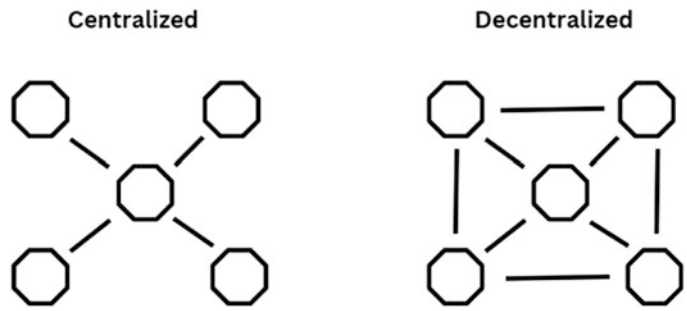

Figure 1-1 Overview: centralized and decentralized systems

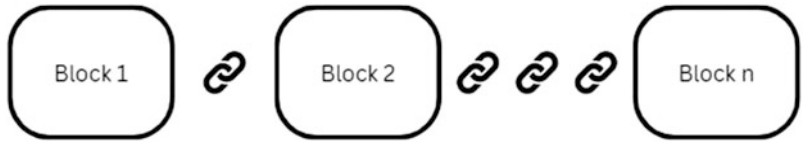

Figure 1-2 Blocks and chain in blockchain

together and cooperate with each other to solve societal issues. Decentralization and blockchain work together to create a secure, transparent, and tamper-proof system that operates without the need for a central authority.

1.4 What Is Blockchain?

Blockchain is an append-only, immutable, never-ending chain of data where data, once added, cannot be deleted or modified, achieving a tamper-proof system. The immutable property of blockchain means no one can change it. Its append-only nature ensures that no one can erase data once they are written in the blockchain. This append-only nature of blockchain makes it a never-ending but fully traceable system. Figure 1-2 shows the basic idea of blocks and chain in blockchain.

Every individual player maintains a copy of the blockchain, removing the need for central administration or centralization. The addition of information to the existing blockchain happens in the form of a new block appended at the end while at the same time ensuring that all copies of the local blockchain available to the different network players must also be updated in the same order. This will ensure data consistency in the blockchain, and all copies will be the same. This doubtlessly will require an additional authentication and validation mechanism, but at a superficial level, everyone will have an updated copy of the blockchain.

The data structure in blockchain consists of a chain of blocks linked together with the help of current and previous pointers. These two fields store the hashed data of the contents of the block, the previous pointer stores the hashed data of the previous block, and the current pointer stores the hashed data of the current block.

The data are stored in the blockchain in a transparent way and are available to everyone, allowing anyone to validate and verify the data as and when required.

Definition 1.1 Blockchain is a decentralized, immutable, append-only public ledger.

1.5 Disruptive Technology

Clayton Christensen introduced the idea of disruptive technologies in a 1995 *Harvard Business Review* article. Disruptive technology refers to any innovation that disrupts an existing market or industry, displacing established products or services and creating new markets and opportunities. These technologies often have a transformative effect on society, leading to changes in business models, consumer behavior, and even cultural norms.

Not all innovations are disruptive technologies. It is the process rather than product or services. Blockchain is a sustaining innovation rather than a disruptive innovation in the financial sector.

Disruptive technologies typically emerge from unexpected sources and are often initially dismissed as inferior or irrelevant by established players in the market. However, as they gain momentum and become more widely adopted, they can completely change the competitive landscape and reshape entire industries.

The following are examples of disruptive technologies:

- Ecommerce: The rise of ecommerce in the 2000s disrupted traditional brick-and-mortar retail, creating new opportunities for businesses to sell products and services online.
- Personal computers: The development of personal computers in the 1970s and 1980s disrupted the established mainframe computer industry, creating new markets and opportunities for businesses and individuals.
- Social media: The emergence of social media in the 2010s disrupted traditional media and advertising industries, leading to the rise of new platforms for content creation and distribution.
- Digital photography: The advent of digital photography in the 1990s disrupted the traditional film photography industry, leading to the demise of many established companies and the emergence of new players in the market.

Blockchain is considered a disruptive technology for several reasons:

- Decentralization: One of the key features of blockchain technology is its ability to operate in a decentralized manner, without the need for intermediaries such as banks or government institutions. This eliminates the need for trust in centralized institutions, which can be slow, expensive, and prone to corruption.
- Immutable and transparent: Blockchain technology is immutable and transparent, meaning that once data are added to a blockchain, it cannot be modified or deleted. This creates a high degree of trust in the data stored on the blockchain and eliminates the need for intermediaries to verify data.
- Security: Blockchain technology is secured by cryptographic algorithms that make it virtually impossible to tamper with the data stored on the blockchain. This creates a high degree of security for transactions and other data stored on the blockchain.
- Smart contracts: Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This eliminates the need for intermediaries to execute and enforce contracts, which can be slow, expensive, and prone to errors.
- Tokenization: Blockchain technology enables the creation and exchange of digital assets, or tokens, which can represent anything of value, such as currency, property, or ownership rights. This creates new opportunities for businesses to generate value and disrupt traditional business models.

1.6 History

Blockchain, a technology with the potential to become the foundation of global record-keeping systems, was introduced a mere decade ago by anonymous individuals associated with the digital currency Bitcoin, under the pseudonym Satoshi Nakamoto. Despite its relatively recent inception, blockchain has quickly gained recognition as a transformative innovation, poised to revolutionize various industries through its decentralized and secure nature.

1.6.1 Milestones in Blockchain Development

The subsection discusses some of the significant milestones in the development of blockchain technology (Figure 1-3).

1. 2008 – The publication of Bitcoin's whitepaper by Satoshi Nakamoto marked the groundbreaking introduction of the cryptocurrency. This event revolutionized the financial landscape, ushering in a new era of decentralized digital currency. The whitepaper laid the foundation for a peer-to-peer electronic cash system that would eventually disrupt traditional monetary systems worldwide.
2. 2009 – The inaugural Bitcoin transaction between Satoshi Nakamoto and Hal Finney stands as a significant milestone in cryptocurrency history. This historic event symbolized the practical application and transferability of Bitcoin as a digital currency. The transaction showcased the

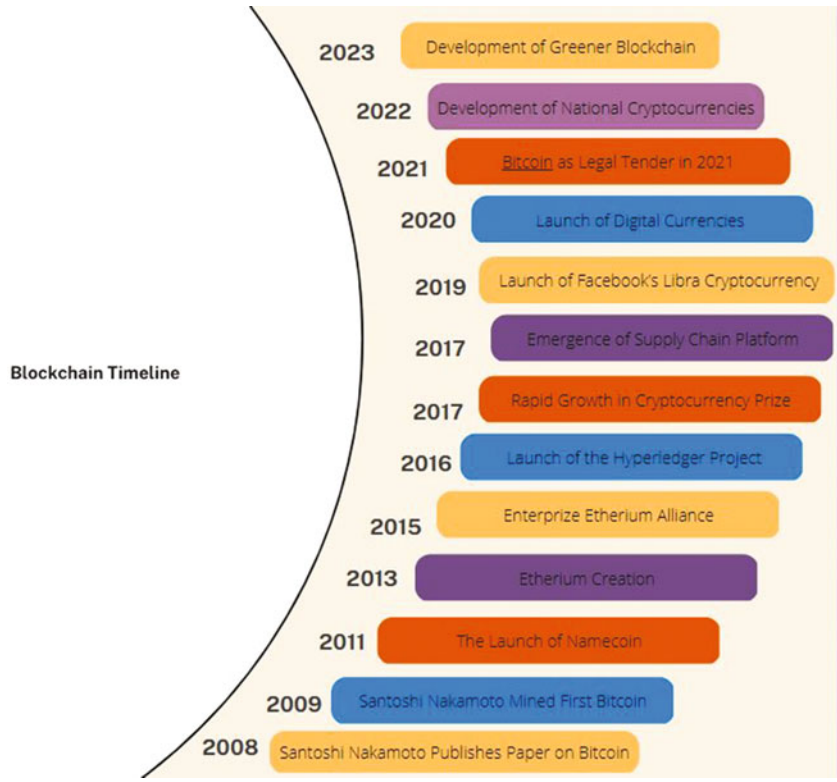

Figure 1-3 Blockchain timeline

potential of Bitcoin as a decentralized payment system, setting the stage for its widespread adoption and subsequent impact on the financial industry.

3. 2011 – Namecoin's launch marked a groundbreaking moment as it became the first alternative cryptocurrency to utilize blockchain technology. This pioneering step opened the door for a multitude of innovative blockchain-based digital assets. Namecoin's introduction demonstrated the potential for decentralized systems beyond traditional currencies, paving the way for the development of various blockchain applications and cryptocurrencies.
4. 2013 – Vitalik Buterin's creation of Ethereum unleashed a revolutionary platform enabling the creation of smart contracts and decentralized applications (dApps). Ethereum's emergence introduced a new paradigm in blockchain technology, empowering developers to build complex applications on a decentralized network. Buterin's vision laid the foundation for a vibrant ecosystem of dApps, fueling innovation and transforming industries through the power of decentralized computing.
5. 2015 – The formation of the Enterprise Ethereum Alliance united leading corporations and blockchain startups, fostering collaboration in the advancement of blockchain technology. This alliance served as a catalyst for exploring the potential of Ethereum in various industries and promoting blockchain adoption on a global scale. The Enterprise Ethereum Alliance aimed to accelerate innovation, establish industry standards, and drive the mainstream integration of blockchain solutions across sectors.
6. 2016 – The Hyperledger Project, initiated by the Linux Foundation, set out to develop open-source blockchain software specifically tailored to enterprise applications. This strategic launch brought together industry leaders and technologists to collaborate on building scalable and interoperable blockchain solutions. By providing a collaborative platform, the Hyperledger Project aimed to accelerate the adoption of blockchain technology among businesses, fostering transparency, efficiency, and trust in enterprise operations.
7. 2017 – The cryptocurrency market witnessed an unprecedented surge in value, primarily led by Bitcoin, accompanied by an explosive growth in initial coin offerings (ICOs). This phenomenon resulted in widespread frenzy and speculation, attracting investors seeking to capitalize on the potential returns of digital assets. The soaring value of cryptocurrencies and the ICO boom reshaped the financial landscape, bringing both opportunities and risks while fueling the development of innovative blockchain projects worldwide.
8. 2018 – Blockchain-based platforms like IBM's Food Trust have emerged as transformative solutions for supply chain management, enabling enhanced transparency and traceability within the food industry. By leveraging blockchain technology, these platforms offer a secure and immutable record of every step in the supply chain, promoting accountability and reducing fraud. The adoption of such blockchain solutions has the potential to revolutionize the way we track and verify the origins, quality, and safety of food products, ensuring consumer confidence and driving industry-wide improvements.
9. 2019 – Facebook's launch of the Libra cryptocurrency encountered substantial regulatory scrutiny and widespread resistance from governments worldwide. The ambitious project aimed to create a global digital currency, but concerns over data privacy, monetary sovereignty, and potential risks to the financial system led to intense pushback. The Libra initiative highlighted the complex challenges and regulatory hurdles that arise when tech giants venture into the realm of cryptocurrencies and sparked discussions on the future of digital currencies in a regulated environment.
10. 2020 – Major financial institutions like JP Morgan and Goldman Sachs have embraced blockchain technology, recognizing its potential for efficiency and security in financial operations. Simultaneously, numerous countries have launched their own central bank digital currencies (CBDCs),

aiming to leverage the benefits of blockchain and enhance their monetary systems. This combined trend showcases the growing acceptance and integration of blockchain technology within the traditional financial sector, paving the way to transformative changes in how transactions and currencies are managed globally.

11. 2021 – In a historic move, El Salvador became the first country to officially adopt Bitcoin as legal tender in 2021. This decision enabled businesses to utilize Bitcoin for paying employee salaries and established its acceptance as a valid payment method throughout the country. El Salvador's embrace of Bitcoin as a form of currency marked a significant milestone in the mainstream acceptance and integration of cryptocurrencies into national economies.
12. 2022 – The year 2022 witnessed notable blockchain growth, particularly in the emergence of national cryptocurrencies. This concept revolved around the idea of CBDCs, where central banks opted to develop their own digital coins instead of relying on decentralized cryptocurrencies. This trend highlighted a shift toward more centralized control over digital currencies, with central banks exploring the benefits and challenges of issuing their own blockchain-based currencies.
13. 2023 – The year 2023 has witnessed a notable focus on environmentally friendly blockchains, facilitated by carbon offsetting practices and energy-conscious network architectures. The adoption of greener blockchains will be made more feasible through the utilization of eco-friendly algorithms like proof of stake. These developments signify a growing commitment to reducing the environmental impact of blockchain technology and promoting sustainable practices within the industry.

1.7 Features of Blockchain

The remarkable attention and interest surrounding blockchain technology can be attributed to several key factors (Figure 1-4).

1. Immutable
   Immutability lies at the core of blockchain technology, rendering it an unchangeable and enduring network. By operating through a network of nodes, the blockchain ensures that once a transaction is recorded, it becomes permanent and resistant to modification. This immutability characteristic establishes the blockchain as a secure and trustworthy ledger, bolstering confidence in its integrity and authenticity.

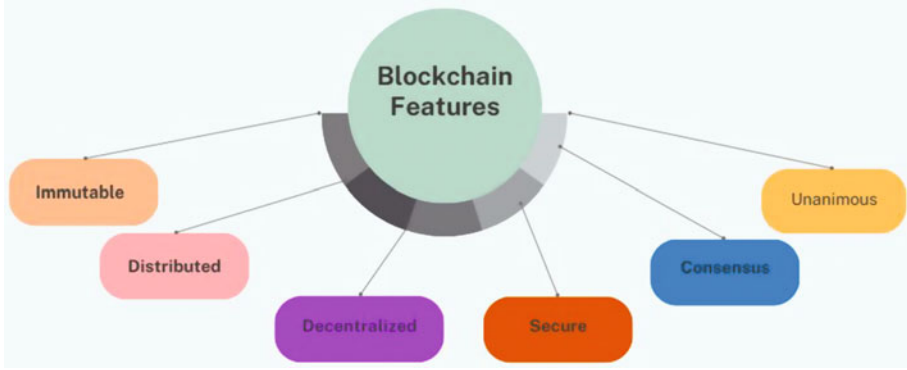

Figure 1-4 Features of blockchain