Hui LI • Han WANG

Principles and Applications of Blockchain Systems

How to Overcome the CAP Trilemma in Consortium Blockchain

IEEE Press

WILEY

Principles and Applications of Blockchain Systems

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

Principles and Applications of Blockchain Systems

How to Overcome the CAP Trilemma in Consortium Blockchain

Hui Li
Peking University
China

Han Wang
Peking University
China

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is applied for:

Hardback ISBN 9781394237227

Cover Design: Wiley
Cover Image: © Yuichiro Chino/Getty Images

Set in 9.5/12.5pt STIXTwoText by Straive, Pondicherry, India

Contents

Foreword by Peter Major

It is with great pleasure that I provide my heartfelt recommendation for the book, *Principles & Applications of Blockchain Systems: How to Overcome the CAP Trilemma in Consortium Blockchain*. As the Vice-Chairman of the United Nations Commission on Science and Technology for Development (CSTD) and the Founding Chairman of the World Digital Technology Academy (WDTA), my commitment lies in fostering sustainable development within the digital economy.

In this digital age, ensuring the trustworthy exchange of digital assets and effective governance of cyberspace stands as a paramount objective. Blockchain technology is a fundamental tool in establishing digital trust and advancing the digital economy. However, it faces a significant challenge known as the CAP trilemma, which restricts the simultaneous achievement of strong consistency, high availability, and partition fault tolerance within distributed systems. This book skillfully expounds upon the core principles of blockchain technology, empowering readers to gain a comprehensive understanding of the CAP trilemma. Furthermore, the author presents an innovative and unprecedented solution that provides both theoretical and practical support for consortium blockchains, effectively resolving the CAP trilemma conundrum.

I firmly believe that the benefits of digital technology and economic achievements should be accessible to all individuals. Beyond addressing the CAP trilemma, this book delves into essential concepts such as Web3, multilateral governance of cyberspace, DAO, DID, the digital economy, and digital assets. Web3 signifies the future direction of the Internet, paving the way for a more open, transparent, and secure network environment through decentralization and blockchain technology. Governance of cyberspace emphasizes democratic, inclusive, and cooperative global cyber governance, empowering all stakeholders to participate collaboratively in decision-making and rule-making processes. DAO and DID, as significant applications of blockchain technology, embody the decentralized autonomy of organizations and personal identity, profoundly impacting the future of the digital economy and digital asset management.

The author, Prof. Hui Li, is a prominent expert in the field of blockchain at our WDTA organization, with impressive achievements in both research and practical applications. The works presented in this book offer valuable insights and serve as a source of inspiration for readers. Through a meticulous dissection of the principles and mechanisms underlying blockchain technology, this book presents an innovative solution that empowers consortium blockchains to overcome the CAP trilemma. Whether you are a newcomer intrigued by blockchain or an experienced professional, this book will provide you with a profound understanding of the subject matter and practical solutions to address the challenges at hand.

I hope that this book provides you with valuable insights into the utilization of blockchain technology and effective resolutions to the CAP trilemma. Let us join forces to drive sustainable development within the digital economy. By immersing yourself in this book, you will acquire a comprehensive grasp of the fundamental concepts and principles of blockchain technology, thereby offering robust support for your research and practical endeavors within the realm of the digital economy. May this book enrich your knowledge and serve as an abundant source of inspiration, empowering you to make positive contributions to the advancement of the digital economy.

Peter Major
Vice-Chairman,
United Nations Commission on Science and Technology
for Development
Founding Chairman, World Digital Technology Academy

Foreword by Zhang Jing-an

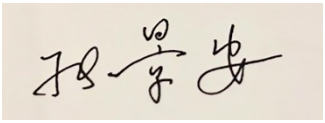
In the current era of rapid development in the digital economy, the rise of blockchain technology has undoubtedly injected strong innovative momentum into various industries. With its unique attributes – decentralization, immutability, and high transparency – blockchain is profoundly reshaping our business models and data governance frameworks. Against this backdrop, the monograph "Principle and Applications of Blockchain Systems: How to Overcome the CAP Trilemma in Consortium Blockchain," authored by Prof. Hui Li and Dr. Han Wang from Peking University, arrives at a crucial moment. It systematically and deeply analyzes the foundational theoretical framework, core key technologies, and extensive practical applications of blockchain, making significant academic contributions and offering strategic insights for guiding policy practice.

This monograph not only systematically explains the core concepts of blockchain but also provides an in-depth analysis of key technologies such as consensus mechanisms, physical topology, and P2P networks. It builds a solid foundation for academic research while offering rigorous and practical references for policymakers. In particular, the book's profound examination of the CAP trilemma provides a fresh perspective on the limitations and challenges faced by blockchain technology in practical applications, which is vital for promoting healthy technological development.

The Chinese government places a high priority on the development of blockchain technology. Since 2019, Chinese leaders have repeatedly emphasized the strategic importance of blockchain, and relevant government departments have introduced a series of policies aimed at accelerating the deep integration and widespread application of blockchain in sectors such as finance, logistics, and healthcare. The timely publication of this monograph undoubtedly provides policymakers with rich theoretical nourishment and practical guidance, helping us better understand the potential and risks of blockchain technology while fostering a positive interaction between technological and social development.

Additionally, the monograph proactively addresses cutting-edge topics such as privacy protection, quantum computing, and cross-chain technology, showcasing the vast application prospects of blockchain. It offers valuable theoretical support and practical insights for exploring compliant application paths for blockchain under the evolving landscape of laws and regulations, ensuring data security and privacy protection.

I believe "Principle and Applications of Blockchain Systems: How to Overcome the CAP Trilemma in Consortium Blockchain" serves not only as a high-quality textbook for students and faculty in higher education but also as an important reference for researchers in technology policy and colleagues in the blockchain industry. I hope that readers will seize this opportunity to gain deeper insights into the essence of blockchain technology and boldly explore its application potential across various domains, collectively contributing wisdom and strength to promote the high-quality development of China's digital economy and accelerate technological innovation. Let us work together, using this monograph as a key to unlock the doors to a new technological era and contribute to the scientific formulation and effective implementation of global technology policies.



Zhang Jing-an
Academician of the International Eurasian Academy
Secretary-General of the International Eurasian Academy (Beijing)
Chairman of the China Science and Technology System
Reform Research Association
Former President of Science and Technology Daily
Former Secretary-General of the Ministry of Science and Technology of China.

Foreword by Yale Li

It is an honor to introduce this groundbreaking work, *Principles and Applications of Blockchain Systems: How to Overcome the CAP Trilemma in Consortium Blockchain*, authored by Prof. Hui Li and Dr. Han Wang. As the Chairman of the Cloud Security Alliance (CSA) Greater China Region and Executive Chairman of the World Digital Technology Academy (WDTA), I recognize the immense potential that blockchain technology presents, especially in the rapidly evolving domain of consortium blockchains. Blockchain technology has revolutionized the way we think about distributed systems, offering unprecedented levels of security, transparency, and efficiency.

However, blockchain is not without its challenges. The CAP trilemma – balancing Consistency, Availability, and Partition tolerance – has been a significant barrier to the widespread adoption of blockchain technology, particularly in large-scale, enterprise-level consortium blockchains. In this context, the authors delve deep into the theoretical and practical aspects of addressing this issue. In an interconnected Web3 era where decentralized applications are becoming the norm, their detailed focus on reliable physical networks and smart contract security is particularly noteworthy, providing invaluable guidance for developing robust and secure blockchain systems in the Web3 era.

Prof. Hui Li, with his extensive background in future networks, cyberspace security, and blockchain technology, has been a pioneer in the field. His contributions to the development of the highly secure Multi-Identifier Network (MIN) and his recognition as a leading figure in the international digital technology community underscore his authority on this subject.

Further, the exploration of CAP-solving cases, including a mimic secure storage system and a co-governed multi-identifier system, illustrates how combining consortium blockchain technologies can innovate distributed applications. This approach enhances data and user safety and reliability, offering new insights into efficient and secure blockchain systems, which are crucial for enterprise-level applications.

Lastly, the forward-thinking exploration of quantum blockchain technology and the CAP trilemma provides a glimpse into the future of blockchain. The unique advantages of quantum computing may offer revolutionary solutions to the traditional security challenges of distributed theory and blockchain systems, positioning this book at the cutting edge of technological advancements.

In summary, this book combines meticulous research with practical insights, making it a significant contribution to the field of blockchain technology. I am confident that it will serve as an indispensable guide for anyone looking to navigate the complexities and harness the full potential of consortium blockchains. This book is a valuable resource not only for students and academics but also for engineers and practitioners developing and implementing secure, scalable blockchain solutions without being limited by the CAP trilemma.

Prof. Yale Li
Executive Chairman, World Digital Technology Academy
Chairman, Cloud Security Alliance Greater China Region
Foreign Academician, Ukrainian Academy of Engineering Sciences

Foreword by Feng Han

In 2008, Satoshi Nakamoto introduced Bitcoin, a decentralized and self-operating electronic cash system. This innovation, powered by a distributed computing network, established a new global consensus on value and currency without relying on centralized control. Bitcoin is often considered the digital equivalent of gold, as its design prevents arbitrary currency creation and circumvents the need for centralized monetary authorities. At the time of writing, Bitcoin's market capitalization has surpassed two trillion dollars, reaching an all-time high. According to the Web3 industry consensus, Bitcoin is expected to continue its growth trajectory in the coming decades.

Building on Bitcoin's legacy, Ethereum introduced smart contracts in 2014, enabling programmable execution of economic protocols directly on the blockchain. This innovation allowed for the automation of complex agreements, further advancing the vision of decentralized, self-executing economic systems. In 2024, a group of Harvard students and alumni launched the New Bretton Woods (NBW) project, which then secured a student membership at Harvard Innovation Labs to advance the initiative independently. This project leverages Bitcoin-Elastos Layer 2 blockchain technology to expand the utility of the Bitcoin ecosystem. Integrating advancements in artificial intelligence, particularly large language models, with the NBW monetary framework, the team explores the intersection of AI and blockchain technology.

Central to their vision is the concept of "AI Kallipolis," inspired by Plato's Republic. The NBW team aims to develop a fully autonomous economic management AI agent capable of on-chain asset issuance, decentralized private key management, and full Decentralized Autonomous Organization (DAO) operations. The NBW project envisions a digital economic system free from human intervention, aligning with Friedrich Hayek's advocacy for an economy governed by conscience and consensus rather than an extractive central authority. This model aspires to promote universal values of openness, fairness, transparency, security,

and freedom, potentially elevating human civilization to new levels of economic autonomy and equity.

The concept of computational power lies at the heart of artificial intelligence, a point widely acknowledged by scholars. This idea aligns with Leslie Gabriel Valiant's influential concept of the "ecorithm." Valiant, a Turing Award-winning computer scientist, introduced ecorithms as computational theories that explain how natural processes – such as learning and evolution – operate through algorithmic mechanisms. This solar-powered "natural algorithm" has enabled millions of species, beginning with single-celled organisms, to "compute" iteratively across generations, adapting to their environments. Darwin's insight into natural selection, often summarized as "survival of the fittest," exemplifies this process, and it shows just how natural computation over billions of years has led to the emergence of complex traits in species: the flight of birds, the swimming of fish, and the cognitive abilities of mammals, including highly intelligent humans.

Arithmetic computation also underpins foundational economic theories, as seen in the work of Adam Smith and Friedrich Hayek, who demonstrated how free-market dynamics can be understood through principles akin to algorithmic computation. In this view, each transaction represents a form of "computation" that fosters the division of labor, promotes the efficient distribution of goods, and enables the rise of urban centers and trade hubs. Over time, these economic "computations" give rise to complex social structures, from ethical norms to legal frameworks, which collectively form the foundations of modern civilization. From the perspective that all systems – biological, social, or economic – can be framed as computational processes, the development of advanced artificial intelligence appears not as an anomaly, but as an inevitable outcome of this computational paradigm.

The AI Kallipolis project, developed by NBW, represents a new phase in the evolutionary trajectory of computational and economic systems. Designed as an impartial executor of market rules, AI Kallipolis operates without the influence of external interest groups, and it promises a freer, more transparent marketplace where interactions between humans and AI are secured, and the integrity of market dynamics is upheld. In this model, AI functions as a tool for advancing societal goals, fostering an "algorithmic harmony" that aligns with the natural and economic order. This system, in principle, reflects the Buddhist ideal of the "equality of all beings," ensuring that every entity, whether carbon- or silicon-based, is respected within this computational ecosystem.

This vision aligns with Elon Musk's aspiration for an "interstellar civilization," but here, NBW anticipates a future where such a civilization is not limited to humanity alone. A Mars-based civilization could well be predominantly composed of AI agents, converging with human society within a unified digital economy. On that day, AI Kallipolis, underpinned by Bitcoin's decentralized framework, could

serve as a bridge between carbon-based and silicon-based civilizations, giving Bitcoin's narrative economy a critical and tangible role. As the GDP of this encrypted economy expands into the trillions, Bitcoin may indeed take on the function that Ray Dalio predicts, addressing global debt challenges and fostering economic resilience on an unprecedented scale.

It is with this profound understanding of the importance of AI and blockchain governance for the future of human civilization that we eagerly anticipate Professor Hui Li's monograph, "Principles and Applications of Blockchain Systems: How to Overcome the CAP Trilemma in Consortium Blockchain".

Feng Han
Independent Researcher
Harvard University

Foreword by Ramesh Ramadoss

I feel honored to write this foreword. I have witnessed firsthand the rapid evolution, groundbreaking innovations, and gradual adoption of blockchain and distributed ledger technologies (DLTs).

The CAP theorem for distributed systems has demonstrated that the software optimization of blockchain, as a distributed system, is constrained by the CAP trilemma, which reveals the impossibility of simultaneously achieving strong consistency, high availability, and partition tolerance. While several blockchain trilemmas have emerged in recent years, the CAP trilemma remains the only one that has been rigorously proven. This book squarely addresses the challenges posed by the CAP trilemma in the blockchain field by conceptually linking the CAP theorem with blockchain challenges. Particularly, this book discusses consistency, scalability, and partition tolerance as the focal points of the trilemma and explores potential solutions in the context of permissioned blockchains.

In terms of content, this book delves deeply into the core layers of the blockchain system, such as the physical layer, the network layer, and the consensus layer. It proposes a practical design framework for a consortium blockchain system that effectively addresses the CAP trilemma. The design is inspired by engineering practice, where the domain of P includes both the failure scenario (when partitioning occurs) and the correct scenario (when partitioning occurs but is handled correctly). The former scenario requires a trade-off between CA, while the latter does not. The consortium blockchain solution, from an engineering perspective, eliminates partition failures at the hardware level through meticulous implementation strategies. At the same time, it ensures strong consistency and high availability by leveraging the software level to implement CA in most cases. The practical application cases in the book demonstrate the feasibility of this solution in future network management and secure storage applications.

Furthermore, the book explores the impact of quantum computing on classical distributed theory and discusses the potential of quantum blockchain to transcend the limitations of the FLP and CAP theorems. This perspective sheds light on the

future direction and potential impact of blockchain systems, presenting exciting possibilities for the field.

Prof. Hui Li and Dr. Han Wang, with their extensive research backgrounds and practical experience, provide a comprehensive guide that bridges the gap between theory and practice. I highly recommend this book to anyone seeking to understand and address the challenges of the CAP trilemma and its application to blockchain technology. The theoretical foundations and practical solutions presented here are certain to leave a lasting impact on both the current understanding and the future development of blockchain technology.

I have no doubt this significant contribution will inspire further research and development in this field. The work presented here stands as a testament to the authors' relentless pursuit of innovation and excellence. Their work is not merely an academic treatise; it is a practical guide for engineers, researchers, and students.

September 12, 2024
Oxford, UK

Ramesh Ramadoss, PhD
Chair, IEEE Blockchain Technical Community
Member, Board of Governors, IEEE Standards Association

About the Author

Hui Li is a Emeritus professor of Peking University, chief information scientist of IASTIC (International Academician Science & Technology Innovation Center); foreign academician of Russia Academy of Natural Science, member of the National Academy of Artificial Intelligence US (NAAI), member of Expert Committee of World Digital Tech. Academy under guidance of UN Commission on Sci. & Tech. for Developments, fellow of IET, distinguished member of CCF China. He is director of PKU Lab of CENI (China Environment for Network Innovations), National Major Research Infrastructure; Technology Execute Director of Sino-EU Intelligent Connected Vehicle and Autonomous Driving Industry Innovation Alliance (SASD). He received his BEng and MS degrees from School of Information Engineering, Tsinghua University, Beijing, China, in 1986 and 1989, respectively, and PhD degree from Department of Information Engineering, The Chinese University of Hong Kong in 2000.

Prof. Hui Li proposed the first co-governed sovereignty network MIN (Multi-Identifier Network) based on future network architecture and blockchain technology, and implemented its prototype and system on operator's network in the world. MIN was obtained the award of World Leading Internet Scientific and Technological Achievements by the 6th World Internet Conference (WIC) on 2019, WuZhen, China. He was invited to give keynote speech on topic MIN more than hundred conferences around the world, including at the International Side Event of 2023 WIC Wuzhen China held by IEEE, 2023 World AI Conference Shanghai; 2024 Digital World Conference Geneva Summit organized by WDTA

(World Digital Technology Academy), The 27th Session of the United Nations Commission on Science & Technology for Development "Shaping the Future of AI" Side Event (UN CSTD 2024). He was invited as guest editor of ZTE COMMUNICATIONS March 2020 Vol. 18 No. 1 (Issue 69), with topic: Domain Name and Identifier of Internet: Architecture & Systems. The first English monograph by theme of "Cyberspace UN" in the world has been published by Springer Publisher with title *Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture* on 2021. His research interests include network architecture, cyberspace security, blockchain, distributed storage. As the first author, he has published four monographs with field on Future Network Architecture, Consensus Algorithms on Blockchain, and Distributed Storage Theory and System.

Han Wang received her BSc degree in communication engineering from Jilin University in 2017, followed by the completion of her PhD degree in computer application technology from Peking University in 2024. Currently, she holds the position of a postdoctoral fellow at PengCheng Laboratory. Her research interests include multi-identifier network architecture, blockchain technology, and cybersecurity.