



Hui LI • Han WANG

Principles and Applications of Blockchain Systems

How to Overcome the CAP Trilemma
in Consortium Blockchain

 **IEEEPress**

WILEY

Principles and Applications of Blockchain Systems

IEEE Press

445 Hoes Lane

Piscataway, NJ 08854

IEEE Press Editorial Board

Sarah Spurgeon, *Editor-in-Chief*

Moeness Amin

Jón Atli Benediktsson

Adam Drobot

James Duncan

Ekram Hossain

Brian Johnson

Hai Li

James Lyke

Joydeep Mitra

Desineni Subbaram Naidu

Tony Q. S. Quek

Behzad Razavi

Thomas Robertazzi

Diomidis Spinellis

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

 **IEEEPress**

WILEY

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved.

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

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

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	<i>xv</i>
Foreword by Zhang Jing-an	<i>xvii</i>
Foreword by Yale Li	<i>xix</i>
Foreword by Feng Han	<i>xxi</i>
Foreword by Ramesh Ramadoss	<i>xxv</i>
About the Author	<i>xxvii</i>
Preface	<i>xxix</i>
Acknowledgments	<i>xxxiii</i>
Introduction	<i>xxxv</i>

1	Fundamentals of Blockchain	1
1.1	Introduction to Blockchain	1
1.2	Evolution of Blockchain	4
1.2.1	Value Evolution in Blockchain Applications	4
1.2.2	Blockchain Underlying Platform	7
1.2.2.1	Public Blockchain	7
1.2.2.2	Consortium Blockchain	8
1.2.2.3	Blockchain as a Service	8
1.2.3	Blockchain Security, Regulation, and Governance	9
1.2.3.1	Security	9
1.2.3.2	Regulation	11
1.2.3.3	Governance	12
1.3	Blockchain-Layered Architecture	13
1.3.1	Physical Layer	14
1.3.2	Data Layer	14
1.3.3	Network Layer	15
1.3.4	Consensus Layer	15
1.3.5	Incentive Layer	15
1.3.6	Contract Layer	15
1.3.7	Application Layer	15

1.4	Theoretical Constraints of Blockchain Trilemma	16
1.4.1	CAP Theorem for Distributed Systems	16
1.4.2	Classic Blockchain Solution to Trilemmas	19
1.4.3	General Blockchain Trilemma	21
1.4.3.1	Consistency	23
1.4.3.2	Scalability	23
1.4.3.3	Partition Tolerance	23
1.4.4	Consortium Blockchain Framework for Resolving Trilemma	24
1.4.4.1	Upper Layer: Consensus and Data Layer	24
1.4.4.2	Middle Layer: Network Layer	25
1.4.4.3	Lower Layer: Physical Layer	26
1.5	Chapter Summary	26
	Discussion Questions	27
	References	28
2	Physical Topology in Blockchain	31
2.1	Basic Physical Topology of Computer Network	31
2.1.1	Bus	32
2.1.2	Star	33
2.1.3	Ring	35
2.1.4	Tree	36
2.1.5	Mesh	37
2.1.6	Hybrid Topology	39
2.2	N-Dimensional Hypercube-Based Topology – Making it Possible to Reach CAP Guarantee Bound in Consortium Blockchain	40
2.3	Hierarchical Recursive Physical Topology of N-Dimensional Hypercube	43
2.4	Theoretical Analysis	45
2.4.1	Basic Physical Topology	46
2.4.1.1	Quantitative Model for the Partition Tolerance Property	46
2.4.1.2	Simulation	49
2.4.2	Hierarchical Recursive Physical Topology	49
2.4.2.1	Partition Tolerance Property	51
2.4.2.2	Link Consumption	52
2.5	Chapter Summary	54
	Discussion Questions	54
	References	56
3	P2P Network in Blockchain	59
3.1	P2P Network Structure	59
3.1.1	Traditional P2P Network Structure	60

3.1.2	P2P Network Structure in Blockchain	61
3.2	Node Discovery Method	64
3.2.1	Bitcoin Node Discovery	64
3.2.1.1	Hard-Coded Seed Nodes	64
3.2.1.2	Address Broadcast	64
3.2.1.3	Addresses Stored in Database	65
3.2.2	Ethereum Node Discovery	66
3.2.2.1	Seed Nodes	66
3.2.2.2	Addresses Stored in Database	66
3.2.2.3	Address Query	67
3.2.2.4	Address Broadcast	67
3.2.3	Hyperledger Fabric Node Discovery	67
3.2.3.1	Seed Nodes	67
3.2.3.2	Address Broadcast	68
3.2.3.3	Specification Through Command Line	69
3.3	Broadcast Protocol	69
3.3.1	Gossip	69
3.3.2	Innovative Broadcast Protocol	71
3.3.2.1	New Node Joining	73
3.3.2.2	Message Broadcasting	75
3.3.2.3	Adaptability Analysis in Future Network	78
3.3.2.4	Experiments and Analysis	80
3.4	Chapter Summary	83
	Discussion Questions	83
	References	84
4	Blockchain Consensus	87
4.1	Basic Concepts of Distributed Consistency	87
4.1.1	SMR Model in Blockchain System	87
4.1.2	FLP Theorem	88
4.1.3	Distributed Network Assumption	88
4.1.4	Paxos	92
4.1.4.1	Prepare Phase	92
4.1.4.2	Accept Phase	93
4.1.5	Raft	93
4.1.5.1	Leader Election	94
4.1.5.2	Log Replication	94
4.2	Byzantine Generals Problem	95
4.2.1	Oral Message Algorithm	96
4.2.2	Signed Message Algorithm	98
4.3	Voting-Based Consensus	100

4.3.1	Partial Synchronization Class	101
4.3.1.1	Practical Byzantine Fault Tolerance	101
4.3.1.2	Consensus of Trust	105
4.3.2	Synchronization Class	107
4.3.2.1	RPCA	107
4.3.2.2	SCP	109
4.3.3	Asynchronous Class	110
4.3.3.1	HoneyBadgerBFT	110
4.3.3.2	Dumbo	112
4.3.3.3	Dumbo-NG	114
4.4	Proof-Based Consensus	115
4.4.1	PoW	116
4.4.2	Variants of PoW	118
4.4.2.1	Bitcoin-NG	119
4.4.2.2	GHOST	120
4.4.3	PoS	121
4.4.3.1	Coinstake Transaction	123
4.4.3.2	Kernel Protocol	123
4.4.3.3	Coin Age	124
4.4.3.4	Stake Reward	124
4.4.4	Variants of PoS	124
4.4.4.1	Ouroboros	125
4.4.4.2	DPoS	126
4.4.4.3	Conflux	128
4.4.5	PoX	130
4.5	Consensus Integrating Proof and Voting	130
4.5.1	PoV	131
4.5.2	PPoV	135
4.5.2.1	Prepare Phase	136
4.5.2.2	Vote Phase	137
4.5.2.3	Commit Phase	138
4.5.3	Lightweight PPoV	140
4.5.3.1	Adaptive Timeline Adjustment Method	142
4.5.3.2	Tentative Transaction Query Method	143
4.5.4	Mimic PPoV	145
4.5.5	HotStuff	147
4.5.5.1	Basic HotStuff	148
4.5.5.2	Chained HotStuff	149
4.5.6	VaaP	150
4.5.6.1	Processing at Leader	152
4.5.6.2	Processing at Replicas	153
4.6	Evaluation and Analysis of Blockchain Consensus	155

4.6.1	Evolution	155
4.6.1.1	Main Line One: Development of Voting-Based Consensus	155
4.6.1.2	Main Line Two: Development of Proof-Based Consensus	157
4.6.1.3	Main Line Three: Development of Consensus Integrating Proof and Voting	158
4.6.2	Evaluation and Comparison	159
4.7	Chapter Summary	160
	Discussion Questions	163
	References	164
5	Smart Contract and Its Security in Blockchain	169
5.1	Concept of Smart Contracts	169
5.2	Vulnerability in Smart Contracts	171
5.2.1	Solidity Layer	171
5.2.1.1	Reentrancy	171
5.2.1.2	Integer Error	171
5.2.1.3	Exception Handling	171
5.2.1.4	Logical Error	172
5.2.1.5	Access Control	172
5.2.1.6	Unchecked Call Return Value	172
5.2.2	EVM Layer	172
5.2.2.1	Short Address	172
5.2.2.2	Tx.origin	173
5.2.2.3	Call-Stack Overflow	173
5.2.3	Block Layer	173
5.2.3.1	Timestamp Dependency	173
5.2.3.2	Transaction Order Dependency	173
5.2.3.3	Block Parameter Dependency	173
5.2.4	Web 3.0 Vulnerabilities	174
5.2.4.1	Identifier Verification	174
5.2.4.2	Rent Tampering	174
5.2.4.3	Single Oracle	174
5.2.4.4	Sandwich Attack	175
5.3	Taxonomy of Approaches to Detecting Vulnerabilities	175
5.3.1	Formal Verification	175
5.3.2	Symbolic Execution	177
5.3.3	Fuzzing	178
5.3.4	Taint Analysis	180
5.3.5	Machine Learning	182
5.3.6	Improved Integration of Symbolic Execution and Machine Learning	183
5.3.6.1	Deep Learning Module	184

5.3.6.2	Symbolic Execution Module	185
5.3.6.3	Data Processing Module	186
5.4	Detection Tools for Smart Contract Vulnerability	186
5.4.1	Traditional Tools	186
5.4.1.1	VaaS	186
5.4.1.2	Mythril	187
5.4.1.3	Securify	187
5.4.1.4	Manticore	187
5.4.1.5	Slither	187
5.4.2	Detecting Vulnerabilities in Smart Contracts for Web 3.0	188
5.4.3	Comparison of Existing Tools	192
5.4.3.1	Vulnerability Coverage	192
5.4.3.2	Detection Effectiveness	194
5.4.3.3	Open-Source Availability	194
5.4.3.4	Integration Capabilities	195
5.5	Chapter Summary	195
	Discussion Questions	196
	References	197
6	Multi-Identifier System Based on Large-Scale Consortium Blockchain	203
6.1	Background Introduction and Requirement Analysis	203
6.2	System Architecture	204
6.2.1	Basic Single-Chain Architecture	205
6.2.1.1	Tier 1: Network Tier for Blockchain Nodes	205
6.2.1.2	Tier 2: Lightweight Consensus Tier	208
6.2.1.3	Tier 3: Index Tier	211
6.2.1.4	Tier 4: Storage Tier	212
6.2.2	Hierarchical Architecture for Large-Scale Network	213
6.3	Core Functions	215
6.3.1	Identity Management and Access Control	215
6.3.2	Registration, Update, and Revocation of Identifiers	217
6.3.3	Resolution of Identifiers	219
6.3.4	Inter-Translation of Identifiers	220
6.4	Building a Community of Shared Future in Cyberspace with Sovereign Blockchain	222
6.4.1	Background Introduction	222
6.4.2	Cross-Chain and Sovereign Internet	223
6.4.2.1	Hash-Locking	223
6.4.2.2	Sidechains	225
6.4.2.3	Notary Schemes	227

6.4.2.4	Relay	228
6.4.2.5	Distributed Private Key Control	230
6.4.2.6	Communication Protocol Suites	230
6.4.3	Co-Governed Community of Shared Future in Cyberspace	231
6.4.3.1	The Challenge of Interconnectivity	232
6.4.3.2	A Central Relay Chain as the Solution	232
6.4.3.3	The Role of MIS in Cross-Chain Solutions	232
6.4.3.4	Performance and Efficiency	232
6.4.3.5	Implementation of MIS as a Relay Chain	233
6.4.3.6	The Shared Sovereign Internet and a Co-Governed Cyberspace	234
6.4.3.7	The Future of Co-Governed Cyberspace	234
6.4.3.8	Ensuring Security and Privacy in a Co-Governed Cyberspace	235
6.4.3.9	Regulatory Compliance and Standardization	235
6.4.3.10	The Role of Multilateral Governance	236
6.5	Chapter Summary	236
	Discussion Questions	237
	References	238

7 Integrating Consortium Blockchain and Mimic Security in Distributed Storage System 241

7.1	Background Introduction and Requirement Analysis	241
7.2	Mimic Distributed Secure Storage System	249
7.2.1	System Principle	249
7.2.1.1	Related Technologies	249
7.2.1.2	Mimic Distributed Object Storage Model	250
7.2.1.3	Storage Model Characteristics	251
7.2.2	System Architecture	252
7.2.2.1	Mimic Interface Service	253
7.2.2.2	Metadata Service	253
7.2.2.3	Data Service	253
7.2.3	Core Functions	254
7.2.3.1	Data Positioning	254
7.2.3.2	Data Migration	255
7.2.3.3	Data Recovery	256
7.3	Logging System in Mimic Storage Based on Consortium Blockchain	256
7.3.1	System Architecture	257
7.3.2	Core Functions	259
7.3.2.1	Log Collection and Dispatch	259
7.3.2.2	Design of Blockchain-Based Log Storage	260
7.4	Chapter Summary	267

Discussion Questions	267
References	268

8	Quantum Blockchain and Its Potential Applications	271
8.1	Quantum Computing and Communication Theory	271
8.1.1	Quantum Physical Concepts and Qubit Properties	272
8.1.2	Quantum Gates and Quantum Circuits	282
8.1.2.1	Bell Circuit	286
8.1.2.2	Reverse Bell Circuit	286
8.1.2.3	GHZ Circuit	287
8.1.2.4	W State Circuit	287
8.1.3	Quantum Memory and Quantum Computers	291
8.1.3.1	Quantum Memory	292
8.1.3.2	Quantum Computers	297
8.1.4	Quantum Key Distribution and Quantum Communication	303
8.1.4.1	Quantum Key Distribution	304
8.1.4.2	Superdense Coding	305
8.1.4.3	Quantum Teleportation	306
8.2	Quantum Blockchain – Solving Trilemma of Distributed Systems	308
8.2.1	Quantum Blockchain Solution	308
8.2.2	Quantum Proof of Vote Consensus	311
8.2.2.1	Quantum Fourier Transform and Two Quantum Entangled States	312
8.2.2.2	Design of Q-PoV Consensus	315
8.2.2.3	Q-PoV Workflow Example	319
8.2.3	FLP and CAP Theorems in Quantum Blockchain	320
8.2.3.1	Quantum Technology and FLP Theorem	320
8.2.3.2	Quantum Technology and CAP Theorem	321
8.3	Scalable Quantum Computer Network	322
8.3.1	Quantum Internet	323
8.3.2	Quantum Multi-Identifier Network Architecture with Quantum Identifier	332
8.3.3	Quantum Multi-Identifier System and Router	340
8.3.4	Future Prospect of Quantum Technology	341
8.4	Chapter Summary	342
	Discussion Questions	343
	References	344
9	Practical Application of Large-Scale Blockchain	347
9.1	Construction of Network Topology	347
9.2	P2P Broadcast Protocol	353
9.2.1	Environment Setup	354

9.2.1.1	Manual Environment Setup	354
9.2.1.2	Using Docker Containers for Simplified Setup	355
9.2.2	Operation and Evaluation	356
9.3	Solidity Language	357
9.3.1	Getting Started Example	358
9.3.1.1	Open the Online Compiler	358
9.3.1.2	Solidity Program	359
9.3.1.3	Compile	359
9.3.1.4	Deploy	360
9.3.1.5	Test	361
9.3.2	Basic Syntax	362
9.3.2.1	Common Types	362
9.3.2.2	Function Types	364
9.3.2.3	Special Variables	364
9.3.2.4	Event Logs	366
9.3.2.5	Error Handling	367
9.4	Establishment of Blockchain Infrastructure	369
9.4.1	Establishment of a Private Blockchain	369
9.4.2	Deployment and Testing of Smart Contracts	371
9.5	Smart Contract Security Detection	373
9.6	Chapter Summary	374
	Discussion Questions	375
	References	375
	Index	377

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

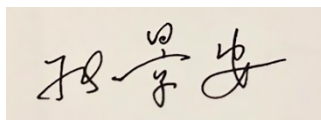
In the current era of rapid development in the digital economy, the rise of blockchain technology has undoubtedly injected strong innovative momentum into various industries. With its unique attributes – decentralization, immutability, and high transparency – blockchain is profoundly reshaping our business 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.

A handwritten signature in black ink, reading "Yale Li". The signature is fluid and cursive, with the first name "Yale" and the last name "Li" clearly distinguishable.

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".

A handwritten signature in black ink, reading "F. Han". The "F" is large and stylized, with a horizontal bar. The "H" is also large, and the "an" is written in a cursive, flowing style.

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

A handwritten signature in blue ink, appearing to read 'R. Ramadoss', with a stylized flourish at the end.

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.