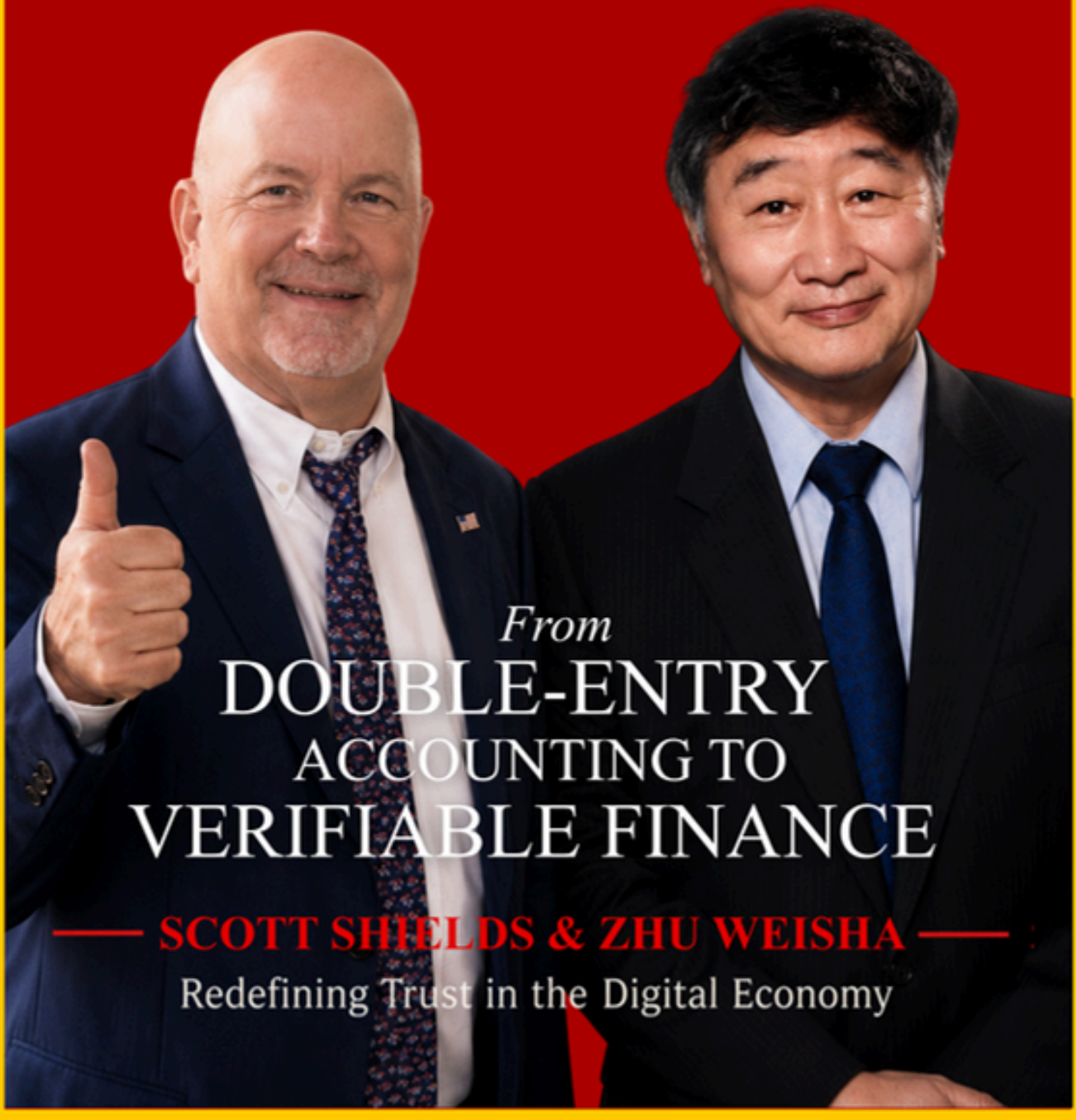
WWW.CAPITOLTIMESMEDIA.COM Vol. 2 ISSUE 37 - BUSINESS EDITION ISSN: 2998-8004

CAPITOL TIMES MAGAZINE



From

DOUBLE-ENTRY ACCOUNTING TO VERIFIABLE FINANCE

SCOTT SHIELDS & ZHU WEISHA

Redefining Trust in the Digital Economy

THE SECRET IS NOW OUT!

WHAT IS MOST POPULAR AT CONVENIENCE STORES IS NOW BECOMING THE TWO FAVORITE TOPPINGS AT PIZZERIA'S.

PizzaRelish.com

PIZZA RELISH BELONGS ON A SLICE TOO.

IT STARTED AT THE CORNER CONVENIENCE STORE.

MORE CRUNCH. MORE FLAVOR. MORE LOVE.

PIZZA PICKLE RELISH

The Crunch That Changed Everything.

From the hot dog stand to the cheese pull, our Pizza Pickle Relish adds a zesty tang that cuts through the grease perfectly.

PIZZA PEPPER RELISH

A Perfect Blend of Peppers.

The second half of the ultimate topping combination for the spicy pizza lover.

TWO TOPPINGS. ENDLESS POSSIBILITIES.

Add Both. Thank Us Later.

SPONSORED ADVERTISEMENT

GRISSINI'S®

AUTHENTIC ARTISAN BREADSTICKS

THE ART OF AUTHENTIC ITALIAN BREADSTICKS

Handcrafted. Artisan. Unforgettable.

Born from generations of Italian baking tradition, Grissini's artisan breadsticks are crafted using a legendary sourdough starter perfected over 40 years. Every breadstick delivers authentic flavor, delicate crunch, and premium quality designed for the finest hospitality experiences.

HANDCRAFTED ARTISAN BREADSTICKS

TRADITIONAL SOURDOUGH RECIPE

NO PRESERVATIVES

LOWER SODIUM • HEART HEALTHY

VEGAN OPTION AVAILABLE

PREMIUM QUALITY
FOR HOSPITALITY & CATERING

SIGNATURE FLAVORS

SEA SALT PARMESAN • HERB • FOUR SEED • HONEY GRAHAM • RED PEPPER SPICE

ELEVATE EVERY DINING EXPERIENCE

Whether served at fine dining restaurants, private events, hotels, stadium suites, or executive catering tables — Grissini's transforms a simple breadstick into a premium culinary statement.

Crafted with passion. Inspired by Italy. Served with distinction.

MANUFACTURED IN AMERICA

PREMIUM BREADSTICKS FOR HOSPITALITY & CATERING

WWW.GRISSINIS.COM

SPONSORED ADVERTISEMENT

www.artisemediaent.com

STORIES THAT INSPIRE.
VALUES THAT LAST.

BREAK THE HOLLYWOOD ESTABLISHMENT

WE ARE BUILDING A NEW MOVEMENT

Artise Media Entertainment is a next-generation studio creating powerful, entertaining, and values-driven films that uplift, unite, and inspire.

OUR MISSION

RESTORE REAL AMERICAN VALUES

THROUGH POWERFUL STORYTELLING

FAITH
In God and in each other.

FAMILY
The foundation of our nation.

FREEDOM
Liberty, justice, and responsibility.

INTEGRITY
Doing what's right even when it's hard.

HOPE
A better tomorrow through truth.

WE ARE LOOKING FOR INVESTORS

TO BUILD MORE THAN MOVIES—
TO BUILD A LEGACY.

Join us in creating a new era of family-friendly, faith-based, and patriotic films that America—and the world—desperately needs.
Strong stories. Strong values. Strong returns.
Together, we can change Hollywood.

STRONG MARKET DEMAND
Audiences are hungry for meaningful entertainment.

PROFITABLE POTENTIAL
Family films deliver loyal audiences and long-term value.

GLOBAL IMPACT
Positive content that transcends generations and borders.

VALUES-DRIVEN BRAND
A company built on purpose, not just profit.

EXPERIENCED TEAM
Industry veterans with a bold new vision.

Sponsored Advertisement

COURAGE COSTS. FREEDOM REQUIRES IT.

JUSTICE FOR TINA PETERS.

CAPITOL TIMES MAGAZINE

When the Heartland Speaks, America Listens


ANIL ANWAR
Editor-In-Chief
Capitol Times Magazine
www.capitoltimesmedia.com

GET YOUR CAPITOL TIMES MAGAZINE

PRINT SUBSCRIPTION TODAY

UNFILTERED TRUTH
Hard-hitting journalism the mainstream media won't touch.

DEFEND FREEDOM
Stand for liberty, sovereignty, and our constitutional values.

STAY INFORMED
In-depth analysis on politics, faith, and the issues that matter most.

SUPPORT REAL JOURNALISM
Independent. Bold. Fearless. Committed to the truth.

Your unfiltered source for truth, freedom, and the news they don't want you to read.

capitoltimesmedia.com/magazine-subscription

POWER MOVES IN SILENCE.

WE REPORT IT.

Capitol Times Magazine gives you the real story behind the decisions that shape your world—before they become headlines.

Investigative Reporting. Unfiltered Analysis. No Fluff. No Spin.

Stay Informed. Stay Ahead.

JOHN 3:16 "FOR GOD SO LOVED THE WORLD, THAT HE GAVE HIS ONLY SON, THAT WHOEVER BELIEVES IN HIM SHOULD NOT PERISH BUT HAVE ETERNAL LIFE"

CAPITOL TIMES
MEDIA - MAGAZINE

ISSN - Print: 2998-8004 | Online: 2998-8012

Editor-In-Chief
Anil Anwar

Associate Editor
David Colbert
Saba Jenn

Creative Director
By Saba Jenn

Front Cover
Photos Provided by Scott Shields

Editorial Photos
- Capitol Times Editorial

Photo Editor
Capitol Times Editorial Team

Owned by Capitol Times Media LLC. Printed in the United States of America
All Rights Reserved - 2026

Copyright Disclaimer: Capitol Times Magazine utilizes photos solely for editorial purposes and provides proper credit to the copyright holders.

www.capitoltimesmedia.com

Disclaimer

The views and opinions expressed in the articles or Interviews published in this magazine are solely those of the respective authors and do not necessarily reflect the official policy or position of the Capitol Times magazine, its editors, or its staff. The authors are solely responsible for the content of their articles.

The magazine strives to provide a platform for diverse voices and opinions, and we value the principle of free expression.

The magazine assumes no responsibility or liability for any errors or omissions in the content of the articles. In no event shall the Capitol Times magazine be liable for any special, direct, indirect, or incidental damages.

Furthermore, the inclusion of advertisements or sponsored content in Capitol Times magazine does not constitute an endorsement or guarantee of the products, services, or views promoted by the advertisers. Readers are encouraged to conduct their own research and exercise caution when making decisions based on advertisements or sponsored content featured in this publication.

Thank you for reading and engaging with our publication. Your feedback is valuable to us as we continue to provide a platform for thought-provoking content and diverse perspectives.

Editor's Note

CAPITOL TIMES MAGAZINE – ISSUE 37 | JULY 2026

Dear Readers,

Welcome to Issue 37 of Capitol Times Magazine, an edition dedicated to one of the most consequential debates of the digital age: the future of finance. This Business Edition explores a bold research framework that argues the next evolution of global finance will be built not merely on trust, but on verifiable facts, transparency, and technological accountability.

At the center of this issue is the groundbreaking work of Founder Zhu Weisha, whose extensive research introduces the concept of Verifiable Finance—a framework that examines how blockchain, Bitcoin, artificial intelligence, and transparent banking could reshape financial systems for the twenty-first century. Rather than focusing solely on cryptocurrency prices or speculation, this edition challenges readers to consider how future institutions may evolve toward greater accountability and measurable trust.

The magazine examines topics including the Public Credit Root, Transparent Banks, Bitcoin's institutional role, the future of stablecoins, and the strategic implications of digital finance for the United States. Whether readers ultimately agree or disagree with every conclusion, the ideas presented deserve careful consideration as governments, businesses, and financial institutions prepare for an increasingly digital economy.

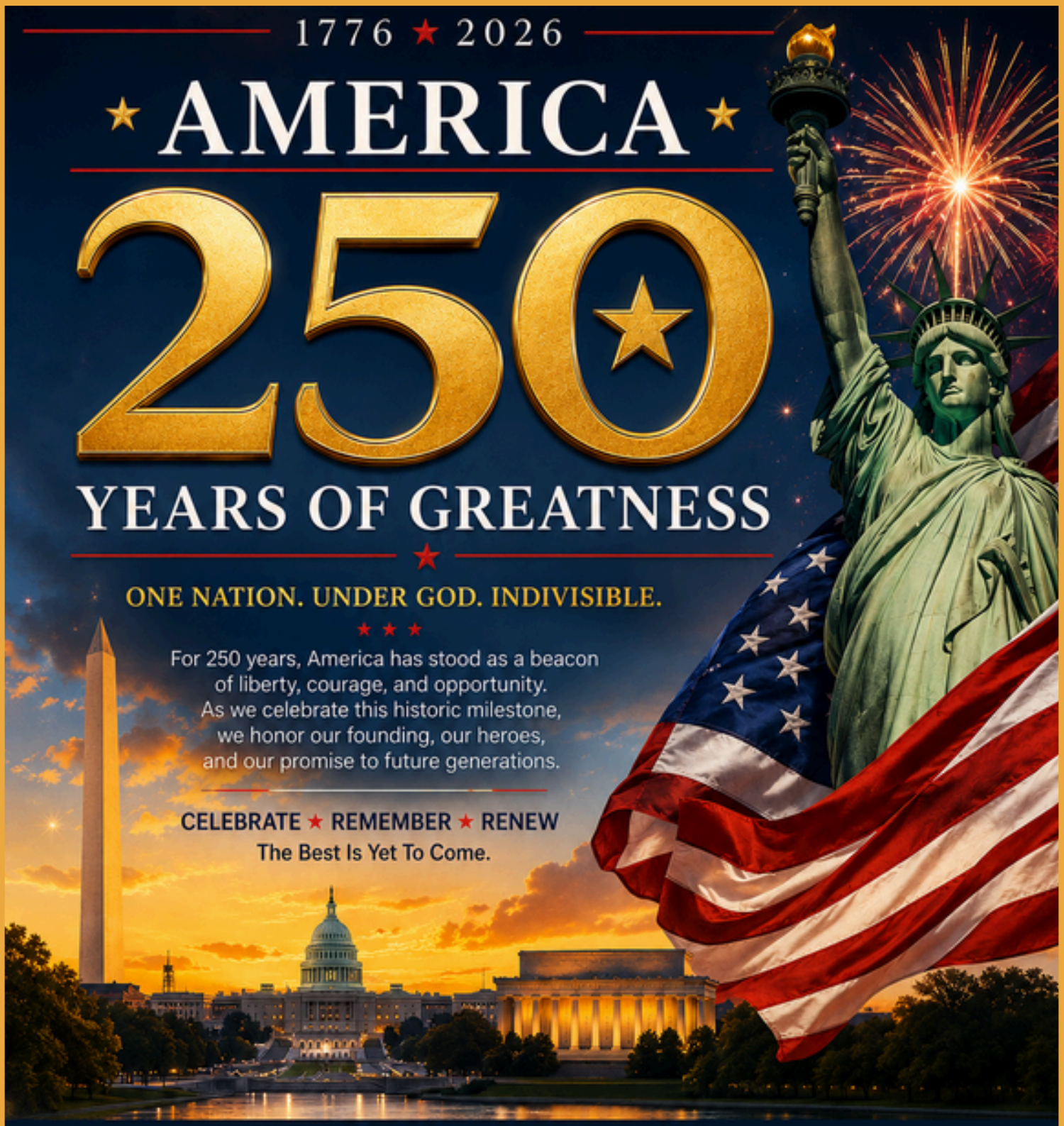
> ***We remain committed to presenting influential ideas, encouraging informed debate, and giving innovators a platform to share their vision with policymakers, business leaders, and our readers across America.***

At Capitol Times, we remain committed to presenting influential ideas, encouraging informed debate, and giving innovators a platform to share their vision with policymakers, business leaders, and our readers across America.

Anil Anwar
Editor-In-Chief

Anil Anwar

CAPITOL TIMES
MEDIA - MAGAZINE



CAPITOL TIMES
MEDIA - MAGAZINE

READ. SHARE. CELEBRATE.
BE PART OF HISTORY.

CAPITOL TIMES

MAGAZINE

REAL NEWS. REAL AMERICA.

Proudly Conservative. Unapologetically American.

SCAN TO VISIT
CAPITOL TIMES
capitoltimesmedia.com

★ ★ ★ ★ ★

Capitol Times
MAGAZINE

Contact Us

ads@capitoltimes.com
www.capitoltimesmedia.com

Capitol Times Magazine offers unmatched access to Washington, DC's most influential audiences.

Why Choose Us?

with a sample ad tailored to highlight our strengths:

1. **Targeted Reach to Power Players :** We deliver directly to policymakers, decision-makers, lobbyists, and VIPs in Washington, DC.
2. **High-Impact, Engaged Audience:** Our readers are affluent, educated, and influential, actively seeking insights and opportunities in the nation's capital. Your ad connects with a captive audience that values quality and relevance.
3. **Cost-Effective Advertising:** Even a small ad delivers big results due to our hyper-focused distribution and premium readership. Maximize your ROI with a platform designed for influence.

Your Brand. Their Power.

Reach DC's policymakers, lobbyists, and VIPs with Capitol Times Magazine. Your ad connects with the nation's decision-makers. Influence the influencers. Advertise Today!

CAPITOL TIMES MAGAZINE Issue 37

CONTENTS

www.capitoltimesmedia.com

Introduction

CONTENTS

www.capitoltimesmedia.com

CONTENTS

www.capitoltimesmedia.com

Subscribe now

Join our mailing list to receive the latest news and trends.

Sign up now
Capitoltimesmedia.com

REAL NEWS. HONEST VIEWS. CONSERVATIVE PRINCIPLES.

CAPITOL TIMES

MAGAZINE

INDEPENDENT. UNAPOLOGETIC. ALWAYS AMERICA FIRST.

In-depth political analysis, exclusive interviews, and conservative commentary on the issues that shape our nation.

POLITICAL INSIGHTS
In-depth reporting on policy, elections, and government.

EXCLUSIVE INTERVIEWS
Conversations with leaders, thinkers, and change makers.

CONSERVATIVE VOICES
Principled perspectives on the issues that matter most.

AMERICA FIRST
Strong. Sovereign. Free. That's the American way.

NOT AFFILIATED WITH THE U.S. GOVERNMENT OR CONGRESS.
PRIVATELY OWNED. INDEPENDENT. TRUE TO OUR READERS.

SUBSCRIBE TODAY
AND NEVER MISS AN ISSUE.

PRINT EDITION
High-quality print delivered to your door.

DIGITAL EDITION
Read anywhere, anytime on your favorite device.

GREAT GIFT
Perfect for family, friends, and patriotic readers.

AVAILABLE ON

amazon · BARNES & NOBLE · BAM! BOOKS-A-MILLION · INDIEBOUND

AND OTHER MAJOR BOOK & MAGAZINE RETAILERS

CAPITOL TIMES MEDIA · MAGAZINE

INFORMING. INSPIRING. EMPOWERING AMERICANS.

VISIT US ONLINE
CAPITOLTIMESMEDIA.COM

FOLLOW US

Capitol Times Media LLC IS AN INDEPENDENT MEDIA COMPANY AND IS NOT AFFILIATED WITH THE U.S. GOVERNMENT OR CONGRESS.

Introduction to Founder Zhu Weisha

Graduated from the Department of Automatic Control, Beijing University of Technology. Subsequently, he conducted research at the Institute of Industrial Economics, Chinese Academy of Social Sciences. In 1991, he left his position and founded Yuxing Tech. Yuxing became the first privately-owned high-tech enterprise from Mainland China to be listed on the Hong Kong Growth Enterprise Market in 2000. He sold Yuxing Tech in 2015, and in 2019, he participated in buying Yuxing back. Since then, he has remained a major shareholder and serves as an advisor. He is a legendary figure in China's industrial sector.

Characteristics

Meticulous in his approach, with deep research and practical experience in product design and market operations. He also has research and accumulated knowledge in macroeconomics, monetary theory, capital operations, management theory, and investment theory. He began studying cryptocurrencies in 2017 and got involved in investments. The Chainless System White Paper and the series of articles on the Chainless website are the results of his years of learning, understanding, practical involvement, research outcomes, and product expertise.

The 2021 article "Out of the Misunderstanding of Blockchain" published on the Chainless website represents his summary of blockchain studies. The 2024 article "A New World Needs an Unchanging Financial Ruler" expresses his expectations for the next era. The series of articles "What is the Internet Era" published in the same year reveals that Web3, centered on encryption, is a human revolution that no one can avoid, and this revolution is already taking place in the United States. The series of articles "Problems with Cryptocurrency Regulation" published in 2025, particularly Part IV, points out the impracticalities of the Hong Kong government's principle of "same business, same risks, same rules." The root cause of this problem is that outsiders regulate insiders, leading to a series of policies that are not well received by the market.

The Chainless System showcases Zhu Weisha's highly integrated abilities spanning economics, law, finance, stocks, currency, products, markets, and technology.

Cryptocurrency-Related Achievements

1. Using meticulous analysis through methods of "sweeping coverage" and "deep thinking," he ultimately solved the world puzzle of Satoshi Nakamoto's identity, also demonstrating the effectiveness of his research methods.

2. Using the same research methods, he systematically summarized cryptocurrency theory, restructured the production relations represented by communities in cryptocurrency, wrote over 700,000 words across more than 100 related articles, fully articulated the advanced ideas of Satoshi Nakamoto and cryptocurrencies, and pioneered the proposal of a Web3 chainless financial platform capable of competing with Web2.

3. First proposed the POP (Proof of People) algorithm for token distribution based on headcount. PoW is an algorithm based on time, PoS is based on (stake/equity), and PoP is based on the number of people.

4. Proposed a definition of Web3: Click, Push + Own.

From Double-Entry Accounting to Verifiable Finance

A New Financial Paradigm Combining Institutional Responsibility with Factual Verification

Weisha Zhu - Scott Shields
May 2026

FACTUAL VERIFICATION AND RESPONSIBILITY STRUCTURES FOR THE AGE OF VERIFIABLE FINANCE

Editorial Commentary

This book should not be read as ordinary cryptocurrency commentary, nor as yet another technical manifesto about blockchain. Its deeper ambition is to liberate cryptocurrency from the narrow vocabulary of tokens, chains, and trading cycles, and to place it once again within the long cycle of financial history. The question running through the book is not whether a particular asset will rise or fall, but how human society can move from trusting institutional promises toward verifying financial facts. In other words, this book concerns a deep transformation in the constraint structure of finance: modern finance has long relied on internal institutional constraints, while Verifiable Finance seeks to add externally verifiable constraints on top of that foundation. The first major contribution of this book is its deepening of the concept of the Public Credit Root.

This book emphasizes the distinction between the bitcoin asset and the Bitcoin system. It also emphasizes the distinction between blockchain as a technical component and the Bitcoin system as a whole. The Bitcoin system did not merely create bitcoin as an asset. It also created an external, open, long-running credit root that can be verified globally and in real time. Through mechanisms such as the hash chain, proof of work, open nodes, and continuous verification, the Bitcoin system enables other systems to use it as a final anchoring point.

This concept further releases Bitcoin from the asset narrative of digital gold. Gold is a static asset. The bitcoin asset is a form of digital scarcity. But the Bitcoin system has a deeper institutional function: it can serve as an external proof layer for other financial facts, ledger states, audit records, and responsibility structures. Understanding this point is essential to understanding the entire book. The second major contribution of this book is its insistence that open source is only a means, while verification is the objective.

In the early history of cryptocurrency, open source was necessary because there was no institutional guarantee behind the system. But in the age of AI, AI can help audit code, and it can also help attackers discover vulnerabilities on a large scale. Reliance on open source alone can no longer constitute a complete philosophy of security. Open source is one instrument of transparency; verifiability is the higher-level control objective. Open source, formal verification, operational proofs, responsibility records, audit supervision, and legal acceptance must all be constrained by privacy conditions, business scenarios, and rule design. Different projects have different requirements for privacy, degree of disclosure, and mode of verification.

Open source, public transparency, blockchain, decentralized ledgering, and related mechanisms together form the technical foundation of Verifiable Finance. Their significance does not lie in becoming ends in themselves. Their significance lies in serving verification: enabling key financial facts, key states, permissions, reserves, liabilities, and constraints to be continuously proven, thereby producing objective credit and enabling credit transmission. This book gives special attention to open source because the crypto industry has long suffered from the misunderstanding that open source is security, or that open source is the objective. That misunderstanding must be clarified. Once the existence of a Public Credit Root is recognized, providing final proof for other systems may become one of the most important application directions of the Bitcoin system.

The third major contribution of this book is the proposal of the Transparent Bank and, more broadly, Transparent Finance.

The book does not simply oppose traditional banks, nor does it demand that every commercial process be moved onto public chains. Its argument is more mature: centers will still exist, but centers must become verifiable; commercial systems may preserve partial privacy, but key financial facts must be provable; law, responsibility, privacy, AI auditing, and Public Credit Roots must be combined into a new institutional architecture.

The meaning of the Transparent Bank is not to eliminate banks, but to prevent banks from operating for long periods outside structures of truthfulness. The meaning of Transparent Finance is likewise not to make every financial activity completely public. Rather, while privacy, trade secrets, and legal responsibility continue to exist, Transparent Finance brings key facts into structures that are verifiable, traceable, subject to layered disclosure, and capable of responsibility reconstruction.

These three contributions may be summarized by perceptive researchers. Yet one sentence is repeated throughout the book: gold is a dead object, while the Bitcoin system is a living system. A living system means that it is not a static asset, but an organic system that continues to operate, evolve, and absorb external shocks. Human society itself is composed of living systems, and over thousands of years it has developed institutions to maintain order, reduce uncertainty, handle conflict, and preserve systemic continuity. The Bitcoin system is no exception. The more original part of this book lies in its further discussion of the following question: if the Public Credit Root is the foundation of Verifiable Finance, then the Public Credit Root itself must possess a sufficiently high degree of certainty. For this reason, the mechanisms of Bitcoin's first half, which were mainly based on technical coordination, need to be extended into a more transparent, broader, and more socially and market-acceptable public coordination mechanism.

Under normal conditions, the Bitcoin system can function as a Public Credit Root. But under extreme conditions, it may still face challenges to certainty. Quantum risk, disputes over early addresses, institutional conflicts after financialization, global regulatory pressure, the security model of the AI era, and the responsibility boundaries required before major financial institutions can rely on Bitcoin as a Public Credit Root will all amplify such uncertainty.

Therefore, this book argues that when the Bitcoin system is further understood as a Public Credit Root and begins to face new issues such as financialization, institutionalization, quantum risk, early-address disputes, governance vacuum, and global regulation, technical coordination alone is plainly no longer enough. It needs a broader, more transparent coordination mechanism that can be accepted by the market and the community, in order to strengthen the certainty of the Public Credit Root.

The relevant chapters of this book begin by tracing the intellectual source of Bitcoin and propose that inviting Satoshi Nakamoto to participate in a transparent coordination institution is a reasonable institutional proposal. But this proposal does not mean that Verifiable Finance must depend on Satoshi Nakamoto as an individual. More precisely, Verifiable Finance can continue to advance even if Satoshi never appears. But if Satoshi can participate in second-half coordination through a limited term, without coercive authority, under public procedures, and with UASF as the ultimate backstop, he may become one of the strongest signals and shortest paths for strengthening the certainty of the Public Credit Root. The book also contains a striking judgment: if institutional design can reduce uncertainty around the Public Credit Root, the value of the Bitcoin system may be understood and priced a new.

Based on the above contributions, this book reveals a fundamental turning point in financial history: traditional finance has been built on trust in institutions, while the emergence of the Bitcoin system as a Public Credit Root has made the public verification of facts possible. Finance therefore no longer needs to rely only on the internal self-discipline of institutions. It can further introduce externally verifiable structural constraints. It is within this transition that Verifiable Finance becomes the theoretical ground of a new financial system. What this book attempts to propose is not a plan to replace financial institutions, legal responsibility, or regulatory supervision with technology.

It proposes a new method of financial constraint: key financial facts should not remain dependent for long periods only on institutional statements, periodic audits, or after-the-fact correction. They should gradually enter structures that are verifiable, traceable, subject to layered disclosure, and capable of responsibility reconstruction.

The importance of open networks such as Bitcoin lies in their ability to provide an external Public Credit Root, giving the temporal order and historical integrity of key records stronger external verifiability. But the authenticity of reserves, customer rights, accounting recognition, solvency, and regulatory judgment still require institutions, ledgers, contracts, responsibility, and supervisory mechanisms to work together. Within this boundary, Verifiable Finance does not abolish institutional credit. It pushes institutional credit beyond statements and reputation, so that it can be further grounded in verifiable facts and traceable responsibility.

This book is also a strategic challenge to the United States and to the dollar system. It does not claim that fiat currency will disappear tomorrow, nor does it believe that cryptocurrency can mechanically replace the existing system. Its real proposition is that future financial competition may increasingly depend on who can build verifiable financial infrastructure. Stable coins, the Transparent Dollar, the Bitcoin system as a non-sovereign credit root, Ethereum as a programmable credit root, AI auditing, and Transparent Banks are all components of the competition over the next financial paradigm.

Some proposals in this book are necessarily programmatic. They require implementation, testing, legal design, engineering construction, market adoption, and institutional negotiation. But this is precisely the value of the book. It does not merely describe the existing cryptocurrency industry. It reorganizes the conceptual map of the field. Its most powerful claim is simple but far-reaching: the future of finance will not be defined by making everything decentralized, nor by trusting stronger institutions. It will be defined by making the key facts of financial life verifiable.

AUTHOR'S PREFACE: WHY PROPOSE A RESEARCH FRAMEWORK FOR VERIFIABLE FINANCE

This book was not originally written as a book. It gradually took shape through continuous discussions of cryptocurrency, the Bitcoin system, Transparent Banks, stable coins, the dollar system, and the Satoshi Nakamoto question. Its basic question is simple: if the core of finance is credit, then in an age when AI and cryptocurrency have already appeared, must credit still depend only on institutional promises? My answer is no.

Future finance will certainly still need institutions, law, regulation, and commercial services. But key financial facts must increasingly become verifiable. Whether reserves are real, whether liabilities are clear, whether clearing has been completed, whether permissions have been abused, and whether history has been tampered with - these questions should not remain only in reports, audits, and ex post accountability. They should gradually enter structures of continuous proof, public anchoring, and computable regulation.

This means that the mode of external financial constraint is changing. One mode relies mainly on human judgment, institutional statements, and after-the-fact inspection. Another attempts to embed rules, evidence, and responsibility into verifiable structures. The former is closer to traditional empirical regulation. The latter is closer to the modern rule-of-law spirit of rule-based, evidence-based, and structured governance.

Most discussions in the cryptocurrency industry still remain within asset prices, technical components, and decentralization narratives. They have not fully understood the Bitcoin system as a Public Credit Root, nor have they placed cryptocurrency back within the history of finance and the evolution of credit institutions. This book attempts to fill that theoretical gap.

The Verifiable Finance discussed in this book is not a simple call to put all financial activity on-chain, nor is it a simple opposition to centralized institutions. Its true concern is how, while preserving commercial efficiency, privacy protection, and legal responsibility, centralized financial systems can be subject to machine-verifiable constraints. Transparent Banks, Public Credit Roots, the lowest ledgering cost, verification above open source, verifiable stablecoins, and the Transparent Dollar are different sides of this same problem.

Double-entry bookkeeping constitutes the credit foundation of the modern financial system. It is an internal constraint: people must trust institutions to keep records truthfully, calculate correctly, and obey rules. The appearance of Satoshi Nakamoto made it possible, for the first time, for credit to be publicly verified in an open network. The Bitcoin system thus formed a new credit-root function.

This book summarizes the innovation and development of cryptocurrency and seeks to lift a long technology-centered crypto narrative into a financial narrative, pushing finance from trusting institutions toward verifying facts. It must be emphasized that Verifiable Finance does not replace financial institutions, nor does it replace law, regulation, or accounting systems. Its significance lies in strengthening the evidentiary structure and responsibility structure of financial facts through externally verifiable design, so that institutional credit no longer depends only on statements, reputation, and periodic audits, but can be further grounded in verifiable facts and traceable responsibility.

History has almost unknowingly entered the sixth Kondratieff wave. The previous wave was characterized by semiconductors, computers, and the internet. The internet greatly improved the operational efficiency of finance, but it did not truly shake the credit foundation of modern finance. The underlying feature of the current cycle is Crypto + AI: AI impacts productive forces, while Crypto and Verifiable Finance impact the relations of production represented by modern finance. Verifiable Finance is a new institutional form produced on this foundation. It will not merely improve financial efficiency; it may change financial credit, financial constraints, and financial organization itself.

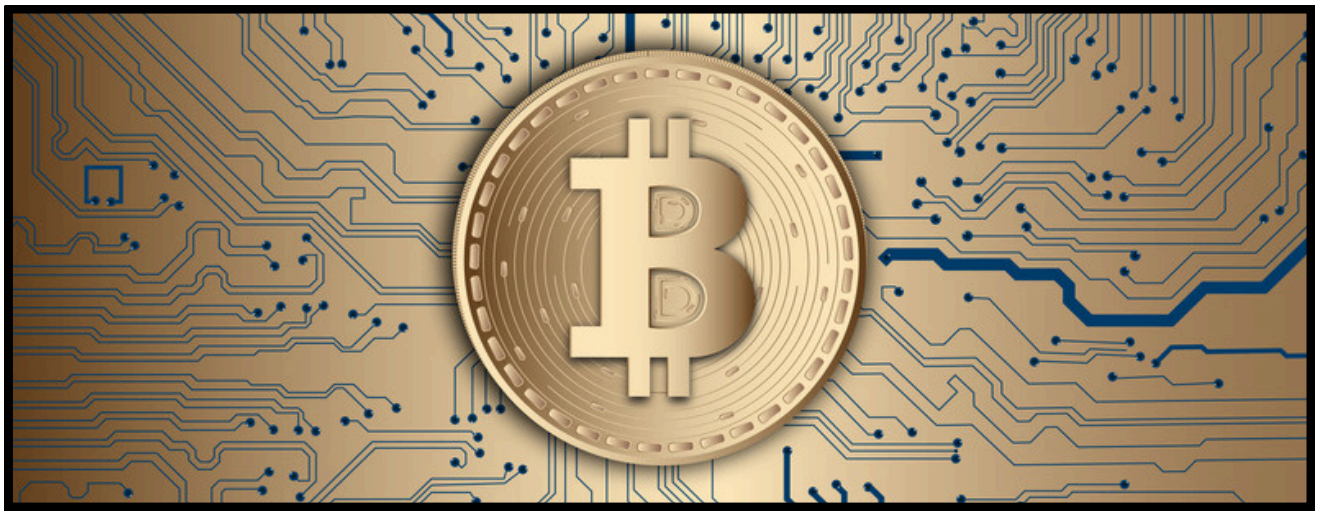
This book is divided into four parts. The general theory clarifies basic concepts; the section on Transparent Banks describes possible forms of future Verifiable Finance; the Satoshi Nakamoto studies explore how the Public Credit Root can be further consolidated; and the final part uses the United States as an example to unfold a basic picture of the strategic development of Verifiable Finance.

The third part, which discusses the Satoshi Nakamoto question, is the most easily misunderstood. The reason is that the crypto industry's long-formed understanding of Satoshi mainly served the ownerless narrative of Bitcoin's first half, but may not be sufficient to explain the new problems that the Bitcoin system faces in its second half as a Public Credit Root. My intention is not to reduce the Satoshi question to identity gossip, nor to claim that Verifiable Finance must depend on any individual. The Bitcoin system has already created a Public Credit Root, and Verifiable Finance can continue to develop even without Satoshi's appearance. But if the Bitcoin system is to move from an asset narrative into a Public Credit Root narrative and be truly accepted by major finance, regulatory systems, and national strategy, then the question of certainty around the Public Credit Root cannot be avoided. Satoshi Nakamoto, as intellectual source, historical source, and institutional source, may be the strongest signal and shortest path for strengthening that certainty, and may also be one of the key catalytic conditions for the implementation of Verifiable Finance.

Mr. Qin Wei, a senior banking expert, designed the verifiable structure of the Transparent Bank and primarily wrote Chapters 6, 7, and 8 of this book. His view that the Transparent Bank is an upgrading, improvement, and revolution of double-entry bookkeeping in banking directly constitutes the intellectual source of this book's title.

This book remains only an initial draft of the Verifiable Finance research framework. Many formulations, ideas, and institutional paths still need to be further verified, revised, and improved in practice. But if this book can help readers liberate cryptocurrency from the narrow mindset of focusing on coin prices and chains, and help them re-understand the significance of cryptocurrency in financial history, then it has completed its first task.

This book is a theoretical monograph with a manifesto-like character. Its emphasis is on raising questions, establishing a framework, and expressing judgments. It therefore does not adopt the strict annotation and citation style of an academic paper. The main ideas in this book have been developed in more than one hundred articles on the Chainless website, chainless.hk. Because the concepts discussed here are relatively new and inevitably controversial, some core arguments are developed from multiple angles and repeated in different contexts. This style may not be concise enough, but for a new theoretical framework that has not yet been widely accepted, necessary repetition is also a form of clarification. It also allows readers who enter the book from different chapters to understand the relevant issues relatively independently.



PART I

THE THEORETICAL STARTING POINT OF VERIFIABLE FINANCE

CHAPTER ONE

THE THEORETICAL GAP IN DIGITAL FINANCE: FROM TECHNICAL VERIFIABILITY TO FINANCIAL CREDIBILITY — CRYPTOCURRENCY AT A HISTORICAL THRESHOLD

I. Cryptocurrency Is Reaching a Historical Threshold

The cryptocurrency industry has already passed through more than a decade. From Bitcoin to Ethereum, from exchanges to stablecoins, from DeFi to NFTs, from public-chain competition to Layer 2, and from Web3 to AI + Crypto, the industry has gone through one narrative after another. But if we look back calmly, a serious question must be raised: What has cryptocurrency actually created that can be commercialized and can carry the future of finance? The answer is not much.

The representative results that have truly reached scale and can continuously enter commercial-financial discussion can be roughly divided into three categories:

First, a small number of public chains with the significance of Public Credit Roots, especially Bitcoin and Ethereum.

Second, centralized exchanges.

Third, centralized stablecoins and their applications.

Strictly speaking, however, the latter two are not victories of cryptocurrency theory itself. Centralized exchanges use crypto assets as trading objects, but their organizational form, credit structure, and business model remain highly centralized. Centralized stablecoins map the credit of the dollar and other fiat currencies onto chains, solving payment and pricing problems in the crypto world, but they do not create a new credit system independent of fiat currency.

The most original capability, and the one most difficult for traditional finance to replace, is the Public Credit Root capability represented by Bitcoin and Ethereum. Unfortunately, the industry has long failed to form a sufficiently systematic theoretical inquiry around this point.

The Bitcoin system created the first ownerless, open, tamper-resistant, verifiable global Public Credit Root. The Ethereum system further demonstrated the possibility of a programmable public verification environment. Before Bitcoin, from traditional computer systems to mobile internet platforms, one ultimately still had to trust a company, a team, an operating system, a database, or a clearing institution. Bitcoin, for the first time, pushed trust in institutions toward verification of rules.

This is the great innovation of cryptocurrency.

But it also reveals the limitations of cryptocurrency: it created a credit root, but did not establish a complete commercial financial system; it created a verifiable ledger, but did not establish Verifiable Finance; it created open-source protocols, but did not systematically solve the problems of commercial security, responsibility, privacy, compliance, and recoverability.

Cryptocurrency is essentially a new branch of finance, yet for a long time it has had only technical theory and has not formed a systematic financial theory. The industry discusses consensus, hashes, signatures, virtual machines, cross-chain systems, zero-knowledge proofs, Layer 2, and TPS in great detail, but it rarely discusses credit, reserves, liabilities, clearing, risk, responsibility, banking forms, and commercialization paths in a systematic way. Fiat currency theory can explain the valuation logic of AI companies, but it cannot fully explain Bitcoin. Gold theory can partially explain Bitcoin's scarcity, but it cannot explain the vitality of Bitcoin as a dynamic network and a Public Credit Root. Gold is a dead object; the Bitcoin system is a living system. When people explain Bitcoin only as digital gold, Satoshi Nakamoto must theoretically disappear or remain forever hidden. This itself is a theoretical predicament that must be reopened.

Today, cryptocurrency has reached a historical threshold.

This threshold is not a technical problem. It is not a TPS problem. It is not a question of whether a certain chain can be a little faster. It is a deeper question:

Cryptocurrency must truly return from the narrative of a technology industry to the essence of the financial industry.

II. Cryptocurrency Is Not a Technology Industry, but a New Branch of Finance

For more than a decade, the cryptocurrency industry has packaged itself as a technology industry.

People discuss consensus algorithms, hash functions, signature algorithms, virtual machines, smart contracts, cross-chain bridges, zero-knowledge proofs, Layer 2, account abstraction, MEV, TPS, gas, and the number of nodes. These are of course important, but they are not the final questions of cryptocurrency.

The real objects that cryptocurrency handles are assets, money, credit, payment, settlement, reserves, liabilities, leverage, liquidity, risk, collateral, custody, exchange, financial intermediation, financial crises, and financial order.

All of these are financial questions.

If an industry handles money and credit but has no financial theory of its own, that industry will inevitably remain in confusion for a long time. This is precisely the problem of the cryptocurrency industry today.

Those who understand technology often do not understand finance. Those who understand finance often do not understand cryptographic technology. Those who understand regulation often do not understand public chains. Those who understand public chains often do not understand commercial finance. Those who understand trading often care only about price and not about institutions. Those who understand code often believe that code can replace responsibility. As a result, the industry has formed a strange situation: a new branch of finance has long lacked a true financial theory.

Traditional fiat finance has a complete theoretical system: central banks, commercial banks, monetary issuance, credit creation, interest rates, debt, fiscal policy, exchange rates, payment and clearing, financial regulation, and the lender of last resort. Although the cryptocurrency industry has created Bitcoin and Ethereum, it has not systematically answered these questions:

What is the credit foundation of crypto finance?
What is the banking form of crypto finance?
What is the risk-control mechanism of crypto finance?
What is the responsibility mechanism of crypto finance?
What is the regulatory boundary of crypto finance?
What is the commercialization path of crypto finance?
What is the security model of crypto finance in the AI era?

Without these answers, cryptocurrency will find it difficult to truly enter the mainstream financial world. If modern financial scholars do not understand cryptocurrency, their knowledge is already incomplete.

Conversely, if cryptocurrency practitioners do not understand financial theory, they cannot truly create the future of finance. This is also an important reason why, more than a decade after the appearance of cryptocurrency, the industry still has not formed a theory of Verifiable Finance based on crypto's underlying capabilities.

The true finance of the future must simultaneously understand fiat currency, banks, credit, blockchain, cryptography, Public Credit Roots, artificial intelligence, verifiable proofs, digital identity, commercial responsibility, and the global financial order. If the characteristics of cryptocurrency are integrated into modern finance, it becomes a new finance.

It may be called Verifiable Finance. To understand it, we must begin with the most important financial characteristics of Bitcoin and Ethereum that have not yet received sufficient attention.

III. The Underappreciated Value of Bitcoin and Ethereum: Public Credit Roots

Bitcoin has many great innovations, but the most important innovation is not decentralization, not blockchain, and not mining itself. The most important innovation of Bitcoin is this: it created a Public Credit Root with no central issuer, no central database, and no central clearing institution, yet one that can be verified globally.

Before Bitcoin, human financial credit mainly came from states, banks, courts, central banks, clearing institutions, and large financial intermediaries. These institutions share one feature: people must trust them. Whether in traditional financial systems, hardware, operating systems, internet platforms, or centralized databases, none of them escapes this logic of trust.

Bitcoin proposed another possibility: one does not have to trust a certain center; one can verify the ledger; one can verify the issuance rules; one can verify the transaction history; one can verify the scarcity of the asset; and one can reach consensus in a global open network. This is a major breakthrough in financial history.

Ethereum further extended this on the basis of Bitcoin, turning the Public Credit Root from a ledgering system into a programmable rule system. The Bitcoin ledger can be publicly verified. The next question is: how can a financial system prove that it is real, safe, compliant, and accountable? Bitcoin and Ethereum provide credit roots, but they themselves are not complete commercial financial systems. A credit root is like a foundation. The foundation is important; only with a foundation can a city be built. We still need tools and materials.

A Public Credit Root provides external proof capability; it does not automatically complete the entire financial proof structure. It requires a bridge connecting the Public Credit Root with modern financial ledgers. Any key fact that can enter a reference chain can, through hashes, indexes, forward and backward references, and anchoring to a Public Credit Root, preserve the consistency between on-chain and off-chain record hashes and remain available for later review. A financial system does not need to expose all facts to a public network. It only needs to bring key facts into the reference chain and proof structure.

Future finance cannot simply be built on the black box of traditional fiat finance, nor can it simply put all business onto public chains. A more reasonable structure is: Public Credit Root + verifiable proof + transparent commercial system + legal responsibility mechanism.

This is the direction of cryptocurrency's second half: not to build chains again and again, but to use verifiable ideas and solutions to raise the trustworthiness of traditional finance, reduce the risks of financial systems, and push technical verifiability further toward provability of financial facts, traceability of responsibility, and institutional acceptance.

IV. Open Source Is Not the Objective; Verification Is the Objective

The cryptocurrency industry has long held a deeply rooted belief: open source means security.

This belief had historical rationality in the early stage. Bitcoin had to be open source, and Ethereum had to be open source, because they had no state credit, no bank endorsement, and no centralized corporate guarantee. They could build trust only through open code, open rules, open ledgers, and open nodes.

But one must see clearly: open source is not the objective; verification is the objective.

Open source exists only to enable verification. If there is a better method of verification, open source is no longer the only answer. Especially after Public Credit Roots such as Bitcoin and Ethereum already exist, commercial systems do not necessarily need to make all code public. What they truly need to disclose and prove are key facts, key states, and key rules. Open source can make code visible, but it cannot guarantee that the code has no vulnerabilities.

Open source can allow audit, but it cannot guarantee that someone has actually audited. Open source can allow white-hat research, but it can also allow hackers to research. Open source can increase transparency, but it may also increase the attack surface. Open source can prove that rules are public, but it cannot prove that deployment, permissions, front ends, dependent libraries, and governance mechanisms are necessarily secure.

Especially in the AI era, the risks of open source will be amplified. AI can automatically read code, search for vulnerabilities in batches, learn historical attack patterns, generate attack scripts, analyze composability risks in smart contracts, and attack wallets, front ends, bridges, governance systems, and user signatures. The security assumption of the past was: the code is open source, and the whole world helps audit it, so it is more secure. The security reality of the AI era may become: the code is open source, the whole world can audit it, and attackers can also use AI to attack it at scale. Therefore, open systems must have a higher-level verification mechanism.

Future financial systems cannot remain at the level of whether something is open source. They must enter the level of whether it is verifiable, how it can be reviewed, and who bears responsibility. The truly important questions are: Can proof of reserves be checked? Are liability boundaries clear? Can clearing results be traced? Are permissions verifiable? Can contract invariants be examined? Can the misappropriation of user assets be discovered? Can over-issuance be identified? Can tampering with key states be reviewed?

This is the core of financial security.
Open source is only a tool. Verification is the objective.

V. The Real Impact of AI on Cryptocurrency: Destroying the Old Security Model and Creating New Financial Infrastructure

When many people discuss the combination of AI and cryptocurrency, they like to talk about AI agents, automated payments, on-chain identity, data markets, model copyrights, and automatic execution of smart contracts. These directions all have value, but they are not the deepest issue. The real impact of AI on cryptocurrency is first of all a security impact. AI will make attackers stronger. In the past, attacking a complex protocol required advanced hackers to spend a great amount of time studying code, deploying environments, constructing vulnerabilities, writing scripts, and simulating transactions.

In the future, AI can lower this threshold: it can help attackers understand code, search for boundary conditions, discover permission vulnerabilities, generate phishing pages, induce users to sign, attack DAO governance, and rapidly replicate historical attack patterns.

This means that AI will challenge the old logic that open source equals security. But on the other hand, AI will also make complex systems that were previously difficult to implement possible. A new financial infrastructure is not a simple wallet, nor is it an ordinary public chain. It must simultaneously handle accounts, assets, liabilities, reserves, clearing, risk control, compliance, privacy, audit, permissions, proofs, on-chain anchoring, off-chain business, user experience, regulatory interfaces, and security monitoring.

In the past, building such a complex system through traditional human labor involved extremely high development costs, long cycles, and great risks. But after the emergence of AI, system construction costs may decline significantly: code generation efficiency improves, test automation improves, audit capability improves, the threshold for formal verification declines, risk monitoring becomes automated, compliance review becomes automated, documentation and architecture design become more efficient, and the capacity to simulate complex systems is strengthened.

Therefore, AI is both a threat and an opportunity for cryptocurrency.

It threatens the old open-source security model, and it also pushes new verifiable financial systems into the realm of possibility. The projects that will succeed in the future will not be those that simply shout AI + Crypto, but those that can truly answer this question: in the AI era, how can financial systems be continuously verified, continuously audited, continuously protected, and continuously proven?

VI. Why Current Cryptocurrency Has Difficulty Achieving Real Commercialization

The cryptocurrency industry has already produced many innovations, but very few projects have achieved real commercialization. The reason is not the absence of technology, but the absence of the complete conditions required by commercial finance.

Commercial finance needs security, stability, privacy, compliance, responsibility, accountability, recoverability, risk isolation, certainty of clearing, legal protection, customer trust, and regulatory interfaces.

Current crypto systems have obvious deficiencies: smart contract vulnerabilities occur frequently; cross-chain bridges carry enormous risks; lost wallet private keys cannot be remedied; user signature risks are difficult to identify; project upgrade permissions are not transparent; governance mechanisms are easily manipulated; after an attack, the responsible party is unclear; on-chain transparency harms commercial privacy; multiprotocol composability amplifies systemic risk; and ordinary users cannot truly verify complex protocols.

Such systems can serve as experiments, speculation, technical toys, and early innovation spaces, but they can hardly become mainstream commercial financial infrastructure directly. Real finance does not only need immutability; it must also answer what happens after an error. Real finance does not only need automatic execution by code; it must also answer who bears responsibility. Real finance does not only need public transparency; it also needs protection of privacy and commercial secrets. Real finance does not only need decentralization; it also needs efficiency, compliance, service, risk control, recoverability, and legal acceptance.

Therefore, future finance cannot simply be built on the current DeFi model. Cryptocurrency must move from open systems without responsibility toward responsible and verifiable systems.

VII. Transparent Banks: A Possible Form for the Real Commercialization of Cryptocurrency

Future finance will not simply return to the black box of traditional banks, nor will it fully move toward anarchic DeFi. The Transparent Bank is an important example. It will be discussed in detail in Part II. A Transparent Bank is not merely a traditional bank put on-chain, nor is it DeFi under another name. It is a new form of financial infrastructure. Its basic principles are: business may remain private, but key facts must be verifiable; centers may exist, but centers must be constrained; customer privacy must be protected, but reserves and clearing must be proven; commercial systems may not need to be fully open source, but key states must be verifiable; all rules should be made as ex ante as possible; financial institutions should operate systems under rule-based constraints; and verification should be rigid, not dependent on moral self-discipline.

The structure of a Transparent Bank can be summarized as: private business system + controlled chain or Chainless System + Public Credit Root + verifiable proof + legal responsibility system + AI security system. The private business system is responsible for customer service, account management, risk control, compliance, privacy protection, and commercial operation. The controlled chain or Chainless System is responsible for internal ledgering, state management, clearing coordination, and asset movement.

The Public Credit Root is responsible for final anchoring, fixing key states, proofs, timestamps, reserve summaries, and clearing results into a globally verifiable network. Verifiable proofs are responsible for proving to users, regulators, counterparties, and the market that the system has not over-issued, misappropriated assets, concealed liabilities, or tampered with key states.

The legal responsibility system is responsible for handling real-world fraud, disputes, compensation, regulation, and accountability. The AI security system is responsible for continuous monitoring, anomaly detection, automatic auditing, risk warning, code inspection, user protection, and compliance assistance.

This is the meaning of the Transparent Bank: it does not eliminate banks, but transforms banks; it does not eliminate centers, but constrains centers; it is not absolute openness, but verifiability of key facts; it is neither traditional finance nor pure crypto finance, but a new form after both.

VIII. The Structure of the Future Financial Ecology

The future financial ecology will not have only one form. It will most likely be a multi-layer structure. The first layer is the Public Credit Root. Bitcoin, Ethereum, and a small number of truly secure, decentralized, long-term verifiable public chains will become global credit anchors. The second layer is the institutional financial network. Banks, investment banks, stablecoin companies, payment companies, and asset management institutions will build their own controlled chains, consortium chains, Chainless Systems, or dedicated networks. The third layer is the Transparent Bank. It combines commercial financial systems, user accounts, assets and liabilities, clearing, reserves, risk control, and verification mechanisms, and provides verifiable financial services to the outside world.

The fourth layer is the AI audit and security layer. AI will continuously inspect code, monitor risk, discover anomalies, assist compliance, protect users, generate proofs, simulate attacks, and prevent systemic risks. The fifth layer is the legal and regulatory layer. It is responsible for real-world identity, responsibility, remedy, compensation, disputes, and public order. The sixth layer is the user application layer. Ordinary users will not directly understand the complex underlying systems. They only need financial services that are safe, convenient, low-cost, verifiable, recoverable, and privacy-protecting. Among these, the fourth to sixth layers are not necessarily vertical superior-subordinate layers. They are more like parallel modules operating around the first three layers: AI provides continuous verification capability, law provides real-world responsibility boundaries, and user applications provide usable entrances. This is the truly possible form of future finance. Not everything will be on public chains. Not everything will be controlled by bank black boxes. Not all code must be open. Not all centers must be eliminated. Rather: the core credit anchor is public; key facts are verifiable; commercial systems can operate; user privacy is protected; central power is constrained; and AI continuously provides security and audit capability.

IX. The Six Transformations the Cryptocurrency Industry Must Complete

If cryptocurrency is to enter its second half, it must complete six transformations. First, from technical narrative to financial theory. Cryptocurrency cannot speak only about technology. It must answer questions of money, credit, reserves, liabilities, clearing, risk, and responsibility. Second, from open-source belief to verification priority. Open source remains important, but it is no longer the endpoint. The future core is that key facts must be verifiable. Third, from the superstition of decentralization to verifiable centers. Centers may not disappear. What must disappear are black-box centers that cannot be verified, audited, or held accountable. Fourth, from the fantasy of pure public chains to a multi-layer financial ecology. Public chains should not carry all commercial business. Public chains are better suited to serving as Public Credit Roots and final proof layers. Fifth, from code is law to the combination of code, law, and responsibility. Code can execute rules, but it cannot replace responsibility in the real world. Commercial finance must have remedies, accountability, and recovery mechanisms.

X. Conclusion: From Trusting Institutions to Verifying Facts

Human financial history has long been built upon trusting institutions. Trusting states, central banks, commercial banks, exchanges, audit firms, custodians, rating agencies, and regulatory systems. But history has proven again and again that institutions make mistakes, deceive, abuse power, and fail under systemic pressure. Bitcoin told humanity for the first time: one does not necessarily have to trust institutions; one can also verify rules. But Bitcoin is not enough, and Ethereum is not enough either. Because real finance is not only a ledger. Real finance has assets, liabilities, customers, privacy, law, responsibility, risk, commercial secrets, regulation, errors, fraud, and remedy. Therefore, future finance cannot remain in the stage of pure cryptocurrency. It must enter the stage of Verifiable Finance. The core of this stage is not issuing more tokens, not creating more public chains, not creating more exchanges, not decentralizing everything, and not making all code public. Its core is to make key financial facts verifiable, and to move further from technical verifiability toward the provability of financial facts, the traceability of responsibility, and institutional acceptance. To accomplish this, hashes, signatures, on-chain records, and open-source code alone are not enough. For a financial system to form a reviewable proof structure, it must complete at least six layers of verification. The first layer is verification of record existence and integrity. It addresses whether a record existed at a particular time and whether it was modified after the event. The second layer is identity and authorization verification. It addresses who initiated, who signed, who approved, and whether permissions matched the action. The third layer is transaction and delivery verification. It addresses what kind of transaction occurred, whether funds or assets were delivered, and whether execution states were consistent.

The fourth layer is accounting and disclosure verification. It addresses whether financial results were correctly recorded and whether they are consistent with what is shown to customers and disclosed externally. The fifth layer is legal and rights verification. It addresses whether ownership, redemption rights, bankruptcy remoteness, priority of responsibility, and settlement finality are established. The sixth layer is risk, supervision, and institutional acceptance. It addresses the evidentiary basis for reserve quality, liquidity, concentrated redemption, capital impact, audit conclusions, and regulatory judgment. Together, these six layers of verification show that Verifiable Finance is not merely putting data on-chain, nor merely proving the existence of a hash value. It requires on-chain and off-chain systems, technical proofs and legal responsibility, accounting records and regulatory materials to form one traceable structure. All verification can use reference chains and the Chainless platform to achieve consistency between on-chain and off-chain hash commitments, thereby proving that the ledger has not been modified without leaving a trace.

Through this layered structure, proof of reserves, liability mapping, clearing results, permission operations, risk states, solvency, and system states can all obtain, to varying degrees, more continuous, more reviewable, and more accountability-oriented evidentiary support. Bitcoin opened this door. Ethereum expanded this door. AI makes new system capabilities possible.

The Transparent Bank, as the practice of Verifiable Finance, may be the true new world beyond this door. This is the true future of cryptocurrency. It is not a repetition of traditional finance, nor a continuation of speculative crypto markets, but a historical turn in human finance from trusting institutions to verifying facts. Humanity is now approaching this new historical threshold.

Chapter Two
Public Credit Root: The Truly Irreplaceable Product of the Bitcoin System

— Why Digital Gold Severely Undervalues Bitcoin

This chapter begins by clarifying several fundamental concepts. The cryptocurrency industry has long built its technical framework around concepts such as blockchain, decentralization, open source, and mining; however, these terms are frequently conflated and even regarded as encompassing the entire value of the Bitcoin system. Only by first understanding the concepts of Bitcoin assets, the Bitcoin system, blockchain, decentralization, and the public credit root can one truly grasp why the Bitcoin system is irreplaceable.

I. We Must First Distinguish "Bitcoin" from the "Bitcoin System"

Discussing Bitcoin requires first distinguishing between two concepts: One is bitcoin.The other is the Bitcoin system. "Bitcoin" refers to the token asset; the "Bitcoin system" refers to the whole that includes the network, miners, nodes, rules, ledger, incentives, and social consensus. These two concepts have long been mixed together, causing theoretical confusion throughout the industry. Bitcoin is the digital asset issued and maintained by this system. The Bitcoin system, by contrast, is a monetary issuance and ledgering system composed of cryptography, proof of work, the node network, miner competition, difficulty adjustment, transaction rules, timestamps, open verification, and social consensus. Bitcoin is a financial application. The Bitcoin system is a technology-finance composite system. It embodies value as both productive force and production relation.

Bitcoin as an asset answers the question: can a non-sovereign digital asset exist? The Bitcoin system as a machine institution answers a different question: in the absence of a central institution, how can a global ledger issue, record, verify, order, settle, and maintain credit over the long term? These are questions at two different levels. If one looks only at bitcoin, it is easy to understand it as a digital commodity, digital gold, a speculative asset, or a store of value. But only by looking at the Bitcoin system can one understand why it changed financial history. The title of the Bitcoin white paper is "A Peer-to-Peer Electronic Cash System." The core problem Satoshi Nakamoto raised in the white paper was how to solve the double-spending problem of electronic cash without relying on a trusted third party, and how to form tamper-resistant transaction records through a peer-to-peer network, proof of work, and a hash chain.

This means that the product of the Bitcoin system is not merely the bitcoin coin. It is a monetary issuance, ledgering, and verification system that does not depend on traditional financial institutions. Bitcoin as an asset is the visible product of the system. The Public Credit Root is the hidden product of the system. The former is easier for the trading market to price. The latter is more difficult to understand, but it is more important.

II. The Components of the Bitcoin System Cannot Represent the Bitcoin System or Bitcoin

One of the greatest misunderstandings in the cryptocurrency industry is the attempt to define Bitcoin and the Bitcoin system by the components of the Bitcoin system. As parts of the Bitcoin system: Blockchain is a component; decentralization is a component; proof of work is a component; the node network is a component; the mining mechanism is a component; difficulty adjustment is a component; open-source code is also a component. All of these components are important, but they are not the final product. Blockchain, in relation to the Bitcoin system, is like a pickaxe in relation to gold. It is important, but it is not value itself. Decentralization, in relation to the Bitcoin system, is like the distribution of gold mines. It affects security and supply, but it is not financial value itself. Proof of work, in relation to the Bitcoin system, is like the cost of gold extraction. It helps form scarcity and a security boundary, but it is not the final institutional product.

The real product is the overall capability formed after these components are combined. The overall capability of the Bitcoin system is not merely that "there is a chain." It is not merely that "there is a group of nodes." It is not merely that "miners mine." It is not merely that "the code is open source." It is not merely that "there is no center." These are all mechanisms. From the standpoint of bitcoin as an asset: Just as the value of gold comes from gold itself, not from the picks, shovels, mining machines, smelting furnaces, or transportation tools used to mine gold. No one would define the gold financial system by "gold-mining tools." In the same way, blockchain, decentralization, and mining cannot be used to define the financial meaning of Bitcoin. The capacity of the Bitcoin system to produce its final products is reflected in two results: the bitcoin asset and the Public Credit Root. The former is a financial asset. The latter is institutional infrastructure.

III. Blockchain Is Only a Technological Improvement, Not the Financial Revolution Itself

Blockchain certainly has value. It arranges data in chronological order; connects history through hash structures; gives ledgers traceability; makes historical tampering more difficult; and allows multiple parties to share the same record. But one must be clear: Blockchain is only a technological improvement, not the financial revolution itself. From the simplest perspective, a blockchain is a continuously appended daybook, ordered by time and connected by hash stamps. This daybook can record transactions, states, proofs, and other data. But a daybook by itself does not automatically generate credit. Without a sufficiently secure consensus mechanism, it can be tampered with. Without sufficiently strong economic incentives, no one will maintain it. Without a sufficiently open verification network, it may be controlled. Without the test of long-term history, it has no depth of credit. Without real assets and real users, it is merely a technical structure. Blockchain solves a ledger technology problem. The Public Credit Root solves an institutional trust problem. These are completely different levels. Blockchain asks: how should records be kept? The Public Credit Root asks: why should they be trusted? Blockchain asks: how should data be arranged? The Public Credit Root asks: can human beings and machines jointly verify a set of rules? Blockchain asks: can a ledger resist tampering? The Public Credit Root asks: can a system without the endorsement of a central institution become a credit anchor for global finance? This is the difference between technological improvement and institutional innovation. Blockchain belongs to the technological domain. The Public Credit Root belongs to the institutional domain. Blockchain can be replaced. Databases can be improved. Hash structures can change. Consensus mechanisms can evolve. Ledgering methods can be upgraded. But once a Public Credit Root is formed, it cannot be replaced by an ordinary technical tool. Because credit is not written by code. Credit is deposited through long-term operation, real value, open verification, social consensus, and historical testing.

IV. Decentralization Is Also Not the Product, but the Means

Decentralization is an important component of the Bitcoin system, but it is also not the final product. The value of decentralization lies in reducing single-point control, single-point corruption, and single-point failure, while increasing censorship resistance and long-term survivability. But decentralization itself is not the purpose. Decentralization serves a higher objective: to make key rules publicly verifiable and to prevent credit from depending on a single center. If a system claims to be decentralized, but users cannot verify whether assets are real, whether liabilities are complete, whether permissions have been abused, or whether rules have been manipulated, then such decentralization has no financial meaning. Conversely, if a system is not completely decentralized, but its key facts can be verified, responsibility can be traced, risks can be isolated, rules can be audited, and states can be anchored to a Public Credit Root, then it may be more suitable for commercial finance. The market's acceptance of systems with centralized governance features hinges not on their absolute decentralization, but on the verifiability of their core ledger, rules, and state. This is the logic of the Transparent Bank. Commercial finance cannot exist without centers. Banks are centers. Exchanges are centers. Custodians are centers. Payment institutions are centers. Regulators are also centers. The question is not whether centers exist. The question is whether centers can lie. The goal of future finance is not to eliminate all centers, but to make centers verifiable, constrained, audited, and accountable. Therefore, decentralization is a means, not an endpoint. What is truly irreplaceable is not the form of decentralization, but the verifiable credit ultimately produced by decentralization. Centralization can be replaced. Decentralization can also be replaced. Blockchain can be replaced. But once a Public Credit Root is formed, it is very difficult to replace.

V. The Two Products of the Bitcoin System: Bitcoin and the Public Credit Root

The Bitcoin system has two products. The first product is bitcoin; the second product is the Public Credit Root. Bitcoin is a non-sovereign digital asset: a globally transferable, holdable asset with verifiable scarcity. The Public Credit Root is globally verifiable credit infrastructure, and marks the beginning of humanity’s movement from trusting institutions toward verifying rules. Bitcoin as an asset solves the problem of value storage and transfer. The Public Credit Root as infrastructure solves the problem of where final credit comes from. The former is a financial asset; the latter is a credit method. This distinction is extremely important. If one sees only bitcoin as an asset, one will interpret it as digital gold. If one sees the Public Credit Root, one will discover that the Bitcoin system far exceeds digital gold. Bitcoin is the surface-level financial product of the Bitcoin system. The Public Credit Root is the deeper institutional product of the Bitcoin system. Bitcoin can rise and fall in price; this is an asset property. The Public Credit Root represents a new credit structure; this is an institutional property. Bitcoin can become part of an asset portfolio. The Public Credit Root can become a foundational anchor for future finance, AI, Transparent Banks, and the machine economy. This is where the Bitcoin system is truly underestimated. The market has seen bitcoin, but the most important thing has instead been overlooked: the Bitcoin system created the first truly globalized, open, machine-based, verifiable Public Credit Root in human history. It has already operated for more than a decade without the guarantee of traditional financial institutions.

VI. What Is a Public Credit Root?

A Public Credit Root refers to a foundational credit structure that can be openly verified globally, runs over the long term, is difficult to tamper with, does not depend on a single institution, and can serve as the final anchor for other financial systems. In traditional society, credit roots mainly come from people

and institutions. A central bank is a kind of credit root; a commercial bank is a kind of credit root; a large internet platform is also a kind of credit root. These credit roots share one common feature: people must ultimately trust a certain center as the root of credit. They trust that the central bank will not overissue money, that the bank has not misappropriated assets, and that the platform has not altered data. The Bitcoin system proposed another possibility. Not trusting a person, not trusting a company, not trusting a government, and not trusting a database administrator, but verifying a set of public rules. This is the historical transformation from trusting people to verifying rules. It may also be described as a transformation from institutional credit to machine credit. But machine credit here does not mean blindly trusting machines. Machines themselves may make errors, may be attacked, and also require rule constraints. What truly matters is that, through cryptography, open networks, competitive mechanisms, economic incentives, the accumulation of time, and public verification, credit is built upon verifiable rules. The essence of the Public Credit Root is not machine worship. Its essence is to move part of the key records, key states, and key proofs from institutional promises that are difficult to verify toward a more verifiable rule system and external proof structure. This is the true institutional innovation of the Bitcoin system.

VII. Gold Does Not Have the Function of a Digital Public Credit Root

Many people explain Bitcoin as digital gold. This metaphor has some meaning, because both bitcoin and gold possess scarcity, both can serve as stores of value, and neither depends on a single issuing institution. But digital gold can explain only one part of bitcoin. It cannot explain the whole Bitcoin system. Gold is a dead object. The Bitcoin system is a living system. Gold has value, but gold does not have the function of a digital Public Credit Root. Gold cannot automatically keep accounts, cannot verify the order of digital transactions, cannot provide hash anchoring and an external proof layer for Transparent Banks, and cannot serve as a computable and reviewable final verification layer in a machine economy. The credit of gold comes from scarcity and historical consensus. The credit of the Bitcoin system comes from the superposition of scarce assets, an open ledger, long-term operation, cryptographic proof, node verification, social consensus, and the Public Credit Root. Therefore, using only the gold framework to understand Bitcoin is like describing an automobile only by its carrying function: it sees the store-of-value attribute, but not the essential transformation in systemic verification capability. It seriously underestimates the Bitcoin system. Gold is an important credit asset of the human era. The Bitcoin system possesses the function of a Public Credit Root for the machine era. Gold suits the store-of-value logic of human society; the Bitcoin system better suits the verification logic of the AI era. Future AI systems, automated trading systems, Transparent Banks, machine audits, smart contracts, cross-institutional clearing, digital identity, and automated finance all require an external, open, long-running, difficult-to-tamper-with proof anchor that can be jointly verified by machines and human beings. Gold does not have this function; traditional bank databases do not have this function; centralized cloud platforms do not have this function; and ordinary blockchain projects do not naturally possess this function. The Bitcoin system has this function. The Ethereum system extends this function to the level of programmable rules. Therefore, the value of gold cannot be simply compared with the value of the Bitcoin system. Gold has only an asset property; the Bitcoin system has both an asset property and an institutional property. From a functional perspective, gold can only perform the function of a store-of-value asset; the Bitcoin system not only produces a store-of-value asset, but also provides a Public Credit Root. Therefore, the value of Bitcoin should not be estimated only within the framework of gold. On the day when Bitcoin's market capitalization surpasses that of gold, it will be the credit-root function at work.

VIII. In the AI Era, Machine Systems Must Rely on Credit Roots

After the arrival of the AI era, the importance of Public Credit Roots will rise further. One of the core questions of the AI era is not whether machines can compute, but how verifiable trust can be established among machines, between machines and human beings, and between AI agents and financial systems. AI can generate content, but who proves the source of that content? AI can execute transactions, but who proves the authorization of those transactions? AI can manage assets, but who proves that those assets have not been misappropriated? AI can audit reports, but who proves that the state of those reports has not been tampered with? AI can conduct automatic clearing, but who proves that the clearing result is trustworthy? AI can make decisions on behalf of human beings, but who proves that it has not exceeded its authority? These questions cannot be solved by gold, by ordinary databases, or by promises from centralized platforms. All these questions require an external, open, tamper-resistant final verification layer. They require a Public Credit Root. The stronger the AI era becomes, the more it will need a final verification layer; the more machines there are, the more they will need a credit anchor commonly recognized among machines; the more complex automated finance becomes, the more it will need unfalsifiable state proofs; the more mature Transparent Banks become, the more they will need external verifiable credit roots. Without Public Credit Roots, AI financial systems may become more efficient black boxes. With Public Credit Roots, AI can serve transparency, verification, audit, and responsibility. This is why Public Credit Roots connect the underlying logic of machine trust and AI finance. The Public Credit Root is the institutional foundation of the machine trust era. It is also in this sense that the underlying logic of the sixth Kondratieff wave can be understood as Crypto + AI. AI provides new productive forces; Crypto provides new credit roots and verification structures. The two are indispensable to each other.

IX. Why the Public Credit Root Is Irreplaceable

The Public Credit Root is irreplaceable for at least four reasons.

First, it requires long-term history. Credit is not written into existence, not created by publicity, and not designed into existence by technology alone. Credit requires time. The Bitcoin system has operated for more than a decade. It has experienced market crashes, regulatory shocks, competition in hash power, community splits, technical disputes, exchange collapses, state crackdowns, miner migration, capital cycles, and global attacks, yet its core rules have survived. This history itself is part of its credit. A new system can copy Bitcoin's code, but it cannot copy Bitcoin's history; it can copy the block structure, but it cannot copy more than a decade of global verification; it can copy proof of work, but it cannot copy the depth of credit formed by the market over the long term.

Second, it requires the largest scale of social consensus. A Public Credit Root is not a purely technical system, but the result of combining a technical system with social consensus. Why does the same copied code fail to produce the same credit? Because credit does not reside in the code itself; it resides in the consensus jointly formed by global users, miners, nodes, developers, capital, regulators, media, institutions, and history.

Third, it requires real value accumulation. A system without real value accumulation cannot become a credit root. A Public Credit Root must carry real assets, real risks, real transactions, real disputes, and real attacks.

Fourth, it requires extreme simplicity and stability. A credit root cannot change frequently. A system that frequently changes rules, changes narratives, upgrades its core logic, and depends on a founding team to operate is unlikely to become a Public Credit Root. Bitcoin is strong not merely because its technology is advanced, but because its core rules are extremely simple and extremely stable. In finance, stability itself is value. The reason a Transparent Bank chooses Bitcoin as a credit anchor is precisely its extreme simplicity and stability, not its technological complexity.

X. Conclusion: The Credit Root Is the Bitcoin System's Most Undervalued Product

The product of the Bitcoin system is not only bitcoin. Bitcoin as an asset is of course important, but the Bitcoin system as a Public Credit Root may be even more important. Bitcoin gave humanity a non-sovereign digital asset. The Public Credit Root gave humanity, for the first time, a globally verifiable financial anchor. Blockchain is only a component, decentralization is only a means, open source is only a method, and tokens are only a manifestation. The reason the cryptocurrency industry has long failed to establish a mature financial theory is precisely that it has mistaken components for products, means for ends, and blockchain for the revolution itself.

The real revolution is not the technical component called blockchain. The real revolution is the emergence of the Public Credit Root and the externally verifiable constraint that it produces. It means that human finance begins to move from mainly trusting people toward more verification of rules; from mainly trusting institutions toward more verification of facts; from centralized credit toward Public Credit Roots; and from merely relying on institutional credit toward a combination of institutional responsibility and machine-verifiable evidentiary structures. The first half of the Bitcoin system allowed the world to see bitcoin. The second half of the Bitcoin system should allow the world to understand the credit root. The credit-root value of the Bitcoin system will ultimately be reflected in the long-term value of the bitcoin asset. This is precisely the understanding that the second half of the cryptocurrency industry most needs to grasp and most needs to communicate.

It must be pointed out that cryptocurrency systems have a boundary of credibility: matters that enter on-chain records and on-chain rules can be publicly verified; off-chain facts that have not entered on-chain records cannot be verified by blockchain itself alone. The core of Verifiable Finance is to bring off-chain assets, off-chain ledgers, and off-chain responsibility into verifiable structures through mechanisms such as hash commitments, reference chains, audit proofs, and anchoring to Public Credit Roots.

Verifiable Finance also has boundaries. It mainly solves the questions of whether history has been tampered with, whether proof exists, and whether temporal order is trustworthy. It does not directly solve the questions of whether input data are true, whether audits are effective, or whether courts will accept the evidence. The latter must be jointly completed by Transparent Bank rules, audit systems, accounting systems, and legal responsibility systems.

Chapter Three
Reducing the Ledgering Cost of Public Chains: Reconstructing the Financial Ledgering System with the Public Credit Root

I. What the Financial System Truly Needs Is Not Repeated Chain-Building, but Low-Cost Trusted Ledgering

What is the core of finance? Many people would say assets, credit, payment, clearing, trading, and risk control. All of these are correct. But if we ask one level deeper, the most basic action of the financial system can be reduced to two words: keeping accounts. Where assets come from, where they go, who owns what, who owes whom, when something occurred, whether it has been completed, whether it has been cleared, and whether it can be redeemed - all of these ultimately fall back onto the ledger. The trustworthiness of a financial system is, in essence, inseparable from the trustworthiness of its ledger. In the past, the answer offered by the cryptocurrency industry was this: since the ledgers of traditional finance are black boxes, put the ledger onto a public chain and let everyone keep accounts and verify them together. The industry therefore formed a default logic: to be trusted, one must build a chain; to build a chain, one must establish one's own consensus; to have consensus, one must issue tokens; and to issue tokens, one must maintain validators, miners, nodes, incentives, governance, and a security budget.

The result is that the entire industry keeps building chains again and again, repeatedly constructing consensus systems and repeatedly paying high ledgering costs, while failing to answer the question that commercial finance cares about most: is there a way to complete daily ledgering at a relatively low cost while still obtaining a sufficiently high level of final tamper-resistant proof?

After the long-term stable operation of the Bitcoin and Ethereum systems, the Public Credit Root has already emerged. They provide finance with external, open, long-term, difficult-to-tamper final credit anchors. Financial systems no longer have to choose only between “traditional bank black-box ledgering” and “putting all business onto public chains.” Commercial finance needs to ask a more basic question again: do I actually need a chain, or do I only need tamper-resistant proof of the ledger? If the purpose is only to prove that the history of a ledger has not been modified without leaving a trace, the most economical method may not be to build a complete chain, but to keep accounts internally, make hash commitments, and anchor them to a Public Credit Root. For a large number of financial ledgering scenarios, the better solution may not be “one chain for every institution,” but “one ledger for every institution, with key states anchored to a Public Credit Root.”

This is not a return to the traditional black box, nor is it the placement of all daily business onto expensive public chains. Rather, it is to maintain the low ledgering cost of centralized systems while making key facts continuously verifiable. The Public Credit Root is precisely the core of this structure. Of course, the extent to which this structure can reduce ledgering costs also depends on anchoring granularity, anchoring frequency, exception handling, privacy protection, and regulatory acceptance. Internal bank ledgering does not require every entry to be confirmed by a global network. Corporate internal accounting does not require every line of the journal to go onto a public chain. The daily transactions of payment institutions do not need to be exposed to global nodes. The most common misunderstanding when traditional financial institutions build their own chains is to misuse the construction method of a Public Credit Root in ordinary commercial ledgering scenarios. Public chains are suitable as final credit anchors, but they are not suitable for carrying all daily ledgering. The value of Bitcoin and Ethereum lies precisely in the fact that they can become credit roots for other systems, rather than requiring every system to become Bitcoin or Ethereum again.

II. The Advantages and Defects of Traditional Banks: Low Cost, but Black Box

The daily ledgering cost of traditional banks is actually not high. They do not need to pay global consensus costs for every internal ledger entry. From the perspective of pure ledgering, centralized systems are extremely efficient. This is precisely why traditional banks have existed for so long: they keep accounts quickly, clear efficiently, protect privacy, handle complex business, conduct credit and risk control, and can also correct mistakes and compensate losses when errors occur. But the problem with traditional banks is that their ledgers are black boxes to the outside world. Users can only trust reports; regulators can only rely on filings and spot checks; audits can only be conducted periodically; the public finds it difficult to continuously verify reserves; the clearing process is not necessarily transparent; and risk accumulation is often exposed only when a crisis breaks out. The advantage of traditional banks is low-cost ledgering; their defect is low verifiability. The advantage of public chains is high verifiability; their defect is high ledgering cost. The key to future finance is not simply choosing one side, but keeping accounts at low cost like banks while using the Public Credit Root for low-cost verification.

III. Single-Party Ledgering Is Not the Problem; Unverifiability Is the Problem

The cryptocurrency industry has long been wary of "single-party ledgering," because traditional finance is precisely a system in which centralized institutions keep accounts themselves, interpret those accounts themselves, and are difficult to verify continuously from the outside. But we must distinguish single-party ledgering from unverifiable single-party ledgering. Single-party ledgering itself is not the problem. The real questions are: can the ledger be modified afterward without leaving a trace? Can reserves, liabilities, clearing results, permission operations, and historical states be verified? Can key facts be anchored to an external credit root? If the answer is no, then single-party ledgering is a black box. If the answer is yes, then single-party ledgering can become an efficient, low-cost, verifiable financial infrastructure. The Public Credit Root makes a third structure possible: institutions can continue to keep accounts efficiently, and systems can continue to protect trade secrets and customer privacy, but key ledger states must periodically generate proofs and be anchored to the Public Credit Root. Once a dispute occurs, the outside world can verify whether history has been tampered with. This turns single-party ledgering from "black-box ledgering" into "verifiable ledgering." The key question of future finance is not "who keeps the accounts," but who can prove that the accounts have not been changed; it is not "whether ledgering is single-party," but whether single-party ledgering can be constrained by a Public Credit Root.

IV. Hashing Ledger Pages Onto the Chain: The Lowest-Cost Model of Trusted Ledgering

One realistic way to balance low cost and high trust is to hash ledger pages onto the chain. The basic logic is simple: financial institutions continue to maintain internal ledgers; they form ledger pages by time or by batch; each page generates a hash value; and those hash values are periodically anchored to a Public Credit Root such as Bitcoin. The anchoring frequency is not fixed; it should be determined jointly by business risk, cost tolerance, regulatory requirements, and verification needs. When verification is needed, the original ledger page can be produced and its hash recalculated, then compared against the commitment on the Public Credit Root, thereby proving whether the ledger page has been tampered with. This does not require all data to go on-chain. It only requires key ledger states to leave an undeniable external commitment. It is like adding an external timestamp to the ledger and periodically submitting the historical fingerprint to the Public Credit Root. The ledger is still maintained by the institution, but the institution cannot modify the ledger afterward without leaving a trace. At the same time, hashing ledger pages onto the chain does not mean that accounting records can never be corrected. Real finance inevitably involves error correction, reversing entries, cancellation, reclassification, and exception handling. What Verifiable Finance seeks to do is not to prohibit corrections, but to make the correction process itself leave continuous evidence: the original state, reason for modification, authorizing party, scope of impact, and new state commitment should all be traceable and replayable. This is precisely low-cost internal ledgering plus high-trust public anchoring. How to systematize, productize, and regulate this structure is an important financial innovation of the Transparent Bank.

V. The Public Credit Root Separates Daily Ledgering from Final Proof

One of the greatest engineering meanings of the Public Credit Root is that it separates two kinds of costs: the cost of daily ledgering and the cost of final credit proof. In the past, these two costs were often mixed together: traditional banks lowered daily ledgering costs but lacked sufficient final proof capability; public-chain systems had strong proof capability, but daily ledgering costs were too high. The Public Credit Root provides a third approach: daily ledgering does not all have to go through public chains, while final proof can be anchored to the Public Credit Root. This is a fundamental change for financial systems. What financial systems need most is not for every business event to be processed by global consensus, but for key facts to be verifiable when disputes, audits, regulation, clearing, redemption, and risk events arise. The Public Credit Root allows financial systems to operate at low cost in ordinary times and remain verifiable at critical moments; to protect privacy in daily operations while preserving tamper-resistant history; and to process internally with high efficiency while anchoring externally at the final level. This is the essence of the Lowest Ledgering Cost: it is not a reduction of security. Rather, while satisfying the requirements of financial responsibility, risk control, privacy protection, and regulatory verification, it places the highest level of proof cost where it is most needed.

VI. This Is Not an Ordinary Blockchain Application, but an Application of the Credit Root

Hashing ledger pages onto the chain may appear on the surface to be a blockchain application, but its underlying idea is entirely different. Ordinary blockchain projects try to become new systems themselves: issuing tokens, establishing consensus, maintaining nodes, designing incentives, forming ecosystems, and claiming tamper resistance. The essence of this path is the repeated construction of credit roots. Using a Public Credit Root is different. It recognizes that Public Credit Roots or programmable credit roots such as Bitcoin and Ethereum have already matured, and that there is no need to reinvent the wheel. Ordinary blockchain projects ask, "How can I make others believe in my chain?" Applications of the Public Credit Root ask, "How can I use the most trusted chain to prove that my ledger has not been tampered with?" The former pursues "becoming the root oneself"; the latter pursues "connecting to an existing root." In the future, the vast majority of financial systems do not need to become Public Credit Roots. They only need to connect to Public Credit Roots. This will greatly reduce the complexity and cost of financial infrastructure.

VII. Why the Transparent Bank Must Use the Public Credit Root

The goal of the Transparent Bank is to make key financial facts verifiable while preserving banking efficiency, privacy, compliance, and service capability. This means it must simultaneously satisfy two conditions: it must be more trustworthy than a traditional bank, and its ledgering cost must not be much higher. If a Transparent Bank puts all business onto high-cost public chains, it will be difficult to compete with traditional banks. The internal ledgering cost of traditional banks is very low. If the cost of a Transparent Bank is too high, users will not pay for inefficiency over the long term, and enterprises will not pay for unnecessary high-cost infrastructure. Therefore, the Transparent Bank must adopt the Lowest Ledgering Cost. Its correct structure is not "all business on-chain," but this: internal ledgers operate efficiently; ledger pages periodically generate hashes and are anchored to Public Credit Roots; reserves, liabilities, clearing, permissions, and risks form verifiable proofs; and users, regulators, and counterparties obtain different levels of verification capability according to their roles. Without using the Public Credit Root, the Transparent Bank can only continue to rely on traditional audits and regulatory reports, making it essentially no different from a traditional bank. If it relies excessively on public chains to record every transaction, the cost will become too high. Only through anchoring to the Public Credit Root can the Transparent Bank obtain low cost, high trust, auditability, regulatability, traceability, privacy protection, and the ability to prove key facts at the same time.

VIII. The Lowest Ledgering Cost Is Not the Lowest Security, but the Optimal Security Allocation

Some may misunderstand the "Lowest Ledgering Cost" as meaning that security is unimportant. The opposite is true. Its objective is to avoid unnecessary and repetitive consensus costs while satisfying the requirements of financial security. Security requires expenditure, but the money must be spent in the most critical places. For Bitcoin and Ethereum, it is reasonable to spend costs on maintaining Public Credit Roots. But for ordinary commercial financial ledgers, having every entry pay the cost of public consensus is not necessarily the optimal allocation. A more reasonable structure is this: the core credit root bears the highest level of security; commercial systems handle daily business processing; hash commitments connect the two; AI auditing continuously checks for anomalies; the legal system handles responsibility boundaries; and the regulatory system conducts external supervision. This is not a reduction of security, but layered security. Mature financial systems have never been single-layer structures. They are layered structures: payment layer, clearing layer, custody layer, audit layer, regulatory layer, and final credit-anchor layer. The Public Credit Root gives digital finance, for the first time, a truly external, open, machine-verifiable final credit-anchor layer. Therefore, the true meaning of the "Lowest Ledgering Cost" is this: to obtain sufficiently high final trustworthiness at the lowest daily cost.

IX. How the Public Credit Root Reconstructs Financial Infrastructure

The Public Credit Root reconstructs financial infrastructure not by replacing all financial institutions, but by changing the underlying trust structure of the financial system. In the past, trust in financial infrastructure mainly came from institutions: the bank said the accounts were correct; the auditor said the statements were true; the regulator said the institution was compliant; the exchange said the assets were safe; and the platform said the data had not been tampered with. In the future, these promises can all be proven. Banks will still keep accounts, but ledger pages can be anchored. Audits will still exist, but results can be reviewed. Regulation will still be important, but it can obtain stronger evidence. Exchanges will still operate, but asset states can be verified. Platforms will still process business, but key states cannot be modified without leaving a trace. Verifiable mechanisms strengthen the evidentiary structure and the responsibility structure; they do not replace accounting, auditing, regulation, or judicial judgment. The Public Credit Root does not necessarily change the external appearance of every financial institution, but it changes the underlying constraints. In the past, users could only believe what institutions said. In the future, what institutions say can be verified. This is not about turning banks into public chains, not about turning enterprises into DAOs, and not about making all data public. It is about connecting key financial facts to the Public Credit Root. This will bring a new paradigm: institutions will still operate, but key financial facts cannot be asserted for long periods outside verification structures; ledgers will still be maintained internally, but they cannot be modified without leaving a trace; business will still remain confidential, but key states must be provable; finance will still require trust, but trust will increasingly be built upon verification.

X. Conclusion: The Public Credit Root Brings Financial Ledgering into a New Stage

Financial systems will always need ledgering. The question is not whether there is a ledger, but whether the ledger can be trusted; not who keeps the accounts, but whether the accounts can be verified after they are kept; not whether something is on-chain, but whether key facts can obtain final proof. Traditional banks solved low-cost ledgering, but did not solve continuous verifiability. Public chains solved verifiability, but are not suitable for carrying all daily commercial ledgering. The Public Credit Root provides a third path. It allows financial systems to keep accounts at low cost, anchor with high trust, protect privacy, support audit, accept regulation, prevent tampering without trace, and prove key facts. This is the true meaning of the Lowest Ledgering Cost. After the emergence of the Public Credit Root, human financial systems can, for the first time, more clearly

separate the cost of daily ledgering, the cost of key proof, and the cost of final anchoring. Future finance does not need every institution to build chains repeatedly, and it cannot continue to remain in the traditional black box. What future finance needs is: one ledger for every institution, with key states anchored to the Public Credit Root. This is not a simple technical optimization, but an institutional reconstruction of the financial ledgering system. The Bitcoin system created the Public Credit Root; the Public Credit Root reduces the final proof cost of trusted ledgering; and the Lowest Ledgering Cost gives Transparent Banks and more Verifiable Finance systems real commercial competitiveness. This is the practical meaning of the Public Credit Root, and it is also a key step for the financial system to move from trusting institutions to verifying facts. If today's market still has not fully understood the long-term value of the Bitcoin and Ethereum systems, one important reason may be that the mainstream cryptocurrency industry still has not truly understood the Public Credit Root, nor has it truly understood the significance of the Lowest Ledgering Cost for the future of financial infrastructure.

Chapter Four
Open Source Is a Means; Verification Is the Future of Finance

— How the AI Era Redefines Trusted Systems

The rapid development of AI is launching an unprecedented challenge to the most basic open-source trust model of cryptocurrency. In the past, open source was an important way for cryptocurrency to establish trust. Now, AI is changing the capability structure of both attackers and defenders, making "code disclosure" no longer sufficient to constitute financial-grade security. The new trust paradigm must answer two questions: first, why open source is not the endpoint of financial security; and second, what future finance should actually verify.

I. The Cryptocurrency Industry Must Re-understand "Open Source"

In the cryptocurrency industry, open source has long been regarded as an almost sacred principle. Bitcoin is open source. Ethereum is open source. A large number of public chains, wallets, smart contracts, and DeFi protocols also use open source as the foundation of their own credibility. The industry generally believes that because the code is public and everyone can examine it, the system is safer; because the rules are public and everyone can verify them, the system is more trustworthy; and because the project is open source and developers and users can participate, the system is more decentralized. This logic was valid in the early stage of cryptocurrency. When a system has no state credit, no bank endorsement, no corporate guarantee, and no legal enforcement, it can obtain trust only through public code, public ledgers, public rules, and public nodes. Bitcoin and Ethereum had to be open source because they had to prove that they were not black boxes, not scams, and not new databases disguised by centralized institutions. But one fundamental point must be seen clearly: open source is not the objective. It is only an important means of enabling independent third-party verification. Verification is the objective. If people cannot effectively verify a system, then open source loses its financial meaning. More further, even if a system is already open source, if it still cannot prove that the system is secure, that assets are real, that liabilities are complete, that permissions have not been abused, and that key states have not been tampered with, open source itself cannot constitute the trust foundation of a financial system. There is a major misunderstanding in the cryptocurrency industry: equating "visible code" with a "credible system," equating "public code" with "financial security," and equating "open-source culture" with "financial responsibility."

This misunderstanding will become especially dangerous in the AI era.

II. Why Open Source Does Not Equal Security

Open source allows people to see code, but it cannot guarantee that the code has no vulnerabilities. This is the first layer of the problem. A large financial system may contain millions of lines of code, involving the protocol layer, wallet layer, front end, back end, databases, key management, permission systems, smart contracts, APIs, node software, dependency libraries, compilers, deployment scripts, operation and maintenance systems, and governance mechanisms. Making the code open source only means that these codes can, in theory, be reviewed. It does not mean that they have actually been sufficiently reviewed. More importantly, the risks of a financial system often do not lie only in the code itself, but at the boundary between code and reality. The same piece of code may carry completely different risks if the deployment method is different, the permission configuration is different, the front-end invocation is different, the dependency-library version is different, the administrator key-management method is different, the oracle data is different, or the governance parameters are different. Therefore, at most, open source proves what a certain piece of code looks like. It does not automatically prove the following facts: that the deployed version is exactly this code; that the contract deployment has not been replaced; that upgrade permissions have not been abused; that the front end has not induced users to sign incorrectly; that dependency libraries have not been contaminated; that the oracle has not been

manipulated; that multi-signature control has not fallen into the hands of a few people; that governance has not been manipulated by capital or AI-driven public opinion; that key assets have not been misappropriated; or that system liabilities have not been hidden. This is why many open-source projects are still attacked, why many audited smart contracts still encounter problems, and why many seemingly transparent DeFi protocols still cannot become mainstream financial infrastructure. Therefore, open source and verification are not a simple relationship of substitution. Open source can improve inspect ability, while verification advances inspect ability into a structure that can be reviewed, assigned responsibility, and absorbed by institutions. What a financial system needs is not a single tool, but a combination of open source, formal verification, operational proofs, permission control, audit supervision, and legal responsibility. What financial systems need is not "visible code," but "proof of key facts." Open source asks: "Can you see it?" Finance asks: "Can you prove it?" These are not the same question.

III. In the AI Era, the Risks of Open Source Will Be Systematically Amplified

The emergence of AI has fundamentally changed the open-source security model. In the past, understanding complex code, discovering deep vulnerabilities, and writing usable attack scripts required extremely high professional barriers. Excellent security researchers were scarce resources, so the risks and benefits of open source were roughly balanced: good actors could read the code, and bad actors could read it too, but truly understanding and exploiting vulnerabilities was not easy. AI has completely changed this balance. It can help attackers quickly read code, understand architecture, search for boundary conditions, analyze permission paths, reproduce historical vulnerabilities, generate test cases, construct attack transactions, simulate on-chain states, and automatically discover compositional risks among contracts.

AI compresses vulnerability analysis that previously required weeks into days or even hours. It turns attacks that previously targeted a single project into batch scanning, batch reasoning, and batch attacks. This means that open-source code is no longer only a resource for white-hat auditors. It may also become training material, a reasoning map, and a vulnerability library for black-hat attackers. In the AI era, attackers are no longer merely isolated individual hackers. They may become AI attack systems operating twenty-four hours a day. Such systems can continuously scan code repositories, monitor new commits, analyze version differences, generate phishing pages, forge community opinion, induce governance votes, and combine code vulnerabilities, economic vulnerabilities, governance vulnerabilities, and social engineering. Therefore, the old logic that "open source allows everyone to audit, so it is more secure" is no longer sufficient. A more accurate statement should be this: AI makes white hats stronger, and it also makes black hats stronger. Open source remains important, but without higher-level verification mechanisms, permission controls, operational proofs, and responsibility records, open source may turn from part of a security advantage into part of an attack entrance.

IV. Why Systems Full of Uncertainty Can Hardly Become Real Financial Systems

What financial systems fear most is not complexity, but uncertainty. A financial system can be complex, but it must possess certainty: the rules must be certain, the assets must be certain, the liabilities must be certain, the permissions must be certain, the clearing must be certain, the risk boundaries must be certain, the responsible parties must be certain, and the mechanisms for handling errors must also be certain. If a system contains uncertainty that cannot be evaluated, it is very difficult for it to carry large-scale financial credit. This is precisely the problem faced by many open-source crypto projects: the code is public, but whether it is secure is uncertain; the audit has been performed, but whether all major problems were discovered is uncertain; the contract has been deployed, but whether it will be upgraded in the future is uncertain; governance is public, but whether it has been manipulated is uncertain; assets have been locked in, but whether the bridge is safe is uncertain; the protocol is running, but whether compositional risks are out of control is uncertain; the front end displays a balance, but whether the asset can be redeemed is uncertain; and the project promises transparency, but whether liabilities are complete is also uncertain. Such systems can be used for experiments, speculation, and early innovation spaces, but they cannot easily be treated as financial infrastructure. A financial system is not a game. A financial system handles savings, payments, wages, debts, pensions, corporate assets, public finance, national credit, and social stability. A system that cannot withstand AI attacks, long-term operation, stress tests, legal accountability, and customer-protection requirements cannot be regarded as a mature financial system simply because it is open source. Therefore, the core standard of future finance should not be "whether it is open source," but whether it has operated stably for a long time, whether it has endured real stress tests, whether it has verifiable proofs, whether it has clear risk boundaries, whether it has recovery mechanisms, whether it has responsible parties, and whether it can prove key financial facts. Only a system capable of answering these questions is qualified to enter mainstream finance.

V. Only Large Open-Source Systems That Have Withstood Long-Term Testing Can Stand Firm

This does not mean that open source has no value. On the contrary, certain open-source systems have extremely high value. Bitcoin, Ethereum, Linux, some mature cryptographic libraries, and infrastructure projects have gradually established credibility precisely because they have been open for a long time, reviewed for a long time, operated for a long time, and fought attacks for a long time. But there is a key condition here: truly durable open source is not "code that has just been made public," but "an open

system that has endured long-term testing and has not suffered fundamental failure." A new project cannot immediately obtain financial-grade trust simply by placing its code on GitHub. A smart contract cannot immediately obtain financial-grade trust simply because it has passed one audit. A team cannot immediately obtain financial-grade trust simply by announcing that it is open source. A protocol cannot immediately obtain financial-grade trust simply because it has operated for a few months without incident. A financial-grade open-source system needs time. It needs long-term operation, multiple rounds of attack testing, multi-client implementations, continuous auditing, pressure from real assets, a stable developer community, prudent upgrade mechanisms, clear ecosystem dependencies, a traceable history of major vulnerabilities, and the ability to survive extreme market environments. Bitcoin's credit does not come only from open source. It also comes from more than a decade of global node verification, six-block confirmation, the extreme simplicity of its core rules, and its tenacious survival. Ethereum's credit likewise comes not only from being open source, but from years of actual operation, protocol upgrades, ecosystem verification, and real asset pressure. Therefore, we cannot treat "open source" itself as the source of credit. A more accurate hierarchy is this: open-source code provides initial transparency; long-term operation forms historical credit; verifiable proofs constitute financial trust; and the Public Credit Root provides final anchoring. An open-source project without the test of time should not be easily regarded as financial infrastructure. An open-source project without verification mechanisms should even less be regarded as safe simply because its code is public.

VI. How to Redefine Open Source

In the AI era, open source must be redefined. The old definition was relatively simple: the code is public, and viewing, copying, modifying, and distribution are allowed. That is open source. But "open source" in a financial system cannot remain only at the level of software licensing. Financial open source must add stricter meaning. In the financial sense, open source should include at least five levels.

First, code disclosure. Core code, key contracts, protocol logic, and client implementations should be made public as much as possible so that external parties can review them.

Second, rule disclosure. The issuance rules, clearing rules, permission rules, risk rules, upgrade rules, and exit rules of the system must be public. What matters most in a financial system is not whether the code is elegant, but whether the rules are clear.

Third, state verifiability. Users and external institutions must be able to verify key states, including assets, liabilities, reserves, permissions, clearing results, collateralization ratios, and redemption capacity.

Fourth, reviewable proofs. The system cannot merely say "I am safe," "I am compliant," or "I have reserves." It must provide proofs that can be reviewed, including cryptographic proofs, audit proofs, on-chain anchoring, state roots, zero-knowledge proofs, or other verifiable mechanisms.

Fifth, traceable responsibility. Financial open source cannot exist without responsibility. Who deployed, who upgraded, who custodies, who audits, who operates, and who bears responsibility must all be clear. Therefore, financial open source in the AI era can no longer be merely "code open source." It should mean: code is visible, rules are knowable, states can be proven, proofs can be reviewed, and responsibility can be traced. If a project achieves only code disclosure but has no state verification, proof mechanisms, or responsibility boundaries, it should not be called financial-grade open source.

VII. Full Code Open Source Is Not a Necessary Condition for Financial-Grade Verification

In financial systems, what we truly need to verify is often not all internal details, but whether key results are correct, whether key states are consistent, and whether key facts are real. This is similar to zero-knowledge proofs, hash chains, or state-root mechanisms: the verifier does not necessarily need to see all original data, nor does the verifier necessarily need to know all business details. The verifier only needs to be able to verify that the result has not been tampered with, that the rules have not been broken, and that the state is consistent with the commitment. Therefore, immutability and verifiability are higher objectives. If state verification can be achieved through verifiable computation, zero-knowledge proofs, trusted execution environments, on-chain anchoring, audit proofs, and multi-party review, then whether the code is fully open source is no longer the only source of trust.

This is not a defense of black boxes, but a restoration of the proper meaning of financial-grade verification. The problem of traditional finance is opacity; the problem of extreme open-source thinking is the belief that public code is sufficient. The Transparent Bank takes a third path: protecting privacy and commercial security while proving key facts.

VIII. Conclusion: Verification Is the Future of Finance

Open source is important. A large number of open-source projects on GitHub have provided enormous convenience to ecosystem developers and created important conditions for technical collaboration, code reuse, and infrastructure construction. But financial systems place greater emphasis on security, responsibility, and reviewability. Therefore, verification is far more important than open source. The future of finance is not that all code becomes public, but that key facts cannot be falsified.

The future of finance is not that all centers disappear, but that centers cannot claim key facts outside a verification structure. The future of finance is not that all business goes onto public chains, but that key states can be anchored to a Public Credit Root. The future of finance is not that all risks are eliminated, but

that risks can be identified, measured, isolated, and assigned responsibility. The future of finance is not that open source replaces banks, but that the key financial facts of banks must become verifiable. In the first half of the cryptocurrency industry, open source established the initial trust. In the second half of the cryptocurrency industry, verification must be used to enter the real financial world. Bitcoin and Ethereum proved the possibility of Public Credit Roots.

AI has exposed the fragility of the old security model and has also provided the capability to build new verification systems. What the Transparent Bank must do is combine Public Credit Roots, AI, and commercial finance, and push finance from “trusting institutions” toward “verifying facts.”

To overcome black boxes, future finance will not rely on open source itself. Open source is only a means. Now that we already have Public Credit Roots such as Bitcoin and Ethereum, verification is the future of finance. Human finance must move from relying solely on open-source trust toward an age that combines verification, responsibility, and institutional absorption.

Part II
Transparent Finance and Banking Practice

Chapter Five
Transparent Bank:
Not Ex Post Supervision, but a Banking Form of Continuous Verification

— *Verification Constraint Structures within Licensed Financial Institutions*

Core Proposition

Traditional finance faces a structural difficulty: credit expansion lacks verifiable constraints. The root of financial bubbles lies not only in human greed or market speculation, but more fundamentally in the fact that credit can expand inside black boxes, and risks can accumulate inside the system until they are forced into the open by a crisis. What the Transparent Bank attempts to establish is a hard constraint that places credit expansion inside a verifiable structure. The Transparent Bank does not abolish bank responsibility, nor does it make all customer data and business processes of a bank public. The core of the Transparent Bank is this: while licensed banks continue to assume responsibility for accounts, accounting, risk, customer protection, compliance, and legal liability, key business facts, key authorizations, key delivery events, key accounting results, and key responsibility records must be capable of continuous verification. In this structure, transparency does not mean full disclosure. Transparency means that key facts must exist, must be referable, must be traceable, and must be able to provide an appropriate degree of verification to customers, auditors, regulators, and partner institutions according to permission.

I. From Bitcoin to Transparent Bank: The Evolution of Verification Systems

Verifiable Finance was difficult to realize in the past, not because the direction was wrong, but because the conditions were not yet mature. Public Credit Roots, controllable accounting systems, AI continuous auditing, verifiable proofs, and legal responsibility systems had not yet formed an effective combination. After 2025, these conditions began to mature at the same time, but the industry still has not fully discovered their financial application.

1. The Trusted Cornerstone of Verification: The Maturity of Public Credit Roots

The Bitcoin ledger does not require trust in any individual or institution. Whether Satoshi Nakamoto exists or not, he cannot change ledger history that has already been fixed. Once any data, especially a hash value, is anchored into it, that data obtains uniqueness, temporality, and verifiability. This constitutes the foundation of machine credit, namely the Public Credit Root. The purpose of the openness and transparency of a Public Credit Root is not to display all business details, but to allow key facts to be independently verified. It does not require all financial data to be exposed on a public network. Rather, it provides an external, open, long-running, difficult-to-tamper-with public credit anchor.

2. The Bitcoin Ledger Cannot Directly Replace Traditional Financial Ledgers

The Bitcoin ledger is essentially a public general ledger, and its structure differs greatly from the general ledgers, subsidiary ledgers, customer ledgers, compliance ledgers, and internal business ledgers of traditional banks. Bitcoin can verify on-chain transfers, but it cannot directly verify the off-chain asset-liability structure of a bank. When Bitcoin's idea expands to Ethereum and stablecoins, the problem of off-chain verification still remains. For example, the on-chain issuance volume of a stablecoin can be verified, but its dollar reserves, liability structure, custody arrangements, and redemption capacity still require off-chain proof. If these off-chain facts cannot be continuously verified, the system can only once again rely on audit institutions, regulatory licenses, and market trust. One of the great meanings of the Bitcoin system is that it avoids requiring all projects to repeatedly build chains. Other ledgers

can obtain Public Credit Root anchoring through hash commitments. As long as the hash values of key ledgers are periodically anchored to a Public Credit Root, external verifiability can be established for off-chain ledgers. This lays the technical foundation for the Chainless System and the Transparent Bank.

3. The Chainless System: The First Step in Using Public Credit Roots

The Chainless System realizes the principle that "facts can be anchored, while disclosure can be selective," and lays another cornerstone of Verifiable Finance. It does not make everything public, nor does it put every business activity on-chain. Instead, it places key facts into a verifiable structure. The Chainless general ledger adopts a transparent index ledger and, through the Bitcoin Public Credit Root timestamping service, stores journal hash values in the Bitcoin system, establishing a verifiable audit trail. At the same time, the platform supports browser-based auditing, third-party data downloads, node participation, and multi-layer data-verification mechanisms. The general-ledger structure of Chainless consists of coin indicators, the latest transaction records of subledgers, a subledger hash index table, an indicator log ledger, a transaction log ledger, and a verification log ledger. The verification log ledger calculates the hash value of the transaction log ledger through checkpoints and records it into the Bitcoin system, corresponding to the log ledger at the relevant time point. This is the technical foundation of "facts can be anchored."

"Selective disclosure" absolutely does not mean "selective facts." Facts must enter the verifiable structure, while disclosure can be layered, role-based, and permission-based. Users can decide which plaintext information is disclosed to which parties, under what conditions, and at what granularity. But key facts cannot detach themselves from the verification structure merely because they are not disclosed. This is already very close to the structure required by the Transparent Bank: the public layer sees the existence of facts and state summaries; the customer layer sees the customer's own complete results; the bank compliance layer penetrates according to law; the regulatory and audit layers conduct sampling according to permission; and the market layer sees only content that has been approved or that the customer has chosen to disclose.

4. Transparent Bank: From "Can Be Verified" to "Must Be Verified"

The evolution of the Transparent Bank can be summarized in three steps: Chainless solves the question of "whether verification is possible"; the reference chain of the Transparent Bank solves the question of "whether verification can be bypassed"; and banking rules together with the legal responsibility system solve the question of "whether verification is mandatory."

When verification capability is combined with rule-based constraints and embedded into the banking structure, the financial system undergoes a fundamental change: the bank is no longer merely an institution that performs compliance judgments, but becomes the financial base that carries "verification plus constraint." On-chain verification reversely constrains off-chain data, making it impossible for off-chain data to change arbitrarily outside the verification structure. The key to the Transparent Bank is not putting the bank on-chain, but placing the bank inside a verifiable structure; not making banks disappear, but making the key facts of banks unable to be asserted or maintained outside the verification structure.

II. The Core Principle of the Transparent Bank: Realizing Verifiable Finance

The core problem solved by the Transparent Bank is to establish a structure in which on-chain and off-chain record hashes cannot become inconsistent without leaving a trace. A financial system does not need to disclose all business activities. But for any key fact that enters the reference chain, a proof relationship must be formed that is verifiable, traceable, and capable of assigning responsibility.

1. Consistency of On-Chain and Off-Chain Record Hashes

The consistency of on-chain and off-chain record hashes is the institutional foundation of the Transparent Bank. Business brought into this structure must form reviewable proof relationships across six dimensions: On-chain facts: whether external anchoring and time commitments have already been formed. Off-chain accounting: whether the internal ledger is consistent with the anchored state. Financial facts: whether assets and liabilities, income, gains, and losses match the accounts.
Regulatory facts: whether compliance reports, penetration checks, and responsibility boundaries are consistent with the real business. Responsibility facts: whether who initiated, who authorized, who reviewed, and who bears responsibility can be traced. Reconciliation facts: whether internal reconciliation is correct. These six dimensions address the most fundamental questions of the financial system: whether something is true, whether it occurred, whether it was completed, and whether the attribution of responsibility is clear.

2. Consistency and Disclosure Must Be Distinguished

The Transparent Bank must distinguish between "consistency" and "disclosure." Consistency is a mandatory rule; disclosure is a governance choice. Consistency addresses whether something is true, whether it occurred, whether it was completed, and whether attribution of responsibility is clear. Disclosure addresses who can see, what can be seen, how much can be seen, and under what conditions it can be seen. The core expression is this: facts must exist, while disclosure can be layered. "Selective disclosure" must not be misunderstood as "selective facts."

III. The Structural Model of the Transparent Bank

1. Reconstruction of the Bank's Role

In a Transparent Bank, the bank is not merely a compliance judge, nor is it simply an on-chain interface. The bank must build a chain of truthfulness judgments and organize accounts, accounting, authorization, clearing, risk, and responsibility into a unified verifiable structure. The bank still preserves customer service, risk control, privacy protection, compliance handling, and legal responsibility, but its key states must be constrained by the Public Credit Root. On-chain verification reversely constrains off-chain data, so that off-chain data must also obey the verification structure.

2. The Division of Labor Between Chainless and the Reference Chain

Chainless brings off-chain data into a verifiable structure through its general-ledger and subledger structure: the general ledger records states and indexes; subledgers carry complete data; and the Public Credit Root is responsible for key hash anchoring. The reference chain embeds verification into business processes. Each link references the others, states are forcibly aligned, and on-chain anchoring is bound to off-chain business. It turns verification from a mere ex post action into the business structure itself. Therefore, the essential change of the Transparent Bank is this: verification changes from a capability into a structure, from an audit action into a financial constraint, and from an external inspection into an internal operating rule. The reference chain is the key function for realizing the Transparent Bank.

3. The Overall Structure of the Transparent Bank

The overall structure of the Transparent Bank can be summarized as: private business system + controllable accounting system + Public Credit Root anchoring + verifiable proofs + AI continuous auditing + legal responsibility system. Within this structure, the private business system preserves commercial efficiency and customer experience; the controllable accounting system reduces daily ledgering costs; the Public Credit Root provides key hash anchoring; verifiable proofs provide independent review capability; AI continuous auditing provides real-time monitoring capability; and the legal responsibility system handles responsibility, remedy, and disputes in the real world.

IV. The Practical Landing Point of the Transparent Bank: Solving Pain Points in Crypto and Traditional Finance

The Transparent Bank is not an abstract theory. It can directly solve several core pain points in crypto finance and traditional finance.

1. The Stablecoin Problem: From Trusting Reserves to Verifying Reserves. The key to stablecoins is not on-chain issuance volume, but off-chain reserves, liabilities, and redemption capacity. The traditional model relies on audit institutions and issuer disclosures. The Transparent Bank can instead bring reserves and liabilities into a continuously verifiable structure. In a feasible model, the stable coin company is responsible for business initiation and asset management, while the Transparent Bank is responsible for recording, verifying, generating hashes, and anchoring them to a Public Credit Root. Without lawful initiation by the stable coin party, the Transparent Bank has no authority to move assets. Without the verification structure of the Transparent Bank, reserves and liabilities cannot obtain continuously credible proof. Ordinary users see simplified disclosure, regulators obtain penetrative verification, and the market obtains overall credibility.

2. The Centralized Exchange Problem: From the Ability to Generate False Positions to Asset-Liability Consistency The greatest risk of centralized exchanges is not centralization itself, but whether assets, liabilities, positions, and customer rights are truly consistent. The Transparent Bank can transform an exchange into a transparent centralized exchange: key states are anchored to a Public Credit Root, and customer rights, exchange liabilities, custodied assets, and risk exposures must enter a verifiable structure. In this way, the exchange can still preserve matching efficiency and user experience, but it cannot hide liabilities, misappropriate assets, or generate false positions inside the system without leaving a trace.

3. The Custody and Audit Problem: From Periodic Manual Inspection to Structured Continuous Verification Traditional auditing is periodic, while the verification of the Transparent Bank is continuous. Auditing no longer relies only on manual sampling and report inspection, but realizes real-time review through AI continuous monitoring, on-chain proofs, ledger-page hashes, permission records, and anomaly detection. Audit institutions remain important, but their role will shift from being an "ex post judgment center" to rule design, proof certification, dispute adjudication, and high-risk review.

4. Essential Return: Finance Is Built on Verification

The essence of the Transparent Bank is to build the financial system on verification, not merely on trust. Once the Transparent Bank works, its model and principles will apply not only to banks, but also to stable coins, exchanges, custody, funds, supply-chain finance, corporate ledgers, and public finance. In this sense, the Transparent Bank is not an isolated project, but the practical entrance to Verifiable Finance.

V. What Exactly Does the Transparent Bank Verify?

The core of the Transparent Bank is not to "make everything public," but to make key financial facts verifiable. What it verifies is not every commercial secret, but those key facts that determine financial trust.

First, it verifies reserves. When a financial institution claims how many assets it has, this cannot rely only on reports. The Transparent Bank must provide verifiable evidence for the existence, ownership, and state of reserves. Reserves may be cash, Treasury securities, bitcoin, ether, stable coins, other assets, or qualified collateral, but they must enter the corresponding verification structure.

Second, it verifies liabilities. Proof of reserves alone is not enough. If an institution has 10 billion in reserves but 20 billion in liabilities, it is still unsafe. Therefore, the Transparent Bank must verify the completeness of liabilities. It must not only prove "what I have," but also "how much I owe."

Third, it verifies asset-liability matching. Reserves and liabilities must be viewed together. What truly matters is not isolated proof of assets, but whether the balance sheet is healthy. The Transparent Bank must prove that assets cover liabilities, liquidity matches redemption needs, maturity mismatch is within a controllable range, and collateral value can withstand stress tests.

Fourth, it verifies clearing. The core of the financial system is clearing. Where money comes from, where it goes, when it is settled, whether it has been completed, whether it can be reversed, and whether there is double spending, duplicate accounting, or hidden misappropriation must all be verifiable.

Fifth, it verifies permissions. Many financial risks do not arise because assets do not exist, but because permissions are out of control. Who can transfer assets? Who can upgrade contracts? Who can change rules? Who can freeze accounts? Who can approve large transfers? Who can modify the reserve structure? Who can touch keys? The Transparent Bank must make key permissions visible, verifiable, traceable, and limitable.

Sixth, it verifies rules. Financial systems cannot change rules at will. Interest-rate rules, redemption rules, collateral rules, clearing rules, risk-control rules, upgrade rules, and user-protection rules should be set in advance as much as possible. Rules can be updated, but updates must have procedures, delays, notices, reviews, and exit mechanisms.

Seventh, it verifies risk. The Transparent Bank does not prove that there is "no risk." It proves where the risk is, how large the risk is, and whether the risk is controlled. It must verify leverage ratios, liquidity gaps, asset concentration, collateralization ratios, maturity mismatch, single points of failure, counterparty risk, market volatility pressure, and system endurance under extreme scenarios.

Eighth, it verifies redemption capacity. The most critical question for a financial institution is: when users want to withdraw, can you redeem? The Transparent Bank must continuously prove redemption capacity instead of disclosing problems only after a crisis occurs.

Ninth, it verifies system state. The value of blockchain lies in the verifiability of state. The Transparent Bank must extend this capability to commercial financial systems: account states, asset states, liability states, permission states, clearing states, and risk states should all be verifiable under privacy protection.

Tenth, it verifies responsibility. Finally, the Transparent Bank must verify responsibility. Who did what? Who approved what? Who changed what? Who bears what responsibility? Who compensates when an error occurs? Who is responsible in systemic risk? Financial transparency without responsibility verification is incomplete transparency.

Eleventh, it verifies boundaries. Not all verification needs to be public to the entire world. Verification should serve real business relationships and responsibility relationships. A transaction between two people only needs the two parties and the bank, as an independent third party, to participate in verification. Regulatory verification is also participation as a relevant party. From the perspective of privacy protection, the ordinary public does not need, and should not participate in, the verification of all transactions.

Cryptocurrency account transfers lack this layered verification mechanism, causing "coin loss" to become normal: verification responsibility is completely pushed onto users, while ordinary users cannot effectively verify. Verification in the Transparent Bank should be hierarchical and role-based: users verify their own account states, regulators verify compliance, counterparties verify the truthfulness of clearing, and the public verifies the overall health of reserves and liabilities. Not all data must go onto public chains, but key proofs must be capable of anchoring to a Public Credit Root.

VI. How the Transparent Bank Can Effectively Prevent AI Attacks

Preventing AI attacks cannot rely on the phrase "strengthen security." Attacks in the AI era are continuous, automated, and combinatorial. Therefore, defense must also be continuous, automated, and combinatorial.

First, the complexity of the core system must be reduced. Complexity is the soil of vulnerabilities. The more complex the system, the easier it is for AI to find vulnerabilities at the boundaries. Future financial systems must compress core rules to the simplest possible form, place complex business into isolatable modules, and put high-risk operations into strict verification frameworks. One important advantage of Bitcoin is that its core rules are extremely simple. Ethereum is more powerful, but its attack surface is also larger. As a case of Verifiable Finance,

The Transparent Bank must absorb the experience of both: the core credit anchor must be simple, commercial systems can be complex, but complexity must be isolated and verified.

Second, key rules must be set in advance. A financial system cannot rely on the moral self-discipline of its operators. Which assets can be moved, which permissions can be used, which actions must be delayed, which risks must trigger alarms, which operations require multiple verifications, and which states must be publicly proven should all be written into rules as much as possible. Taking the Transparent Bank as an example, the key is not to "believe that the bank will do good things," but to make the bank operate under rule-based constraints so that key facts cannot be arbitrarily falsified.

Third, a continuous verification system must be established. One audit is not enough, one open-source release is not enough, one test is not enough, and one incident-free launch is not enough. AI attacks are continuous, and financial defense must also be continuous. The system needs continuous code scanning, continuous contract detection, continuous anomaly monitoring, continuous transaction analysis, continuous permission checks, continuous reserve verification, continuous liability verification, and continuous risk-control updates.

Fourth, formal verification and machine-checkable proofs must be used. Key financial systems cannot rely only on humans reading code. Core invariants must be formally expressed, for example: assets cannot increase out of thin air; liabilities cannot be hidden; clearing cannot violate balance conservation; user assets cannot be transferred without authorization; permission changes must satisfy delays and multiple approvals; reserve proofs must match liability proofs. AI can help attack code, and it can also help generate and check proofs. Truly secure systems in the future will certainly involve long-term confrontation between attack AI and defense AI.

Fifth, risks must be isolated. One vulnerability should not destroy the entire system. An error in one contract should not empty all assets. An attacked front end should not cause permanent user losses. A manipulated governance vote should not immediately change core rules. A bridge problem should not infect all assets. Financial systems must have limits, delays, circuit breakers, layering, isolation, recovery, accountability, and compensation mechanisms.

Sixth, AI red teams and AI blue teams must be established. Future large financial systems need long-running AI red teams to continuously simulate attacks, and they also need AI blue teams to continuously defend and repair. AI red teams are responsible for finding vulnerabilities, simulating phishing, testing governance attacks, attacking permission boundaries, and constructing extreme market scenarios. AI blue teams are responsible for monitoring anomalies, generating patch suggestions, warning users of risks, verifying proof consistency, and discovering on-chain anomalies and off-chain fraud. Without continuous confrontation, a financial system cannot remain secure in the AI era.

VII. The Transparent Bank Does Not Oppose Open Source; It Transcends Open Source

The Transparent Bank does not oppose open source. It opposes sacralizing open source and treating open source as the endpoint of financial security. The Transparent Bank recognizes the value of open source, but it holds that the trust foundation of future financial systems must be higher than open source. In the Transparent Bank system, parts that can be open source should be open source; parts involving commercial secrets and security risks may remain not fully public; parts involving customer privacy must be protected; parts involving key financial facts must be verified; parts involving system rules must be set in advance; and parts involving public credit must be anchored to a Public Credit Root. This is a more mature view of financial transparency. It is neither the black box of traditional finance nor the naked exposure of extreme crypto-ism. It establishes a new balance among privacy, commercial security, public verification, and legal responsibility.

VIII. Regulatory Outlook: From Audit Judgment to Structural Verification

Traditional regulation relies on reports, audits, and licenses. In essence, it verifies institutions. The Transparent Bank shifts toward verifying structures: the regulatory focus moves from "whether this institution is credible" to "whether this fact is established"; from human judgment to structural constraint; and from ex post accountability to ex ante and in-process verification.

This will greatly reduce regulatory costs and improve regulatory precision. The core of future regulation should not be to restrict financial innovation itself, but to restrict unverifiable financial structures. Verifiable financial innovation should be encouraged, while unverifiable credit expansion should be constrained. After credit expansion is structurally constrained, the "privilege" meaning of licenses will weaken, and finance will gradually return to openness, justice, fairness, and immutability. This is not a departure from Satoshi Nakamoto's spirit, but the continuation and upgrading of Satoshi's spirit in commercial finance. Financial demand will become further disintermediated, and the space for corruption, fraud, and hidden misappropriation will be compressed. Clearing systems will shift from layer-by-layer reconciliation toward real-time settlement and continuous proof, significantly reducing financial friction. The bubble-formation mechanism of financial markets will be exposed earlier, and credit expansion will be unable to remain outside verification structures for long periods. The Transparent Bank is only one project of Verifiable Finance. Verifiable Finance will change the structure of future finance, and this structure is especially suitable

for the AI era: AI is responsible for continuous auditing and anomaly identification, Public Credit Roots are responsible for key hash anchoring, the legal system is responsible for real-world responsibility, and the banking system is responsible for commercial services.

IX. Conclusion: The Transparent Bank Is the Practical Form of Verifiable Finance

Cryptocurrency has already completed the first step: money is constrained. This step was completed by Bitcoin. The Transparent Bank represents the second step: credit is constrained. Through the Public Credit Root, the Chainless System, reference chains, verifiable proofs, AI continuous auditing, and the legal responsibility system, it makes it impossible for credit expansion to detach itself from a verifiable structure. The Transparent Bank strengthens the evidentiary structure of truthfulness; the verification structure strengthens reliability and reviewability; and Verifiable Finance as a whole solves the problem of unconstrained credit expansion. The key to future finance is not who controls the system, but that key facts cannot be asserted, confirmed, or maintained outside a verification structure for long periods. This is neither the simple on-chain migration of traditional finance nor the anarchic experiment of pure DeFi. It is a new form after both: Verifiable Finance. The Transparent Bank is the practice of the historical transition in human finance from "trusting institutions" to "verifying facts." By embedding verification mechanisms into banking, it forms a continuous verification structure in which off-chain data is constrained by on-chain anchoring, and it is especially suitable for the AI era. Its success will inspire the emergence of more Verifiable Finance innovation projects. The next chapter will further explain that as long as innovation can enter a verifiable structure, it has the possibility of being absorbed by institutions.

Chapter Six
From Double-Entry Bookkeeping to Transparent Bank: The Historical Evolution of Financial Constraint Structures

Core Proposition

Every major evolution in financial history appears, on the surface, to be a change in accounting tools, payment media, or financial technology. In substance, however, it is a reorganization of the structure of credit constraints. Double-entry bookkeeping solved the problem of how an institution could make its internal accounts self-consistent. Bitcoin provided an external Public Credit Root. The Chainless System and hash anchoring provide an implementable verification path for real-world finance. The Transparent Bank goes one step further by embedding verification capability into the banking system, so that key financial facts cannot exist for long outside a verification structure. Therefore, the Transparent Bank is neither the simple migration of a traditional bank onto a chain nor an anarchic experiment in pure DeFi. It is an institutional upgrade of the structure of financial constraints after double-entry bookkeeping. It represents a historical transition in finance from being driven by trust to being driven by verification constraints.

I. The Financial System Is Entering a New Era of Credit Constraints

The modern financial system has greatly improved the efficiency of resource allocation and has also greatly amplified the capacity for credit creation. Yet it has always retained one deep defect: credit can continue to expand, while verification remains chronically behind the expansion itself. In traditional finance, assets, liabilities, income, risks, and responsibilities are kept credible mainly through institutional internal accounts, periodic audits, regulatory reports, and legal liability. External parties can understand the true state of an institution only indirectly. Credit expansion occurs inside the system; verification often occurs after the fact. In crypto finance, on-chain assets have verifiability, but off-chain liabilities, reserves, custody arrangements, exchange positions, and the redemption capacity of stable coins still depend heavily on institutional disclosure and third-party proof. As a result, although cryptocurrency introduced verifiability on-chain, in the expansion of off-chain credit it has partly returned to the old path of traditional finance: licenses, audits, regulation, and market trust. Therefore, the fundamental task of future finance is not merely to continue creating credit, nor simply to compress credit, but to prevent credit expansion from existing for long outside a verification structure. The Transparent Bank is a new financial form proposed at this historical turning point. It does not answer a general question of digital upgrading, but a deeper question: how can key financial results be required to be established, maintained, and recognized inside a verification structure?

II. Double-Entry Bookkeeping: The Internal Constraint Structure of Modern Finance

If the Transparent Bank is placed within a longer history of finance, it should not be understood as an isolated innovation. It should be understood as a further evolution of the structure of financial constraints after double-entry bookkeeping. The greatness of double-entry bookkeeping lies not only in the creation of corresponding debit and credit entries. More importantly, through two-sided records it established internal constraints among economic facts, allowing modern banks, corporations, and fiscal systems to possess a systematic internal accounting order for the first time. It solved an extremely basic yet extremely important problem: how accounts could be established as self-consistent inside an institution. For precisely this reason, double-entry bookkeeping laid the accounting foundation of modern financial civilization. Without double-entry bookkeeping, it would be difficult to have the modern corporate system, bank balance sheets, fiscal budgets, capital markets, and the modern audit system. However, the constraints of double-entry bookkeeping still mainly remain within the internal ledger system of an institution. It can prove account balance, account classification, and accounting self-consistency, but by itself it cannot prove that the accounts remain continuously consistent with external facts, custody structures, on-chain states, regulatory records, and chains of responsibility. In other words, double-entry bookkeeping solved the problem of “internal account consistency,” but not the problem of “external verifiability.” The Transparent Bank does not negate double-entry bookkeeping. Rather, it advances on its foundation: it extends internal accounting constraints into external verifiable constraints, and extends debit-credit balance into a continuous consistency constraint among on-chain and off-chain states, accounting records, responsibilities, regulation, and results. If double-entry

bookkeeping laid the internal accounting foundation of modern finance, then what the Transparent Bank seeks is to establish, on that foundation, the external constraint foundation of Verifiable Finance.

III. Bitcoin's Public Credit Root: Providing External Finality for Modern Finance

The reason the Transparent Bank can become possible does not first lie in a change inside the bank itself. It lies in the fact that the financial world, for the first time, has obtained a Public Credit Root on which it can rely over the long term. The most far-reaching historical significance of Bitcoin is not only that it created a digital asset, but that it provided a new credit idea: once any key fact is anchored to an open, long-running, difficult-to-tamper-with public ledger, it can obtain external finality and no longer depend only on an institution's internal statement. This means that Bitcoin's most important contribution to the financial system is not only to constrain the on-chain money supply, but to provide future finance with a Public Credit Root capable of receiving key facts, responsibility anchors, and time commitments. It is in this sense that the Transparent Bank inherits the deeper idea of Bitcoin: a bank should no longer rely only on internal accounts to prove its own truthfulness. It must place key states upon a credit root that can be independently verified from outside. This is the foundation that Bitcoin's credit-root idea provides for the Transparent Bank. It answers why the Transparent Bank can obtain finality, and it also answers why future finance does not need every system to build a new chain again.

IV. Chainless and Hash Anchoring: Providing an Implementable Balance for Real- World Finance

A Public Credit Root alone is not sufficient to directly carry modern finance. The Bitcoin ledger can prove on-chain transfers, but it cannot directly replace a bank's general ledger, customer ledger, compliance ledger, and internal business ledger. Nor can it directly carry complex asset-liability structures, custody relationships, and business processes. Therefore, the Transparent Bank does not move all financial activity onto public chains. Instead, through the Chainless System, hash anchoring, index structures, and timestamp mechanisms, it brings key facts into a verifiable structure while preserving off-chain business processing, layered disclosure, and commercial efficiency. This is the most important institutional meaning of Chainless and hash anchoring. They are not merely ways to reduce technical costs; they establish a realistic balance among authenticity, performance, and privacy. Key facts must enter a verification structure, while sensitive business details may remain off-chain. Facts must be anchorable; disclosure can be governed in layers.

As a result, the Transparent Bank neither moves to the extreme of "everything public and everything on-chain," nor returns to the old path of "complete dependence on an internal black box." Instead, it forms an implementation method truly suitable for commercial finance, regulated finance, and institutional finance.

If Bitcoin's Public Credit Root answers the question "why it is credible," then Chainless and hash anchoring answer the question "why it is implementable."

V. From "Can Be Verified" to "Must Be Verified": The True Leap of the Transparent Bank

The Chainless System gives financial facts the ability to enter a verification structure, but this is not yet the most fundamental breakthrough of the Transparent Bank. The true leap occurs when verification capability is further embedded into the institution: verification is no longer an after-the-fact action, nor an optional add-on, but a precondition for the validity of business. This evolution can be summarized in three steps: the Chainless System solves "whether it can be verified"; the reference chain solves "whether verification can be bypassed"; bank rules and the legal responsibility system solve "whether verification is mandatory."

Therefore, the fundamental difference between the Transparent Bank and all previous experiments in "blockchain finance" does not lie in its use of more on-chain technology. It lies in a deeper institutional transformation: from verification capability to verification constraint. In this structure, key facts cannot merely be recorded; they must be established within the structure. Key states cannot merely be explained; they must be aligned within the process. Key results cannot rely only on after-thefact proof; from the moment they are formed, they must already be in relationships that can be verified, replayed, and assigned responsibility. This means that a ledger is no longer merely self-consistent. It must jointly form a consistency structure with facts, responsibilities, regulation, and external anchoring.

VI. The Essence of the Transparent Bank: Preventing Banks from Existing Outside the Structure of Authenticity for Long

Under the framework of the Transparent Bank, the role of the bank is redefined. The bank is no longer merely a trusted institution authorized by the government, a compliance judge, or a financial intermediary. It becomes the organizer of chains of authenticity, chains of responsibility, and chains of verification.

What it organizes is not only assets and liabilities. It brings subject facts, authorization facts, transaction facts, delivery facts, responsibility facts, and accounting facts that further enter the result domain of the bank into a unified structure of on-chain and off-chain consistency. The Transparent Bank does not emphasize that all business matters must be public. It emphasizes that key facts cannot be absent, key responsibilities cannot leave no trace, and key results cannot be unverifiable. This is also why consistency must be distinguished from disclosure: consistency is a non-optional underlying rule, while disclosure is a surface-level arrangement that can be governed in layers. What the Transparent Bank truly seeks to establish is not crude transparency, but a financial structure in which the authenticity between ledgers and facts cannot be evaded for long.

VII. Five Categories of Key Facts and Accounting Facts: The Minimum Constraint Units of Verifiable Finance

Financial activity in the Transparent Bank is no longer treated as an indivisible comprehensive result. It must be decomposed into several minimum verifiable units. At least five categories of key facts should be included: subject facts, authorization facts, transaction facts, delivery facts, and responsibility facts. Subject facts answer who participates and who has authority. Authorization facts answer who authorized, what the scope of authorization was, and whether authority was exceeded. Transaction facts answer what happened, whether the amount was consistent, and whether the path is traceable. Delivery facts answer whether assets, funds, rights, or obligations were delivered. Responsibility facts answer who approved, who executed, who reviewed, and who bears the consequences. From the perspective of the financial system, another key layer must be added: accounting facts. This is because in the banking system, "a transaction occurred" and "the accounts have been established" are not naturally equivalent. The transfer of assets and the completion of delivery of rights do not automatically mean that a formal accounting result under the bank has already been formed.

Only when transaction facts, delivery facts, and responsibility facts further enter the accounting structure and are formally recorded, confirmed, and made citable does the financial result truly enter the bank's result domain. In other words, the Transparent Bank must verify not only "whether the event occurred," but also "whether this result has been legally established under the bank." This step is precisely the institutional upgrade that the Transparent Bank makes to double-entry bookkeeping: it advances internal debit-credit balance into externally verifiable establishment. These key facts and accounting facts do not all need to be made public in plaintext. But through hashes, indexes, timestamps, state summaries, responsibility records, and necessary proof mechanisms, they must enter a verifiable structure. The key does not lie in "publicity." It lies in the fact that no key fact can be hidden, tampered with, or allowed to exist outside the structure for long.

VIII. The Transparent Bank Connects Not a Single Market, but Web3 and the Sovereign Financial Order

The strategic significance of the Transparent Bank does not lie in providing yet another entry point for digitalasset business. It lies in its first attempt to use a banking institutional structure to bring the programmability, composability, and machine-verifiable capabilities of the Web3 world together with the account system, payment and clearing, custody and rights confirmation, accounting assumption, regulatory interfaces, and legal responsibility of the sovereign financial system into one framework. The relationship between the Transparent Bank and the Web3 ecosystem is not simply to provide on-chain access, crypto-asset accounts, or digital-asset services. Rather, while realizing connection, it provides institutional assumption, risk constraint, and credit enhancement for them. It is neither the simple migration of a traditional bank onto a chain nor the institutional packaging of pure crypto finance. It is a new type of bank-like digital financial infrastructure for the Web3 era. The areas where it will first form advantages will also be those that rely most heavily on authenticity proofs, consistency of title, responsibility penetration, and replay ability of results, especially off-balance-sheet business, custody business, on-chain and off-chain mapping business, and institutional-grade digital-asset business. Stable coins are one of the most natural breakthrough points.

IX. Regulation Will Move from "Auditing Institutions" to "Verification Structures"

The proposal of the Transparent Bank also implies a profound change in regulatory logic. In the traditional model, the focus of regulation is whether rules have been implemented, whether verification institutions are trustworthy, whether reports are sufficient, and whether audits are valid. In the Transparent Bank model, regulation will increasingly turn toward whether the verification structure is established, whether key facts are consistent, and whether chains of responsibility can be replayed. The future focus of regulation should not be to restrict financial innovation itself, but to restrict unverifiable financial structures.

This does not mean that regulation will be replaced by technology. It means that regulation will gradually move from reliance on institutional statements and after-the-fact explanations toward precise governance based on structures, facts, and continuous verification. As a result, the boundary of financial innovation will also be redefined: as long as an innovation can enter a verifiable structure, it has the possibility of being absorbed by the institution; credit expansion that cannot enter a verifiable structure will find it increasingly difficult to obtain legitimacy and continuity.

X. Conclusion: From "Trust-Driven" to "Verification-Constraint-Driven"

What the Transparent Bank truly represents is not a more complex technological form of banking, but a new direction of financial civilization. Double-entry bookkeeping laid the internal accounting order of modern finance. Bitcoin's Public Credit Root provided external finality for modern finance. Chainless and hash anchoring provide an implementable balance among authenticity, performance, and privacy for real-world finance. The combination of reference chains and the banking system weaves these originally scattered verification capabilities into a verification constraint structure that cannot be bypassed for long.

The historical position of the Transparent Bank does not lie in whether it conducts a new type of digital financial business. It lies in the fact that, for the first time, it systematically proposes and attempts to practice this proposition: the key to future finance will no longer be only who operates the system, but whether any key financial result can be asserted, confirmed, or maintained for long outside a verification structure.

In this sense, the Transparent Bank is neither a simple extension of traditional finance nor a partial repair of crypto finance. It is a new financial structure connecting the internal accounting order laid down by double-entry bookkeeping, the Public Credit Root idea opened by Bitcoin, the technical flexibility provided by Chainless, and the institutional assumption capacity represented by the banking system. It truly marks the historical transition of finance from being "trust-driven" to being "verification-constraint-driven."

Chapter Seven
Transparent Finance: A Theory of Layered Verification for Key Financial Facts

— A Theoretical Explanation of Transparent Bank as an Institutionalized Form

This chapter is a further theoretical organization built on Chapter Five, "Transparent Bank: Not Ex Post Supervision, but a Banking Form of Continuous Verification" and Chapter Six, "From Double-Entry Bookkeeping to Transparent Bank: The Historical Evolution of Financial Constraint Structures." The previous two chapters mainly explain why the Transparent Bank can be established. This chapter further explains that the Transparent Bank is not an isolated banking innovation, but the institutional realization of the broader paradigm of Transparent Finance within the banking system.

The idea of Transparent Finance is not limited to banks. It also applies to stable coins, exchanges, custody, auditing, payments, corporate ledgers, public finance, and future financial infrastructure in the age of AI. This chapter necessarily overlaps to some extent with the previous two chapters, in order to explain at a higher level that Verifiable Finance is not merely a solution for the Transparent Bank, but a new constraint paradigm that can be extended to the entire financial system. The theoretical focus of this chapter has two points: first, authenticity is not optional, while visibility can be governed; second, complex financial activities can be decomposed into six categories of basic facts: subject facts, authorization facts, transaction facts, delivery facts, responsibility facts, and accounting facts. These two points have significance for financial institutions, and they also have the potential to be transformed into technical implementation, audit rules, and regulatory frameworks.

I. Definition of Transparent Finance: A Constraint Theory Centered on Key Financial Facts

Transparent Finance is not simply on-chain finance, nor does it mean making all financial data public. With the consistency of on-chain and off-chain record hashes and anchoring to a Public Credit Root as its technical support, and with the verifiability of key financial facts, traceability of responsibility, and governability of disclosure as its core, it may be called a theory of financial constraints through verification. The fundamental problem of modern finance is not merely centralization or decentralization, nor merely the greed, speculation, or governance failures of market participants. It lies in the fact that credit expansion has long lacked verifiable constraints. Credit can continue to expand within institutions, risks can continue to accumulate inside the system, while verification, auditing, and regulation often arrive only after the fact. In traditional finance, credit is mainly formed through the expansion of balance sheets, and its authenticity is indirectly maintained through internal accounts, periodic audits, regulatory reporting, and legal responsibility. In crypto finance, although on-chain assets have verifiability, key off-chain elements such as off-chain liabilities, custody arrangements, stable coin reserves, exchange positions, and customer rights still depend heavily on institutional statements and third-party endorsement. Therefore, the question Transparent Finance seeks to answer is not "whether institutions are still needed," but "how

institutional credit can accept verifiable constraints." It does not abolish banks, auditing, regulation, accounting, or legal systems. Instead, it requires key financial facts to enter structures that can be verified, traced, replayed, and disclosed in layers. Transparent Finance is proposed precisely in this sense: it is not a partial upgrade of tools, but a reconstruction of the logic of financial constraint.

II. Historical Coordinates: From Double-Entry Bookkeeping to Transparent Finance

If viewed from the history of financial civilization, Transparent Finance is not an isolated innovation. It should be understood as a further evolution of financial constraint structures after double-entry bookkeeping. The greatness of double-entry bookkeeping lies not only in forming debit-credit correspondence, but also in establishing internal constraints among economic facts through two-sided recording, allowing modern banks, companies, and fiscal systems to possess systematic internal accounting order for the first time. It solved a basic yet crucial problem: how accounts can become internally coherent within an institution. However, the constraints of double-entry bookkeeping still mainly remain within the internal ledger system of the institution. It can prove account balance, account classification, and accounting coherence, but by itself it cannot prove the continuous consistency of accounts with external facts, on-chain states, custody structures, regulatory records, and responsibility chains. In other words, double-entry bookkeeping solves "internal consistency within the accounts," but it does not solve "external verifiability outside the accounts." Transparent Finance does not negate double-entry bookkeeping. Rather, it advances further on that foundation: it extends internal accounting constraints into externally verifiable constraints, and advances debit-credit balance into continuous consistency constraints among on-chain and off-chain systems, accounts, responsibility, regulation, and results. If double-entry bookkeeping laid the internal accounting order of modern finance, then what Transparent Finance seeks is to establish a new external verification order on top of that foundation.

III. The First Principle of Transparent Finance: Authenticity Is Not Optional; Visibility Can Be Governed

Transparent Finance must distinguish between two concepts: authenticity and visibility. Authenticity is a foundational rule; visibility is a governance arrangement.Whether assets truly exist, whether ownership is consistent, whether a transaction occurred, whether delivery was completed, whether responsibility can be traced back, and whether accounts correspond to results are questions of authenticity. Who can see, what they can see, how much they can see, and under what conditions they can see are questions of visibility. The core principle of Transparent Finance is not "everything must be public," but "facts must enter a verification structure, while disclosure can be governed in layers." Key facts must be recorded, indexed, committed, anchored, and capable of review when necessary. But different subjects may obtain different degrees of information based on permissions, legal necessity, customer-protection principles, and requirements of commercial confidentiality.

This definition is extremely important, because it allows Transparent Finance neither to fall into crude transparency absolutism nor to retreat into the traditional logic of the black box. What it truly establishes is the following financial principle: authenticity is not optional, while visibility can be governed.

IV. Six Categories of Basic Facts: The Minimum Constraint Units of Transparent Finance

Transparent Finance cannot merely discuss abstract "data transparency" or "asset proof." It must decompose complex financial activities into several minimum verifiable units. These should at least include six categories of basic facts: subject facts, authorization facts, transaction facts, delivery facts, responsibility facts, and accounting facts. Subject facts answer: who participates, who has qualification, and who has subject status in the sense of accounts, identity, business, or regulation. They involve customer identity, institutional identity, account ownership, qualification conditions, and boundaries of participation. Authorization facts answer: where permissions come from, what the scope of authorization is, whether the signing status is established, and whether there is any overreach of authority, impersonation, abuse, or unauthorized operation. They must be carried jointly by authorization rules, signature records, permission logs, and operating procedures. Transaction facts answer: what transaction occurred, what the transaction conditions were, whether amount, path, time, and state are consistent, and whether there is duplicate bookkeeping, false trading, hidden misappropriation, or abnormal routing. Delivery facts answer: whether funds, assets, rights, or obligations have been delivered, whether the delivery object is correct, whether the delivery result is consistent with the transaction agreement, and whether there is any incomplete, revocable, failed, or disputed state. Responsibility facts answer: who made the decision, who executed it, who reviewed it, who approved it, who discovered the anomaly, and who bears the consequences. Responsibility facts must be supported jointly by authorization, signatures, operation records, approval records, anomaly records, and responsibility rules. Accounting facts answer: whether the relevant results have been legally established, formally recorded, confirmed, and made referable within the applicable accounting, bookkeeping, disclosure, and reporting structures. Accounting facts must be carried by the applicable accounting system, bookkeeping system, disclosure rules, and reporting structure, and cannot be replaced solely by hashes or on-chain proofs themselves. It is especially necessary to emphasize that hashes, timestamps, on-chain anchoring, or state proofs can prove that a certain record existed at a certain time, prove that history was not modified without a trace, prove that reference relationships exist among records, and maintain the consistency of record hashes within the reference chain. They cannot guarantee facts that have

not entered the reference chain, nor can they automatically prove that input data was already authentic before entering the reference chain. As common sense in cryptocurrency suggests, data that has not entered on-chain rules and record systems cannot obtain authenticity proof merely by relying on blockchain itself. It is first of all an evidentiary structure; confirmation still requires procedures and rules, just as Bitcoin transactions require confirmation. Anything outside the rules and outside the reference chain exceeds the direct coverage of Verifiable Finance.

V. The Six-Level Verifiability Model: From Record Existence to Institutional Acceptance

On top of the six categories of basic facts, Transparent Finance also needs to form a six-level verifiability model. This model advances Verifiable Finance from a purely technical proof into an evidentiary structure that can be accepted by accounting, auditing, regulation, and legal procedures. The first level is verification of record existence and integrity. It addresses whether a record existed at a specific time, whether it was later modified, whether hash commitments are consistent, and whether the reference chain is continuous. Public Credit Roots, timestamps, hash chains, and state summaries mainly function at this level. The second level is identity and authorization verification. It addresses who initiated, who signed, who approved, whether permissions matched, and whether authorization was valid. Digital signatures, permission rules, multiple approvals, identity authentication, and operation logs are the core materials at this level. The third level is transaction and delivery verification. It addresses what kind of transaction occurred, whether funds or assets were delivered, whether execution states were consistent, and whether the clearing path is traceable. Transaction facts and delivery facts form a corresponding relationship at this level. The fourth level is accounting and disclosure verification. It addresses whether financial results were correctly recorded, whether they entered the applicable bookkeeping structure, and whether they are consistent with customer-facing displays, internal statements, and external disclosure materials. Accounting facts must be carried by accounting and bookkeeping systems at this level. The fifth level is legal and rights verification. It addresses whether ownership, creditor rights, redemption rights, custody relationships, bankruptcy remoteness, priority of responsibility, and settlement finality have been established. Rights facts must be carried by law, contracts, regulatory rules, and judicial procedures, and cannot be replaced solely by technical proofs. The sixth level is risk, supervision, and institutional acceptance. It addresses the evidentiary basis for reserve quality, liquidity, concentrated redemption, capital impact, audit conclusions, regulatory inspections, and judicial judgment. Audit systems, regulatory rules, risk models, and legal responsibility systems together constitute this level. This six-level model shows that Verifiable Finance is not merely proving that "a certain hash exists on-chain." It must further answer: who is the subject corresponding to this record, whether authorization was valid, whether the transaction was completed, whether accounting was established, whether rights are recognized by law, and whether regulation and judicial procedures have conditions for acceptance. Only after entering this layered structure can Verifiable Finance move from technical verifiability toward institutional acceptability.

VI. Transparent Finance Does Not Equal On-Chain Finance

Transparent Finance does not equal on-chain finance. Public networks carry only part of the proof-anchoring capability. They cannot, and should not, carry all financial data, all customer information, and all business logic. Crypto systems have a boundary of trust: matters that enter on-chain records and on-chain rules can be publicly verified; off-chain facts that have not entered on-chain records cannot be verified merely by relying on blockchain itself. The core of Transparent Finance is to use mechanisms such as hash commitments, reference chains, audit proofs, and anchoring to Public Credit Roots to bring off-chain assets, off-chain ledgers, off-chain authorizations, and off-chain responsibilities into verifiable structures. In this way, data that originally existed off-chain obtains a verifiable historical position and proof relationship. But Transparent Finance also has boundaries. It mainly addresses the questions of whether history has been tampered with, whether proof exists, whether temporal order is credible, and whether records can mutually reference one another. It does not directly resolve the questions of whether input data is authentic, whether the audit is effective, or whether the judiciary will accept the evidence. The latter must be jointly completed by Transparent Bank rules, audit systems, accounting systems, regulatory rules, and legal responsibility systems. Therefore, Transparent Finance is not about moving all finance onto chains, nor about replacing financial institutions with technical proofs. It is about establishing stronger evidentiary structures, responsibility structures, and replay structures inside the financial system.

VII. From Verification Capability to Verification Constraint: The Dividing Line Between Transparent Finance and Ordinary Blockchain Finance

Ordinary blockchain finance often remains at the level where "data can be recorded" or "states can be queried." Transparent Finance requires the generation, transmission, and acceptance of credit to be embedded in verifiable structures. It includes at least three continuous layers. The first layer is the verification capability layer. The system already has the ability to hash-anchor key facts, record time sequences, and preserve tamper-resistant evidence. Bitcoin, distributed ledgers, and timestamp mechanisms all belong to this layer. It answers the question of "whether verification is possible." The second layer is the Chainless structural layer. The system does not require full data disclosure. Instead, through the separation of general ledgers and sub-ledgers, hash-index mapping, state anchoring, and verification logs, it brings key facts into the verification system while preserving off-chain efficiency, privacy protection, and

layered disclosure. It answers the question of "how verification can be performed in real business." The third layer is the verification constraint layer. Once reference chains, responsibility records, cross-system state references, and legal responsibility systems are included, verification is no longer merely an external plug-in capability; it becomes a precondition for the validity of business. The Chainless System solves "whether verification is possible," reference chains solve "whether verification can be bypassed," and rules together with responsibility systems solve "whether verification is mandatory." It is precisely at this layer that Transparent Finance truly diverges from ordinary blockchain finance: it does not remain at "having the ability to verify," but enters the institutional stage of "verification being mandatory."

VIII. The Relationship Between Transparent Bank and Transparent Finance

Under this theoretical framework, the Transparent Bank should not be understood merely as a new banking business model. It should be understood as the institutionalized realization of Transparent Finance within the banking system. The Transparent Bank is not the whole of Transparent Finance, but it is the representative organizational form of Transparent Finance within the licensed financial system. Its special value lies not in providing several digital-asset businesses, nor in building on-chain channels, but in the fact that the banking system naturally possesses institutional capabilities such as accounts, bookkeeping, accounting, payment and clearing, legal responsibility, and regulatory acceptance. These capabilities can transform Transparent Finance from a theoretical principle into a financial order that can operate over the long term, accept regulation, and bear legal responsibility. The meaning of the Transparent Bank is not "banking business on-chain," but to transform banks further from credit intermediaries into organizers of chains of authenticity, chains of responsibility, and chains of verification. It is the key vehicle by which Transparent Finance moves from theory to institution, and from open networks to sovereign financial order. This also shows that Transparent Finance is not limited to banks. Stable coins, exchanges, custody, auditing, payments, corporate ledgers, supply-chain finance, public finance, and financial infrastructure in the age of AI can all adopt the constraint principles of Transparent Finance to varying degrees. The Transparent Bank is only the most complete and most institutionalized path of implementation among them.

IX. Practical Significance: The Capacity of Transparent Finance to Reconstruct Existing Financial Structures

Transparent Finance is not an abstract idea, but a structural solution that can directly act on real pain points in finance. The problem of stable coins does not lie in their on-chain issuance volume, but in whether off-chain reserves, liabilities, and redemption capacity are continuously verifiable. Transparent Finance can advance the "trusted reserve model" into a "verified reserve model," so that reserves, liabilities, redemption capacity, and responsibility records enter a continuously verifiable structure. The problem of centralized exchanges does not lie in whether they are centralized, but in whether there is genuine consistency among assets, liabilities, positions, and customer rights. Transparent Finance can advance the "black-box position model" into an "asset-liability consistency verification model," making it impossible for exchanges to hide liabilities, misappropriate assets, or generate false positions for long periods without leaving a trace. The problem of custody and auditing does not lie in whether intermediaries exist, but in whether authenticity can only be maintained through periodic inspections. Transparent Finance can advance the "periodic audit model" into a "continuous verification model," allowing auditing to gradually move from ex post judgment toward rule-setting, proof certification, anomaly review, and dispute adjudication. The scenarios where Transparent Finance first produces institutional dividends are often not traditional on-balance-sheet lending, but off-balance-sheet business, custody business, on-chain and off-chain mapping business, institutional cooperation business, and customer self-custody reference structures. These areas depend most on proof of authenticity, consistency of rights, penetration of responsibility, and replay ability of results, and therefore most urgently need a new structure of verification constraints.

X. Regulatory Paradigm Shift: From "Whether It Is Trustworthy" to "Whether It Is Verifiably Established"

The true significance of Transparent Finance for regulation lies in pushing the object of regulation gradually from "institutional statements" toward "structural facts." Traditional regulation is mainly based on judgments of institutional trustworthiness, relying on reports, audits, and licenses; in essence, it verifies the institution. Transparent Finance introduces a new regulatory foundation: regulation based on structural verifiability. The core question is no longer merely "whether this institution is worthy of trust," but "whether this financial fact has been structurally established." Regulation will thus move from report-driven to verification-driven, and from ex post accountability to structural constraints. The focus of future regulation should not be to suppress financial innovation itself, but to restrict unverifiable financial structures. Verifiable financial innovation should be institutionally encouraged; unverifiable credit expansion should be institutionally constrained. Regulatory logic will gradually move from "listening to reports" to "checking structures," and from "judging whether an institution is trustworthy" to "judging whether a fact is verifiably established."

XI. Conclusion: Transparent Finance Is a New Financial Paradigm

If double-entry bookkeeping laid the internal accounting order of modern finance, if Bitcoin's credit-root idea provided proof of external temporal order and historical integrity, and if the Chainless System and hash anchoring provide a realistic balance among record verifiability, performance, and privacy, then what Transparent Finance seeks to establish on this series of

foundations is a new financial paradigm that advances verification capability into verification constraint, and advances internal accounting constraints into externally verifiable constraints. The value of Transparent Finance does not lie in replacing financial institutions with technical proofs, but in giving key facts, key responsibilities, and key results within financial institutions a more continuous, more verifiable, and more replayable evidentiary structure. In this sense, Transparent Finance inherits the accounting discipline established by double-entry bookkeeping, also accepts the institutional constraints formed by auditing, regulation, and legal responsibility, and further strengthens the inspectability of financial credit through digital proofs and external verification capabilities. Transparent Finance is neither an extension of traditional finance nor a simple evolution of public-chain finance. It is a new financial paradigm whose core constraint is verifiability. Its historical significance does not lie in whether it provides a new business model, but in the fact that it, for the first time, systematically proposes and attempts to practice the following proposition: the key to future finance is no longer merely who operates the system, but that no key financial result can be claimed, confirmed, or maintained for long outside a verification structure.

The Transparent Bank is the institutional realization of this new paradigm within the banking system.

XII. Postscript: Transparent Finance Has Arrived at the Right Time

Without AI, the Transparent Bank would very likely have remained only a theoretical conception. The reason is not that the direction is invalid, but that the complexity is too high: it needs to simultaneously handle financial accounts, accounting facts, reference chains, permission control, privacy layering, anchoring to Public Credit Roots, AI continuous auditing, legal responsibility, and regulatory interfaces. Such a system is difficult for a traditional software team alone to fully understand and implement. The emergence of AI has changed this. It significantly lowers the costs of complex system modeling, code generation, testing, auditing, documentation, and continuous monitoring, allowing the Transparent Bank to begin moving from a complex system imagined by a small number of people over a long period into a real engineering project that a small team can also advance. Transparent Finance has arrived at the right time. It requires the joint participation of talent from finance, AI, security, regulation, law, and systems engineering. Those who truly understand AI and financial infrastructure should see that Transparent Finance is not an ordinary project, but a systematic reconstruction of the constraint structure of future finance.

Chapter Eight Characteristics of Verifiable Finance: Implementing the Anchoring of Off-Chain Records to a Public Credit Root

— *Taking the Chainless System Concept as an Example*

I. The First Feature of Verifiable Finance: From Institutional Promises to Verifiable Facts

The foundation of finance is not information display, but the formation of credible facts. Account balances, asset ownership, transaction authorization, clearing results, income distribution, risk disclosure, and attribution of responsibility are all financial facts. The problem with traditional finance is not that there are no facts, but that the generation, confirmation, and evidentiary trace of facts depend heavily on internal institutional systems, making it difficult for external subjects to verify them in a timely, independent, and low-cost manner.

What Verifiable Finance must first do is transform financial facts into verifiable objects. So-called verifiability is not the same as full disclosure, nor does it mean that all data should be exposed on public networks. Its core lies in this: once a fact occurs, it should form verifiable signatures, hashes, timestamps, indexes, state proofs, or audit anchors; in the future, any subject with the corresponding permissions, credentials, or materials should be able to verify whether that fact exists, whether it is complete, and whether it has been modified. The Chainless System carries this logic through a two-layer structure of general ledger and subsidiary ledgers. The general ledger is responsible for system-side transparent indexes, hash summaries, coin indicators, transaction logs, and verification logs; subsidiary ledgers are responsible for complete user-side transaction histories and personal asset records. Its financial meaning is that the general ledger provides public verifiability, while subsidiary ledgers provide private-domain controllability. Thus, the Chainless System does not understand financial transparency as "everything is public," but transforms transparency into "key facts can be proven." This structure is closer to the real needs of financial business: customer privacy must be protected, transaction facts must be verifiable, system states must be auditable, asset flows must be traceable, and the formation of responsibility must be repayable. The first proposition of Verifiable Finance is this: the foundation of financial trust is shifting from institutional promises to verifiable facts. Institutional credit remains important, but the credibility of institutional credit should be supported by continuously generated verifiable records.

II. The Second Feature of Verifiable Finance: From Static Balances to Ownership Objects

Traditional account systems mainly express balances. A balance indicates how much asset exists under an account, but it does not sufficiently express asset origin, flow path, ownership status, restrictions, custody status, collateral status, income attribution, or responsibility relationships. An important change in Verifiable Finance is that assets can be expressed as digital objects that are identifiable, traceable, verifiable, and programmable. An asset is no longer merely a number in an account; it can carry origin, state, rules, rights, and responsibility. This is the core meaning of "asset objectification." Asset objectification does not mean simply turning assets into tokens. Rather, it allows assets to possess a structure that can be recognized by systems, constrained by rules, tracked by state, confirmed in ownership, and absorbed by responsibility. A mature digital financial object must answer at least five questions. First, where is the source of the asset? Assets do not appear out of nowhere. Their issuance, transfer-in, custody, locking, exchange, or generation process should have a verifiable chain of origin. Second, where is the ownership of the asset? To whom does the asset belong, and who has control rights, beneficial rights, or disposal rights? These must be recognized by the system and form verifiable records. Third, where is the state of the asset? Whether the asset is available, frozen, pledged, held in custody, locked, in delivery, or in another state should be continuously verifiable. Fourth, where are the restrictions on the asset? Whether the asset is subject to transaction restrictions, compliance restrictions, use restrictions, geographic restrictions, term restrictions, or risk restrictions must be expressed through rules.

Fourth, where are the restrictions on the asset? Whether the asset is subject to transaction restrictions, compliance restrictions, use restrictions, geographic restrictions, term restrictions, or risk restrictions must be expressed through rules.

Fifth, where is the responsibility for the asset? Around the issuance, transfer, custody, authorization, locking, anomalies, and results of an asset, the responsible subject and chain of responsibility should be identifiable. The coin indicator mechanism in the Chainless System reflects this asset-objectification thinking. Coin indicators are used to distinguish and manage different types of digital assets and represent the total amount of that category of asset; the aggregate of subsidiary-ledger records for each category of asset in the general ledger should remain consistent with the value of that asset's coin indicator. Internal transactions do not change the coin indicator, while external transfers in and out affect the corresponding total asset amount. This mechanism makes assets not merely passive records in accounts, but creates consistency checks among the general ledger, subsidiary ledgers, and total asset amounts. In other words, the Chainless System attempts to establish in digital space an asset-expression structure of "total amount - distribution - flow - verification." Balance records in traditional finance mainly answer "how much remains." Asset objects in Verifiable Finance further answer "where it came from, who controls it, what state it is in, whether it is restricted, whether it can be verified, and how responsibility is attributed." The second proposition of Verifiable Finance is this: the expression of financial assets is shifting from static balances to ownership objects. Assets must not only display quantity, but also express origin, state, restrictions, rights, and responsibility.

III. The Third Feature of Verifiable Finance: From Ex Post Audit to Process Verification

Auditing in traditional finance is mostly delayed. Institutions first keep accounts, process transactions, and disclose information; audit and regulation then inspect afterward. This model can operate in low-frequency and low-complexity financial environments, but in scenarios of high-frequency trading, cross-chain assets, stablecoin payments, automated contracts, and globalized flows, ex post audit faces the problems of high cost, slow response, and difficult penetration. The direction of Verifiable Finance is to advance auditing from ex post review to process verification. Transaction authorization, asset locking, state changes, result delivery, and log generation should all form verifiable traces as they occur. Auditing should no longer be merely an after-the-fact explanation; it should become a background mechanism within system operation. The Chainless System further strengthens this point through hash indexes, transaction logs, verification logs, and anchoring to the Bitcoin system. The financial meaning of anchoring to the Bitcoin system is not to replace business judgment, nor to replace the examination of asset authenticity, but to provide external tamper-resistant timestamps and ex post verifiable evidence for key ledger states. Here, the Bitcoin system assumes the role of a public timestamp credit root. The Chainless white paper proposes storing the hashes of transaction records in the Bitcoin system in order to establish a verifiable audit trail. This structure can be understood as "hash auditing." The system does not need to put all details publicly on-chain; instead, it forms hash anchors from key logs, states, and summaries. In future audits, the original logs can be used to recalculate hashes and compare them with the anchors, thereby confirming whether records existed, whether they were complete, and whether they were tampered with. These upgrades auditing from a low-frequency, delayed, sample-based external activity into a replayable, checkable, and continuously verifiable system capability. The third proposition of Verifiable Finance is this: financial auditing is shifting from ex post sampling to process verification. Auditing should no longer be merely report inspection, but should be embedded in the process of transaction, ledger, and state generation.

IV. The Fourth Feature of Verifiable Finance: From Asset Possession to Permission Governance

Asset control in traditional finance often appears as institutional possession, custody, registration, or transfer. Verifiable Finance changes this logic: asset control no longer depends only on who possesses the asset, but on who has signing authority, who can initiate authorization, who can jointly confirm, who can trigger transfer, who can restore access, and who can bear responsibility.
Therefore, the core of Verifiable Finance is not only asset management, but also permission governance. The Chainless System has distinct features in this regard. Its multi-signature, multi-backup wallet is intended to address private-key loss, multi-device verification, asset inheritance, and usability; the wallet is not only a signing tool, but also the carrier of user subsidiary ledgers, transaction histories, asset records, and disclosure control. At the same time, the Chainless System adopts TSS/MPC cross-chain protocols. Through key sharding and distributed signing, it prevents any single participant from independently controlling or misappropriating user assets. In this structure, asset security no longer relies on a single private key or a single institution, but forms checks and balances through threshold signatures, multi-party collaboration, device distribution, permission layering, and signature records. The Chainless white paper explains that under the TSS mechanism, no participant holds the complete private key, and the complete private key is never reconstructed or centrally held; signing is jointly generated through multi-party computation by holders of key shares that meet the threshold. This marks a change in the boundary of financial security: from "who keeps custody of the asset" to "who controls permissions, who participates in signing, who triggers actions, and who bears responsibility." TSS/MPC and multi-signature wallets are not merely technical tools; they are foundational structures for checks and balances of power and

allocation of responsibility in digital space. They decompose "control rights" into multiple verifiable, authorizable, and traceable permission actions, so that asset transfer no longer depends on single-point control. The fourth proposition of Verifiable Finance is this: financial control is shifting from possession and custody to permission governance. Signatures, thresholds, multi-signatures, backups, recovery, and authorization will become important structures of financial security.

V. The Fifth Feature of Verifiable Finance: From Exposed Transparency to Layered Disclosure

Public-chain finance has long faced a basic contradiction: the higher the transparency, the stronger the exposure of privacy; the stronger the privacy protection, the harder audit penetration becomes. Traditional public chains expose large volumes of transactions, addresses, balances, and interaction behavior on public networks. Although this improves verifiability, it also brings wealth exposure, transaction-path analysis, leakage of commercial privacy, and user-security risks. Mature Web3 finance should not pursue exposed transparency, but verifiable transparency. That is: facts must be verifiable, while disclosure should be layered according to subject, permission, scenario, and necessity. The general-ledger/subsidiary-ledger structure of the Chainless System is precisely a response to this contradiction. The general ledger assumes public-side functions, preserving summaries, indexes, coin indicators, transaction logs, verification logs, and external anchoring. It is used for total-asset verification, system-state verification, hash anchoring, and audit entry points. The responsibility of the general ledger is not to peer into all transaction details, but to ensure that key facts are verifiable, key states are checkable, and key records are traceable. Subsidiary ledgers assume private-domain controllability, preserving complete transaction histories, user asset details, authorized disclosure materials, and original evidence. Subsidiary ledgers are controlled by users and can be managed for disclosure according to different scenarios. The Chainless white paper proposes that subsidiary ledgers exist in the form of multi-signature, multi-backup secure wallets, form reconciliation relationships with the general ledger, and preserve complete user transaction histories. From this, an important principle of Chainless finance can be summarized: facts must be verifiable; disclosure can be selected in layers. This means that facts such as asset existence, transaction occurrence, state changes, authorization establishment, and result delivery cannot be absent; but customer identity, complete transaction histories, transaction details, asset portfolios, and risk profiles should not be public to the entire network by default. Verifiability solves the problem of trust, while layered disclosure solves the problem of privacy. Only their combination can form a financial-grade mechanism of verifiable transparency. The fifth proposition of Verifiable Finance is this: financial transparency is shifting from full public disclosure to layered disclosure. Publicity is not the objective; verifiability is the objective. Privacy is not an obstacle; controlled disclosure is the balance point between financial compliance and user protection.

VI. The Sixth Feature of Verifiable Finance: From On-Chain Execution to a Financial Operating System

Early Web3 finance mainly revolved around smart contracts and emphasized "code as rules." This model is suitable for standardized, automated, formally expressible transaction structures, but financial activity is not always simple condition-triggering. Real finance also includes guarantees, witnessing, default, disputes, inheritance, fraud, recourse, risk disclosure, and complex rights arrangements. Therefore, Web3 finance cannot remain at the level of a single smart-contract layer; it must move toward the level of a financial operating system. It requires ledgers, accounts, wallets, permissions, payments, clearing, cross-chain mechanisms, auditing, disclosure, disputes, and application interfaces to operate together. The contract account design of the Chainless System reflects this direction. A contract account is not merely a code container, but a business container capable of carrying account states, asset states, permission rules, execution logic, and financial applications. It can bring payments, stable coins, cross-chain assets, transaction matching, lending, derivatives, aggregation, big-data analysis, and IoT payments into a unified financial operating environment. This shows that the Chainless System is not merely attempting to become another public chain. It is attempting to become an operating-system kernel capable of carrying the operation of financial business. The Chainless white paper also positions it as a financial system architecture that integrates Web2 user experience with verifiable autonomy, and proposes scenarios such as contract accounts, DeFi applications, stable coin issuance, cross-chain payments, and connection with traditional finance. Its theoretical significance lies in this: the next stage of Verifiable Finance is not merely to improve public-chain performance, but to reconstruct the operating layer of financial business. The chain is no longer the only center, but part of the credit root, evidence-preservation layer, asset network, and cross-chain interface. The sixth proposition of Verifiable Finance is this: financial infrastructure is shifting from a single-chain network to a financial operating system. What future Verifiable Finance needs is not only public-chain performance, but the overall coordination of ledgers, accounts, wallets, payments, cross-chain mechanisms, verification, disclosure, applications, and responsibility mechanisms.

VII. The Financial Characteristics of the Chainless System: Inherited Innovation

The theoretical value of the Chainless System lies in proposing a path of inherited innovation. It does not deny the efficiency of Web2, nor does it deny Bitcoin's machine trust, nor does it abandon verifiable data sovereignty. On the contrary, it attempts to combine the three: using Web2 user experience and processing efficiency to support high-frequency financial activities, using the tamper-resistance of the Bitcoin system to serve as a public timestamp credit root, and using Web3 asset autonomy and data sovereignty to reconstruct the relationship between users and financial systems.

The characteristics of Chainless finance can be summarized in six aspects. First, financialization of ledgers. The general ledger, subsidiary ledgers, coin indicators, transaction logs, and verification logs together constitute a verifiable ledger system. Second, efficiency of payments. Through non-competitive ledgering and indexing mechanisms, it attempts to achieve processing efficiency close to that of Web2 financial systems.

Third, asset objectification. Through coin indicators, subsidiary-ledger records, and hash indexes, it expresses total asset amounts, distribution, origin, and flow states.

Fourth, permission governance. Through multi-signature, multi-backup wallets and TSS/MPC, asset control is transformed into governance of signatures, thresholds, authorization, and responsibility.

Fifth, internalization of auditing. Through hash indexes, verification logs, and Bitcoin anchoring, audit capability is embedded into the process of system operation.

Sixth, layering of disclosure. Through the general-ledger/subsidiary-ledger structure, a balance is formed between verifiability of facts and protection of privacy.

Together, these six characteristics show that the Chainless System is not an ordinary public-chain replica, but a verifiable financial operating-system kernel reconstructed around the ledgering, asset, permission, audit, disclosure, and application need of financial activities.

VIII. The Structural Transformation of Verifiable Finance

Verifiable Finance is not a single technological upgrade, but a systemic transformation in the production mode of financial trust, the expression of assets, the method of auditing, the logic of control, the disclosure mechanism, and the operating carrier. It is reflected in at least six structural transformations.

First, from institutional promises to verifiable facts. Financial credit no longer relies only on institutional statements, brand reputation, and ex post audits, but should rely on continuously generated fact records that can be reviewed.

Second, from static balances to ownership objects. Assets are no longer merely numbers in accounts, but digital financial objects with origin, ownership, state, restrictions, and responsibility.

Third, from ex post audit to process verification. Auditing is no longer merely ex post sampling and report inspection, but should be embedded in the process of transaction, authorization, state change, and result confirmation.

Fourth, from asset possession to permission governance. Asset security no longer depends only on who possesses the asset, but on signing authority, thresholds, authorization paths, recovery mechanisms, and responsibility records.

Fifth, from exposed transparency to layered disclosure. Facts must be verifiable, but disclosure should be governed according to subject, permission, scenario, and necessity.

Sixth, from on-chain execution to a financial operating system. Future Verifiable Finance requires the overall coordination of ledgers, accounts, wallets, payments, cross-chain mechanisms, verification, disclosure, applications, and responsibility mechanisms.

These transformations together show that the mainstreaming of Web3 finance is not merely about improving on-chain throughput, reducing transaction fees, or increasing the number of applications. It must reconstruct how financial facts are generated, verified, disclosed, and made into responsibility.

IX. A Graphical Explanation of the Logic of Verifiable Finance

To present the theoretical structure of Verifiable Finance more clearly, four sets of logical diagrams can be used to summarize the essence of Verifiable Finance and the characteristics of the Chainless System.

First, the trust paradigm: from institutional promises to verifiable facts. The traditional chain is “institutional statement - internal ledger - ex post audit or regulatory endorsement - user trust.” The verifiable chain is “financial action - signature, hash, or timestamp - process verification and responsibility traces - continuously generated trust.” Through the general ledger/subsidiary ledgers, the Bitcoin public timestamp credit root, hash indexes, and verification logs, the Chainless System transforms financial actions into verifiable facts.

Second, the two-layer ledger: the combination of public verifiability and private-domain controllability. The general ledger assumes public-side functions, preserving summaries, indexes, coin indicators, transaction logs, verification logs, and external anchoring, ensuring total-asset verification, state verification, and audit entry points. Subsidiary ledgers assume private-side functions, preserving complete transaction histories, original evidence, user asset details, and authorized disclosure materials, protecting data sovereignty and supporting controlled verification. This structure forms a mechanism of financial transparency that is “verifiable but not exposed.”

Third, asset objectification: from balances to five-dimensional financial objects. A mature digital financial object contains at least origin, ownership, state, restrictions, and responsibility. Coin indicators, subsidiary-ledger records, hash indexes, and verification logs in the Chainless System constitute the underlying support for this expression structure.

Fourth, permission governance: from asset custody to signature checks and balances. The traditional model is centralized

institutional control, customer dependence on institutional performance, and ex post accountability; the Chainless model uses multi-signature wallets, TSS/MPC threshold signatures, distributed key shares, and multi-party collaborative confirmation to realize technical checks and balances of power. Asset security no longer depends on a single private key or a single institution, but realizes distributed control through signing authority, thresholds, authorization paths, and responsibility records.

X. Conclusion: The Institutionalized Expression of Verifiable Finance

The significance of the Chainless System does not lie in becoming another traditional public chain, but in providing an engineering kernel for Verifiable Finance. Through the general ledger/subsidiary ledgers, coin indicators, the Bitcoin public timestamp credit root, TSS/MPC, multi-signature multi-backup wallets, and contract accounts, it transforms the verifiable principles of Web3 into a financial operating system capable of carrying payments, assets, permissions, auditing, disclosure, and responsibility.

The Chainless System is not replacing banks. It is providing banks with a tamper-resistant, verifiable, and traceable operating capability.

The core proposition of Verifiable Finance can be condensed into three sentences: financial trust is no longer produced only by institutional promises, but is continuously generated by verifiable facts; financial assets are no longer merely balances, but digital objects whose origin, state, ownership, restrictions, and responsibility can be proven; financial transparency is no longer equivalent to full disclosure, but is institutionalized transparency in which facts are verifiable and disclosure can be layered.

Based on this proposition, the mainstreaming path of Verifiable Finance is not simply to pursue more assets on-chain, more transactions on-chain, or higher on-chain throughput. Rather, it is to establish a set of financial infrastructure capable of continuously answering the following questions: whether a fact exists, whether a record is complete, whether an asset is real, whether ownership is clear, whether authorization is established, whether a state is verifiable, whether disclosure is appropriate, and whether responsibility is traceable.

The financial characteristics of the Chainless System unfold around precisely these questions: the general ledger provides public verifiability, subsidiary ledgers provide private-domain controllability, coin indicators provide total-asset verification, anchoring to the Bitcoin system provides a public timestamp credit root, TSS/MPC and multi-signature wallets provide permission checks and balances, and contract accounts provide financial-application carrying capacity. Ultimately, Verifiable Finance can be summarized as a new paradigm of financial infrastructure: replacing mere promises with verifiable facts, replacing static balances with ownership objects, replacing delayed audits with process verification, replacing single-point control with permission governance, replacing exposed transparency with layered disclosure, and replacing single on-chain execution with a financial operating system.

This is the deep transformation that Verifiable Finance must complete in moving from concept to mainstream application.
Facts must be verifiable; disclosure can be selected in layers. This principle allows Verifiable Finance to be compatible with the regulatory requirements of licensed finance, such as KYC, AML, and customer protection, while preserving the verification advantages brought by decentralized trust structures. This leap from “on-chain execution” to a “financial operating system” is the necessary path for digital finance to move toward mainstream and institutional-grade application.

Part III
Satoshi Nakamoto Thought and Transparent Coordination Institutions

Chapter Nine
The Satoshi Nakamoto Question Is Not Gossip

— The Key to Strengthening the Certainty of the Public Credit Root

If we acknowledge that the Public Credit Root is the foundation of Verifiable Finance, then the certainty of the Bitcoin system is no longer only an internal question for the cryptocurrency industry. It becomes a key question for whether the financial infrastructure of the future can be established. As a system of issuance and an open ledger, Bitcoin's technical coordination has so far been broadly successful. Relying on open-source code, node consensus, miner competition, community discussion, and market choice, it has passed through more than a decade of major tests. But once the Bitcoin system is further understood as the Public Credit Root of Verifiable Finance, the technical coordination mechanisms of the past may no longer be sufficient to address more complex uncertainties in the future. Quantum-computing risk, early dormant bitcoins, the security of old addresses, long-term governance vacuum, and institutional conflicts that may arise after Bitcoin's financialization have all moved beyond the scope of purely technical maintenance.

That Bitcoin has reached this point is a miracle in both financial history and technological history. Precisely for this reason, we should examine more carefully the ideas, methods, and experience through which it was formed: which principles must be preserved, which mechanisms once worked, which problems were temporarily set aside, and which uncertainties may reappear in the second half. Summarizing these experiences is not meant to weaken Bitcoin, but to strengthen the certainty of the Public Credit Root. Therefore, the Satoshi Nakamoto question is not gossip. It is a question about the source of the credit root. To discuss Satoshi is not to manufacture news, stimulate the market, or consume privacy. It is to understand why the Bitcoin system could be established, why it was able to form a Public Credit Root without a central institution, and how, after Bitcoin enters its second half, its institutional certainty as a Public Credit Root can be strengthened without destroying its ownerless and open character. This also explains a real paradox: if the Public Credit Root is so important, why do many institutions still tend to build their own chains, consortium chains, or closed ledgers instead of directly referencing the Bitcoin system? The root cause is not merely technical prejudice or inertia of interest, but the fact that certainty has not yet been fully understood and institutionalized. Major finance will not incorporate a system into its core infrastructure merely because that system is technically advanced. It must first confirm that the credit root is sufficiently stable, interpretable, coordinatable, clear in responsibility boundaries, and capable of long-term institutional absorption.

Negative news, identity mysteries, governance vacuum, quantum risk, and early-coin issues all amplify uncertainty. Only when the certainty of the Public Credit Root is reinterpreted and institutionalized can the Bitcoin system move from an asset narrative into a financial-infrastructure narrative. These are two completely different levels: the former remains within an asset-price narrative, while the latter enters a financial-infrastructure narrative. What truly determines the future is not the asset price itself, but whether a Public Credit Root can be formed that is adopted by the modern financial system. Many people fail to see this precisely because they remain constrained by short-term prices, individual technologies, and the existing structure.

I. Bitcoin Cannot Rely on Myth Forever

The cryptocurrency industry has an extremely special phenomenon: this industry was created by Satoshi Nakamoto, yet who Satoshi Nakamoto is has long remained within myth, mystery, and even taboo. In the early stage, this condition had historical rationality. Satoshi Nakamoto's withdrawal allowed Bitcoin to escape founder control, avoid corporatization, leader-centered operation, and administration, and gave Bitcoin the spiritual force of an ownerless system. Precisely because there was no founder who could be directly controlled by governments, capital, courts, media, or market sentiment, Bitcoin could more easily be understood as a set of open rules rather than the product of a person, a company, or an interest group. But the problem is that a system that already affects the global financial order, involves trillions of dollars in assets, and touches national regulation, monetary theory, and future financial infrastructure cannot rely forever only on myth. If the Satoshi question is merely the identity puzzle of "who invented Bitcoin," it can indeed easily descend into gossip. But if we understand that what Satoshi truly attempted to establish was a new financial order, then this question has serious significance in intellectual history, institutional history, and financial history. Because Satoshi Nakamoto is not merely a name. Satoshi Nakamoto represents the intellectual source, institutional source, and credit source of Bitcoin. To understand Satoshi is not to consume a person's privacy, create market news, satisfy public curiosity, or destroy Bitcoin's decentralization. To understand Satoshi is to answer a deeper question: where does the cornerstone of this new financial system called Bitcoin come from? Which intellectual traditions does it inherit? Why was it designed in this way? What problems did it solve, what problems did it leave behind, why did the first half require withdrawal, and why does the second half need to be reinterpreted? This is the true meaning of the Satoshi Nakamoto question. Satoshi's withdrawal made Bitcoin's first half possible. It allowed Bitcoin to avoid being directly tied to personal will, corporate governance, or government regulation. But after Bitcoin enters its second half, the problem changes. It is no longer merely an open issuance system or a digital asset network; it is increasingly understood as the Public Credit Root of the future Verifiable Finance system. A Public Credit Root requires an extremely high degree of certainty, and certainty cannot be built forever upon myth, taboo, and matters that cannot be discussed. Therefore, restoring Satoshi from myth to history is not to hand Bitcoin back to an individual. It is to return Bitcoin's intellectual source, institutional logic, and future coordination problems to a framework that can be discussed, understood, and verified. Only in this way can the Bitcoin system move from the success of an ownerless system toward the maturity of a Public Credit Root.

II. What Satoshi Truly Created Was Not Blockchain, but the Institutional Prototype of a Public Credit Root

Many people say that Satoshi invented blockchain. This statement is not accurate, or at least too simple. Blockchain as a technical arrangement of hash linking, time ordering, and appended records had already appeared in earlier timestamp and cryptographic research. To summarize Satoshi's contribution as "blockchain" greatly undervalues it. What Satoshi truly created was a Public Credit Root that does not depend on a state, a bank, a company, a clearing institution, or a database administrator, but can operate continuously, be openly verified, resist tampering, and form global consensus.

The title of the Bitcoin white paper is A Peer-to-Peer Electronic Cash System. Its core problem was not how to build a new database, but how to realize electronic cash without a trusted third party, especially how to prevent double spending. This means that Satoshi's problem consciousness was financial from the beginning, not merely technical. He was not trying to solve "how to write a chain," but rather: without a bank, who confirms payment? Without a clearing institution, who maintains the ledger? Without a central issuer, who constrains the money supply? Without a trusted third party, who prevents double spending? Without sovereign credit, who provides final trust?
The answer of the Bitcoin system is: do not trust a center; verify a set of public rules. This is the birth of the Public Credit Root. Before Bitcoin, human financial credit mainly came from states, banks, courts, central banks, clearing institutions, and large intermediaries. After Bitcoin, humanity for the first time possessed a machine credit structure that could be jointly verified by a global open network. Satoshi was not an ordinary blockchain engineer, but the creator of the institutional prototype of the Public Credit Root. For this reason, the Satoshi question cannot be treated only as an identity puzzle. Only by understanding Satoshi's real contribution can one understand that he opened not a technology industry, but a new financial era.

III. Why the Question of Satoshi's Identity Has Long Been Misread

One reason Satoshi's identity has long been misread is that the industry has mistaken anonymity for something that must never be studied. In the early period, Bitcoin needed Satoshi to withdraw. If Satoshi had remained on stage, Bitcoin could easily have been understood as a founder project, a software company, a political movement, or even a system that could be changed by personal will. Withdrawal protected Bitcoin's ownerless character, and this was an important condition for the success of Bitcoin's first half. But withdrawal does not mean that the intellectual source is unimportant. A system can be ownerless at the operational level, but it must have a source at the level of intellectual history. A protocol can be free from founder control, but its design logic must still be explained. A financial system may have no chairman, but it cannot have no theoretical history. A civilizational invention may escape personal power, but it cannot escape its intellectual source. This is why the Satoshi question has become important again today. Cryptocurrency is no longer only a geek experiment or a niche asset. Bitcoin,

Ethereum, stable coins, exchanges, ETFs, national regulation, AI finance, Transparent Banks, and Public Credit Roots have all pushed cryptocurrency into the structure of mainstream finance. At this stage, it is no longer enough for the industry to say only that "who Satoshi is does not matter." This is not because Satoshi must return to control Bitcoin, but because cryptocurrency must understand where it came from in order to know where it should go next. Therefore, the Satoshi identity question must escape two misreading's: one is reducing it to market gossip; the other is making it an absolute taboo, as if any research would destroy Bitcoin. The former underestimates Bitcoin's intellectual depth, while the latter keeps the Public Credit Root trapped in mythological explanation.

IV. Searching for Satoshi: Not Curiosity, but Reconstruction of an Intellectual Chain

Who Satoshi is is of course an identity question. More importantly, however, it is a question of an intellectual chain.

What we truly need to ask is: who first understood the difficulty of digital cash? Who truly understood the political meaning of the cypherpunks? Who understood cryptography, software engineering, monetary design, and anonymous collaboration? Who could synthesize the intellectual traditions of Wei Dai, Nick Szabo, Adam Back, and others into a system that could run? Who understood both the cryptographic ideal of freedom and the engineering details of implementation? Who had enough ability to write the Bitcoin system and enough restraint to withdraw before and after success? These questions are more important than looking only at a name. What truly matters is not to write the research as "I found a certain person," but to write it as: how the intellectual source of Bitcoin was formed. The reconstruction of this intellectual chain has value in itself. It forces the industry to face one question seriously: Bitcoin is not a price chart, not an ETF product, not a mining industry, not a speculative asset, and not a simple replacement for "digital gold." Bitcoin is the result of decades of cryptography, digital cash, libertarian financial thought, and engineering synthesis. This source must be explained clearly. Only by explaining this source can we understand why Bitcoin could become a Public Credit Root, and why it needs a stronger certainty structure in its second half.

V. The Real Historical Thread of Bitcoin: From Electronic Cash to Public Credit Root

If Bitcoin history is summarized in one sentence, it is not "the invention of a coin from nothing." More accurately, Bitcoin history is an evolutionary line from electronic cash, to machine credit, and then to the Public Credit Root. The first stage was the electronic cash of the Chaum era. The core question was private payment: how could electronic payment protect user privacy like cash? The second stage was the politicized cryptography of the cypherpunk era. The core question was how individuals could use cryptographic technology to escape excessive control by states, companies, and centralized institutions. The third stage was the age of Hashcash and proof of work as verifiable cost. The core question was how to make network behavior bear real cost, thereby preventing abuse and forming a machine-verifiable competitive mechanism. The fourth stage was the distributed-money thought of b-money and Bit Gold. The core question was how to form monetary creation, ownership records, and scarcity without a central institution. The fifth stage was Satoshi's Bitcoin era. The core question was how to synthesize these ideas into a peer-to-peer electronic cash system that needed no trusted third party and could actually run. This historical line shows that Bitcoin was not an accidental technological outbreak, but the final combination of a long-unresolved problem: Chaum proposed private cash, the cypherpunks proposed cryptographic freedom, Wei Dai proposed distributed anonymous money, Nick Szabo proposed digitally scarce assets, Adam Back provided the proof-of-work idea, Hal Finney and other early participants advanced testing and dissemination, and Satoshi completed the system synthesis. Satoshi's historical position lies here: he did not merely write isolated technology into code. He transformed the decades-long unfinished problem of digital cash, for the first time, into a running Public Credit Root.

VI. The Successful Experience of the First Half: Withdrawal, Minimalism, and Technical Coordination

The success of Bitcoin's first half cannot be attributed simply to price appreciation, nor only to open-source code. Its true success lies in forming a set of coordination experiences that allowed long-term operation in an ownerless state. First, Satoshi's withdrawal reduced the risk of personal control. Without a founder standing above the system, Bitcoin became more like a set of rules than a corporate product. Second, Bitcoin's core rules remained extremely simple. Supply cap, issuance schedule, proof of work, node verification, difficulty adjustment, and the longest-chain rule together formed a relatively stable institutional boundary. The lower the complexity, the stronger the certainty of the Public Credit Root. Third, technical coordination played an important role in the first half. Developer discussion, node choice, miner game dynamics, user consensus, and market feedback allowed Bitcoin to be maintained and evolve without a central administrator. Fourth, the community formed a certain self-correction capacity during key disputes. Bitcoin's historical disagreements, scaling disputes, and route competition show that although the system has no formal constitution, it is not completely without coordination mechanisms. It maintained continuity of core rules through public discussion, code choice, node operation, and market judgment. These experiences are very important. They show that the Public Credit Root is not incapable of coordination, but that coordination must be conducted on the premise of not destroying ownerlessness, open verification, or the stability of core rules.

VII. Uncertainty in the Second Half: The Credit Root Cannot Be Maintained Only by Old Mechanisms

After Bitcoin enters its second half, however, the problems change. The first half mainly proved "whether Bitcoin could survive"; the second half must answer "whether Bitcoin can become the Public Credit Root of future finance." These are different questions. As an issuance system, Bitcoin has already proven its vitality. As a Public Credit Root, it will face more complex institutional challenges.

First, there is quantum-computing risk. Regardless of when the risk truly approaches, it will force Bitcoin to confront old addresses, security migration, user choice, and system coordination.

Second, there are early dormant bitcoins and old-address issues. These assets have remained unmoved for a long time. They involve the sanctity of property rights, key security, historical legacy, and market expectations. How these issues are discussed is itself a test of the institutional maturity of the Public Credit Root.

Third, there are institutional conflicts brought by financialization. ETFs, institutional custody, stablecoins, bank access, and regulatory frameworks will move Bitcoin further from its original geek network into sovereign financial systems and institutional balance sheets.

Fourth, there are new requirements brought by AI and machine finance. If the Bitcoin system is used in the future as the final credit anchor of Verifiable Finance, it will face not only human users but bank systems, AI audit systems, machine agents, and cross-institutional clearing networks. None of these questions can be fully solved by ordinary code maintenance. They require a more transparent, more prudent, and more bounded coordination mechanism. The old technical coordination remains important, but it is no longer enough. The certainty of the Public Credit Root must be further institutionalized on the basis of the successful experience of the first half.

VIII. "Inviting Satoshi" Does Not Mean Giving Him Power, but Letting the Intellectual Source Participate in Building Certainty

When many people hear "invite Satoshi," their first reaction is fear. They worry that Satoshi's appearance will centralize Bitcoin, that his words will affect prices, that he controls early coins, that he will become a new authority, and that Bitcoin will shift from an ownerless system into a founder system. These concerns have a real basis. Therefore, "inviting Satoshi" must never be understood as letting an individual take power again. Its real meaning is: invite the intellectual source, not a dictator; invite historical explanation, not administrative control; invite financial theory, not a market operator; invite the direction of the second half, not founder worship. In Bitcoin's first half, Satoshi's withdrawal was an advantage. In cryptocurrency's second half, the return of Satoshi's thought may become one condition for raising the certainty of the credit root. Because the second half is no longer merely "can Bitcoin survive." The questions of the second half are: how does the Public Credit Root serve future finance? How should quantum risk be coordinated? How should early-coin issues be discussed? How can stable coins become verifiable? How can Transparent Banks be established? How should financial security be designed in the AI era? How can Bitcoin and Ethereum move from asset systems into infrastructure for Verifiable Finance? These questions require intellectual sources and financial theory, not merely market slogans. Even without holding power, Satoshi can serve as an intellectual source, historical witness, and special moral role within a transparent coordination mechanism, helping the market understand the boundaries, principles, and direction of the Bitcoin system's second half. Therefore, inviting Satoshi is not to destroy Bitcoin. It is to move cryptocurrency from myth narrative to theoretical narrative, from identity taboo to institutional discussion, and from the success of an ownerless system to the maturity of a Public Credit Root.

IX. The Satoshi Question Ultimately Points to Verifiable Finance

Why, after discussing Transparent Banks, Public Credit Roots, the lowest ledgering cost, and open-source verification, must we return to Satoshi? Because Satoshi is the source of all these matters. The concept of the Public Credit Root begins with the Bitcoin system. The principle that verification has priority begins with the Bitcoin system. The logic of the lowest ledgering cost begins with the Bitcoin system as final anchor. The external credit root of the Transparent Bank also begins with the Bitcoin system. The first foundation of Verifiable Finance remains the Bitcoin system created by Satoshi. Therefore, the Satoshi question is not a question of the past, but a question of the future. It is not as simple as asking "who invented Bitcoin." It truly asks: who opened the first door for humanity to move from trusting institutions to verifying rules? What is the intellectual source of this system? Why did it not complete Verifiable Finance? How should its second half unfold? How can the Public Credit Root enter Transparent Banks and Verifiable Finance? How can Bitcoin move from asset myth into financial institution? This is the value of the Satoshi question. Its endpoint is not identity news, but Verifiable Finance; not price volatility, but certainty of the credit root; not a return to personal authority, but a clearer understanding of the source, boundaries, and future of a new financial institution. Conclusion: From Searching for One Person to Strengthening the Certainty of the Public Credit Root If handled by the media, the Satoshi question easily becomes identity news. If handled by the crypto community, it easily becomes a price risk. If handled by conspiracy theories, it easily becomes a curiosity story. If handled by legal cases, it easily becomes an evidentiary dispute. But if handled through financial intellectual history and institutional history, it becomes another question: where is the intellectual source of cryptocurrency? Why did Bitcoin appear? Why is it not an ordinary technological

product? Why can it become a Public Credit Root? Why has it not yet completed a commercial financial system? Why does it need Transparent Banks, Verifiable Finance, and new institutional absorption in the AI era?

This is why we discuss Satoshi again. Searching for Satoshi is not to hand Bitcoin back to a person. It is to liberate cryptocurrency from identity puzzles, coin-price narratives, and technical slogans, and place it again within financial history, intellectual history, and institutional history.

Bitcoin's first half needed a withdrawn Satoshi. Cryptocurrency's second half needs a Satoshi who is understood. Satoshi should not be only a myth. Satoshi should become the intellectual entrance through which cryptocurrency enters a new financial civilization.

More fundamentally, the true meaning of the Satoshi question is to help the Bitcoin system move from a successful ownerless issuance system toward a mature Public Credit Root. Only when the source, principles, boundaries, and coordination methods of the Public Credit Root are more clearly understood can the Bitcoin system obtain a higher degree of certainty in the age of Verifiable Finance.

Chapter Ten
Why Satoshi Nakamoto Must Be Restored from "God" to "Human"

Chapter Nine argued that the Satoshi Nakamoto question is not gossip, but the key to strengthening the certainty of the Public Credit Root. This chapter further explains why Satoshi must be restored from "god" to "human." This does not mean lowering Satoshi's historical position, nor letting a person take power again. It means releasing Bitcoin's intellectual source, institutional logic, and second-half problems from mythological narrative, and placing them again within the frameworks of financial history, institutional history, and Verifiable Finance.

After Bitcoin enters its second half, the objective has changed. The key question of the first half was whether Bitcoin could survive without a central bank, without corporate governance, and without continuous founder management. The key question of the second half is whether the Bitcoin system, while maintaining ownerlessness and openness, can perform the function of a Public Credit Root and become important infrastructure for Verifiable Finance, Transparent Banks, and the future machine-credit system. Therefore, Satoshi must be restored from "god" to "human." Only in this way can the industry move beyond identity puzzles, mysterious narratives, and taboo psychology, and truly understand why Bitcoin could be established, why the Public Credit Root emerged, and how the Bitcoin system should strengthen its certainty in the era of financialization, institutionalization, and AI.

I. The Mythologized Satoshi Once Protected Bitcoin's First Half

Every great system needs a narrative in its early stage. In its early days, Bitcoin had no state endorsement, no bank support, no corporate credit, no mature market, no regulatory recognition, and no participation by mainstream financial institutions. It faced doubt, ridicule, attack, misunderstanding, and enormous uncertainty. In this situation, Satoshi's anonymity and withdrawal formed a very powerful narrative structure. First, it made the Bitcoin system appear ownerless. With no owner, there was no single point of control. With no founder ruling the system, no personal authority stood above the rules. With no corporate ownership, shareholder interest could not override the protocol. With no management layer, there was no centralized governance in the traditional sense. This owner lessness made Bitcoin more like a public system formed by open rules than the product of a person, a company, or an interest group.

Second, it placed the rules of the Bitcoin system above the individual. After Satoshi disappeared, Bitcoin no longer depended on one person to continue explaining, maintaining, or endorsing it. It had to operate through code, nodes, miners, users, markets, and social consensus. This gradually transformed Bitcoin from an invention into an open system.

Third, it reduced the focal point of external attack. If Satoshi had remained present, governments could investigate him, capital could buy him, courts could summon him, media could besiege him, and markets could overinterpret his words. Withdrawal removed an easily attacked central target from Bitcoin.

Fourth, it created a powerful spiritual symbol. A creator who completes a system and then leaves, without establishing a company, fighting for power, or placing personal will above rules, creates a narrative with great force. It made Satoshi part of Bitcoin's spirit: restraint, anonymity, anti-centralization, and the principle that rules stand above individuals. Therefore, it must be acknowledged that the mythologizing of Satoshi was not meaningless.

In Bitcoin's first half, it helped Bitcoin establish owner lessness, censorship resistance, and public character. But every narrative has boundaries. A narrative that protects a system in its early growth may become a constraint in the next stage.

II. The Public Credit Root Cannot Maintain Certainty by Relying on Myth for Long

The function of myth is to gather belief, but a financial system cannot operate forever on belief alone. Bitcoin is no longer a geek experiment in a small circle. It has entered discussions of capital markets, ETFs, national regulation, institutional allocation, stable coin systems, AI finance, and future financial infrastructure. When a system begins to assume the function of a Public Credit Root, what it needs is not only narrative power, but theoretical explanation, institutional boundaries, and sustainable certainty. When Satoshi is excessively mythologized, several problems appear in the industry. First, the intellectual source is obscured. People know only that Satoshi created Bitcoin, but rarely study seriously which intellectual traditions he inherited, which historical problems he responded to, which predecessors' work he synthesized, and why the system was designed this way. Bitcoin is then reduced to a "blockchain invention," "digital gold," or "decentralized currency," and its depth of financial thought is greatly underestimated.

Second, key questions become taboo. Who Satoshi is, why he withdrew, how to understand early coins, how old addresses should face the quantum era, and how founder thought should connect with future governance all easily become dangerous topics. The result is that the industry avoids problems instead of building mature theory.

Third, governance vacuum is rationalized. Because Satoshi is absent, the industry often treats "no coordination" as naturally correct. But after entering the second half, time has shown that completely loose self-organization may not be enough to address complex problems. Quantum risk, protocol upgrades, early-coin security, institutional entry, and global regulation all require more mature public discussion, transparent coordination, and a strong-signal coordination mechanism.

Fourth, technical narrative replaces financial theory. When Satoshi is mythologized, the industry more easily treats visible technical parts as the core, such as blockchain, decentralization, mining, consensus mechanisms, and open-source code. As a result, the truly important financial questions - credit, reserves, liabilities, clearing, responsibility, commercialization, and verifiability - remain neglected for a long time.

Fifth, the meaning of the Public Credit Root is underestimated. If Satoshi is only a mysterious technical inventor, Bitcoin is easily treated as a technical product. If Satoshi is understood as a creator in financial intellectual history, the Bitcoin system should be understood as a Public Credit Root. These two interpretations determine completely different futures for cryptocurrency. Therefore, Satoshi cannot remain in myth forever. Myth may help Bitcoin be born, but theory is what helps Bitcoin enter its second half and gives the Public Credit Root a higher degree of institutional certainty.

III. Restoring Satoshi from "God" to "Human" Does Not Lower Him;

It Allows Us to Understand Him Some may misunderstand: does restoring Satoshi from "god" to "human" belittle him? The opposite is true. Mythologizing Satoshi actually weakens his real greatness. A mythical figure needs no history, no intellectual source, no explanation of the design process, and no confrontation with boundaries and limitations. But a truly great creator synthesizes the problems of predecessors in history, solves the problems of an era, and opens a path for the future. Satoshi was not a god who appeared out of nowhere. He faced the unfinished electronic-cash problem after David Chaum, the privacy and freedom questions long considered by the cypherpunks, the distributed-money problems raised but not made operational by Wei Dai and Nick Szabo, the verifiable-cost mechanism provided by Adam Back's proof of work, the fundamental difficulty that digital information could be copied while digital value could not easily be made scarce, and the credit problem exposed by the traditional financial system in the 2008 crisis. The credit problem is the true problem that the Bitcoin system sought to solve. It was not accidental that Satoshi referred to central banks and credit issues in the original Bitcoin announcement. Bitcoin was not created merely to manufacture a new asset, but to establish a verifiable payment, ledgering, and credit structure without a trusted third party.

Satoshi's greatness does not lie in creating every component from nothing. It lies in combining these components into a financial system that could actually run. This system can issue assets, maintain a ledger, prevent double spending, form rule consensus through open verification, operate without a central institution, and combine machine cost, economic incentives, and social consensus so that global users jointly recognize a public ledger. Through machines, this series of creations produced credit - a public, verifiable credit that does not require trust in any individual or institution. This is the Public Credit Root.

The Public Credit Root is not a miracle; it is an institutional creation. Restoring Satoshi to human status does not make him smaller. It lets us see what he truly accomplished. He is not a god, but a creator standing at the intersection of cryptography, finance, software engineering, and institutional design. Such a Satoshi is more important than the Satoshi of myth.

IV. Bitcoin Is Not a Religion; a Credit Root Requires Discussable Certainty

Any powerful community tends to religiousize its source. Bitcoin is no exception. Many Bitcoin supporters fear discussing Satoshi because they worry that discussion will damage belief, affect price, trigger regulation, create a center of power, or cause Bitcoin to lose its ownerless character. These concerns are understandable, but they cannot turn the Satoshi question into a taboo. Bitcoin is not a religion. Bitcoin is an experiment in financial institutions. Religion needs mystery; finance needs explanation. Religion may be maintained by faith; finance must withstand verification, risk, governance, and institutional testing.

If Bitcoin can only stand on the premise that Satoshi is forever undiscussable, then Bitcoin is not mature enough. A truly mature Bitcoin should be able to withstand historical research, intellectual explanation, and institutional discussion. Discussing Satoshi does not mean allowing Satoshi to control Bitcoin. Understanding Satoshi does not mean placing the individual above the protocol. Restoring Satoshi does not mean destroying decentralization. Studying Satoshi does not deny Bitcoin's owner lessness. On the contrary, only by restoring Satoshi from myth to history can we more clearly distinguish which things are Bitcoin's rules, which are Satoshi's ideas, which are early narratives, which were needed in the first half, and which must be transcended in the second half. Taboo cannot protect Bitcoin. Mature theory and transparent discussion can protect Bitcoin's certainty as a Public Credit Root.

V. Only Satoshi as Human Can Enter Financial History

A person can enter financial history; a myth can only remain in legend. If a myth cannot be historicized and theorized, it can easily become spiritual consumption. If Satoshi remains forever a mysterious symbol, he will be continuously consumed, guessed about, misread, and used. The media will treat him as an identity puzzle; the market will treat him as a price risk; conspiracy theories will treat him as story material; legal cases will treat him as an evidence dispute. But if Satoshi is placed back into financial intellectual history, he will be understood anew. He will no longer be only the "founder of Bitcoin," but the creator of the Public Credit Root; not merely the "inventor of blockchain," but the systemic synthesizer of machine credit institutions; not only an "anonymous genius," but a key figure in the historical chain from electronic cash to Verifiable Finance; not only a person of the past, but an intellectual entrance that future financial institutions still need to understand. This is why Satoshi must be restored from "god" to "human." Only a human being has history. Only history has thought. Only thought has theory. Only theory can guide the second half. Bitcoin's first half needed a mysterious, withdrawn Satoshi. Cryptocurrency's second half needs a Satoshi who is further understood.

VI. From Identity Restoration to Intellectual Restoration

Restoring Satoshi to human status is not only about knowing who he is. More importantly, it is about restoring his thought. Identity restoration answers: who created Bitcoin? Intellectual restoration answers: why was Bitcoin created in this way? Identity restoration is important, but intellectual restoration is more important. Even if Satoshi's identity were one day fully confirmed, if the industry still did not understand Bitcoin's financial meaning, the Public Credit Root, verification priority, or why cryptocurrency cannot remain within a technical narrative, then the Satoshi question would still not truly be solved. What we truly need to restore is how Satoshi understood cash, trusted third parties, privacy, issuance, proof of work, incentives, nodes and miners, open rules, and ownerless operation after his withdrawal. Only by understanding these questions can we see how he used technical means to realize a financial system that could issue, keep accounts, verify, and continue to operate. This system is a financial credit-root system and laid the foundation for future Verifiable Finance. After Bitcoin, the world issued countless cryptocurrencies, but few systems can truly be called credit roots. A credit root is not only financial infrastructure; it is also an important public witness foundation for tamper-resistant content, machine auditing, Transparent Banks, and future AI financial systems. Its scope of application exceeds the bitcoin asset and exceeds cryptocurrency in the ordinary sense. Only Satoshi research at the level of thought can truly understand Satoshi's contribution. Only at this level will we discover that understanding Satoshi merely from the perspective of the bitcoin asset actually underestimates **him.**

VII. Why Satoshi Needs to Be Reinterpreted in the Second Half

The core task of cryptocurrency's first half was to prove whether Bitcoin could survive. It needed to prove: without a central bank, could monetary issuance operate? Without a trusted third party, could payment be completed? Without corporate management, could the network be maintained? Without a board of directors, could rules continue? Without sovereign credit, could an asset receive market recognition? Bitcoin has completed most of this task. Through long-term operation, global verification, market choice, and many rounds of shock, the Bitcoin system has proven that an ownerless open system can continue to exist. But the second-half question has changed. The question is no longer only whether Bitcoin can survive, but how the Bitcoin system can be understood and used as a Public Credit Root; how the Public Credit Root can serve future finance; how stable coins can move from trusted reserves to verified reserves; how centralized exchanges can move from black-box positions to asset-liability consistency; how traditional banks can move from credit black boxes to Transparent Banks; how the AI-era security model can be rebuilt; how quantum risk can be coordinated; how early-coin issues can be discussed; and how cryptocurrency can return from the technology industry to the financial industry. These questions cannot be answered simply by "Satoshi's withdrawal." They require reinterpreting Satoshi, re-understanding Bitcoin, redefining the Public Credit Root, and establishing a financial theory for cryptocurrency. Therefore, Satoshi is not a question of

the past, but a question of the second half. In the first half, Satoshi needed to withdraw so that Bitcoin could escape personal authority. In the second half, Satoshi needs to be understood so that cryptocurrency can escape myth and enter theory and institution.

VIII. Inviting Satoshi Is Not Inviting Back Authority, but Inviting Back the Intellectual Source

"Inviting Satoshi" is easily misunderstood. Some will think it means letting a person return to power. Some will think it means letting Satoshi affect prices. Some will think it means recentralizing Bitcoin. Some will think it means using founder authority to override the community. None of these is the real meaning of "inviting Satoshi." Inviting Satoshi is not inviting back authority, but inviting back the intellectual source. It is not making Satoshi the ruler of Bitcoin, but making Satoshi the entrance to Bitcoin's intellectual history. It is not asking Satoshi to make decisions for the industry, but allowing the industry to understand where the protocol came from. It is not placing Satoshi above the rules, but allowing the financial thought behind the rules to be seen. Bitcoin should continue to maintain open verification, node consensus, market choice, and public discussion. No individual should stand above the protocol. But this does not prevent us from understanding Satoshi, nor does it prevent Satoshi's thought from becoming an important interpretive resource for strengthening the certainty of the Public Credit Root. A mature system does not fear its founding history. A mature financial theory does not fear its intellectual source. A mature cryptocurrency should not maintain its identity through myth and taboo.

IX. From a Religiousized Satoshi to a Historicized Satoshi

Cryptocurrency needs to complete a transition: from a religiousized Satoshi to a historicized Satoshi, from a mysterious symbol to an intellectual figure, from an identity puzzle to financial theory, from price risk to institutional source, and from first-half narrative to second-half construction. This is not disrespect toward Satoshi. On the contrary, it is true respect for Satoshi. A myth cannot be truly understood; a historical figure can be seriously studied. If Satoshi's contribution is great enough, he should not exist only as a mystery. He should enter human financial intellectual history. Historicizing Satoshi does not mean personalizing Bitcoin again. It means explaining clearly Bitcoin's institutional creation. Only when Satoshi is historicized can the meaning of the Bitcoin system as a Public Credit Root be fully revealed. Only when the meaning of the Public Credit Root is fully revealed can Bitcoin's second-half transparent coordination, quantum-risk response, discussion of early coins, and applications in Verifiable Finance have a more mature theoretical foundation.

X. Conclusion: Bitcoin's First Half Needed a Withdrawn Satoshi; the Second Half Needs a Satoshi Who Is Understood

In Bitcoin's first half, Satoshi's withdrawal was an advantage. Withdrawal protected Bitcoin's ownerlessness, freed it from personal control, placed rules above the founder, and allowed the system to continue operating without a leader.

But in cryptocurrency's second half, withdrawal alone is no longer enough. The second half needs theory, financial history, institutional history, the Public Credit Root, Transparent Banks, Verifiable Finance, the security model of the AI era, and a new understanding of Satoshi's intellectual source. Satoshi should not forever be a god. Satoshi should become a person in human financial history. Bitcoin's first half needed a withdrawn Satoshi. Verifiable Finance, as the second half, does not need a Satoshi who returns to power. But the development of cryptocurrency and the application of the Public Credit Root need a Satoshi who is understood theoretically, historically, and institutionally. Restoring Satoshi from "god" to "human" is ultimately not about discussing the fate of one person. It is about strengthening the certainty of the Public Credit Root and helping the Bitcoin system move from the survival miracle of the first half to the institutional maturity of the second half.

Chapter Eleven
Why Satoshi Nakamoto's Bitcoin System No Longer Needs Trust in a Person

— *From Human Credit to Machine Credit*

The discussion of Satoshi cannot remain only at the level of "he invented Bitcoin." The deeper question is this: Satoshi created a new credit structure - machine credit, that is, the Public Credit Root. What Satoshi truly solved was not only the question of whether there is credit, but the question of whom credit ultimately depends on: does it ultimately depend on people, institutions, and power, or on an open, verifiable machine-checks-and-balances structure that is difficult for any single party to control?

I. Credit Is Not Simply Belief, but Recognition That Results Are Valid

Credit is not merely saying "I believe you." Credit means that a subject or system causes external participants to recognize that its commitments, records, rules, or results are valid. A bank has credit when people recognize its deposits and transfer records as valid. A court has credit when people recognize that its judgments have institutional force. A company has credit when the market recognizes its products, contracts, and financial reports. An operating system has credit when users recognize its operating results and interface standards. The Bitcoin system has credit when global participants recognize its ledger state, issuance rules, and transaction order. Therefore, the core of credit is not merely psychological belief, but institutional recognition. Whose records count? Whose rules are valid? Whose ledger is recognized? Whose state cannot be easily overturned? Behind these questions lies the real question of credit. When credit reaches the deepest layer, a credit root appears. A credit root is the lowest-level structure in a system that is ultimately recognized as the valid basis.

II. People as Credit Roots: Ultimately One Must Trust Key Persons

Human credit comes from character, reputation, competence, historical behavior, and social relations. Human credit has advantages: it can judge complex situations, bear responsibility, adjust during crises, and create solutions in new environments.

But human credit also has fundamental limits: people make mistakes, die, become greedy, can be bought, can be coerced, can abuse power, and can default under pressure. Therefore, human credit naturally needs institutional constraints. Contracts, audits, regulation, courts, corporate governance, separation of permissions, review mechanisms, and legal responsibility all arise to constrain the risks of human credit. Even so, in many traditional systems, one ultimately must still trust that certain key persons will not destroy the system. This is the boundary of human credit roots.

III. The DOS Example: Software Systems Ultimately Trust the Underlying Developers

Microsoft DOS is a good example. On the surface, it led users to trust Microsoft and the PC ecosystem, but at the underlying level, credit still rested to a considerable degree on core developers. Who wrote the core code? Who understood the underlying logic? Who could fix critical errors? Who controlled version evolution? Who could ensure that system behavior and compatibility continued to hold? These questions ultimately point to the people who possess key knowledge, key code, and key maintenance authority. Especially in the early stage, the credit of an operating system depended heavily on a small number of core engineers. This shows that at the bottom of software credit, the foundation is often not the corporate brand itself, but the people who possess the system's key capabilities. This credit can be strong, but it is still human credit.

IV. Apple's Secure Enclave: From Single-Person Credit to Team-Based Check-and-Balance Credit

Apple's Secure Enclave provides another level. Its credit comes from a complex structure: hardware root of trust, Secure Enclave, signature mechanisms, system updates, security teams, internal processes, and the product ecosystem. In this structure, the credit root is no longer a single person, but a group of teams constrained by institutions, processes, and internal checks and balances. Yet Apple's Secure Enclave is still not a public machine credit root. The reason is that users ultimately still have to trust Apple: trust that it will not abuse permissions, arbitrarily change rules, abandon continuous maintenance, or sacrifice user interests

under commercial or regulatory pressure. Apple's credit is strong, but it remains centralized corporate credit. Its advantages are efficiency, security, user experience, and clear responsibility. Its boundary is that users ultimately must trust this center.

V. Why a Central Bank Is Not a Qualified Credit Root in the Sense of Machine Credit

A central bank is often regarded as the credit root of the fiat system. From Satoshi's perspective, however, a central bank is more like a power root than a reliable credit root in the sense of machine credit. The core of Satoshi's criticism of the traditional monetary system is precisely that central banks must be trusted not to debase the currency, yet fiat history repeatedly shows that this trust is often broken. A true credit root must be able to constrain itself. The greatest problem of a central bank is that it can change the rules, but is difficult to subject to continuous external verification and hard constraint. If a central bank wants to obtain credibility in the sense of machine credit, it must bring key ledgers, key issuance, and key asset-liability states into externally verifiable structures, and may even need to hash-anchor key states to Public Credit Roots such as the Bitcoin system for public verification. Otherwise, it still relies mainly on power, policy choice, and institutional reputation, rather than on an unavoidable credit constraint.

VI. Machine Credit Is Not Trusting Machines, but Trusting a Check-and-Balance Structure

The Bitcoin system diverges from the central-bank system because it does not ask people to trust a better central bank. It attempts to create a machine credit structure that does not depend on central-bank credit. The essence of machine credit is not blind trust in machines themselves, but trust in a rule structure that is open, verifiable, repeatable, difficult to tamper with, and not controllable by any single party. Human credit says: I trust that you will not deceive me. Machine credit says: even if you want to deceive me, I can verify it; even if you want to do evil, the system makes it difficult for you to succeed alone. Machine credit must have several conditions: rules are public, execution is determinate, history is traceable, states are verifiable, tampering costs are extremely high, participants check and balance one another, no single party can ultimately control the system, and external observers can independently verify results. Machines without checks and balances do not produce true machine credit. A centralized database can run automatically, but it is not a machine credit root because an administrator can change the data. A corporate server can operate continuously, but it is not a Public Credit Root because the company can control the rules. A central-bank digital currency can use cryptographic technology, but if the issuer can change the rules, it remains a power root.
The key to machine credit is not "mechanization," but the impossibility of single-party control.

VII. The Credit Root of the Bitcoin System Comes from Multi-Party Checks and Balances

The true breakthrough of the Bitcoin system is that it did not hand credit to one person or organization. It placed key participants into a structure of mutual checks and balances. Programmers can write code, but cannot force everyone to run it. Miners can provide hash power, but cannot force nodes to accept invalid blocks. Nodes can verify rules, but cannot create proof of work from nothing. Exchanges can provide liquidity, but cannot change the issuance limit. Markets can price Bitcoin, but cannot rewrite ledger history. Users can choose software, but cannot depart from network consensus. Satoshi created the system, but after his withdrawal, he too could not rewrite rules as an authority. This is the credit-root characteristic of the Bitcoin system: a machine credit structure jointly formed by programmers, miners, nodes, users, markets, the historical ledger, and public rules. Checks and balances are the key. Programmers are checked by nodes and markets; miners are checked by nodes and economic incentives; nodes are checked by software rules and user choice; markets are checked by liquidity, consensus, and real demand. No party can independently become the final credit root. This is the fundamental difference between the Bitcoin system and DOS, Apple, or the central bank. Machine trust is higher than trust in a single person, and higher than trust in a centralized organization. Satoshi was determined to change the trust mechanism of the traditional monetary system, and he did achieve it.

VIII. What Satoshi Truly Completed Was the Creation of a Credit-Root Institution

What Satoshi completed was not only the creation of the bitcoin asset. Bitcoin as an asset is of course great: scarce, liquid, global, a store of value, and non-sovereign. But the greater achievement of the Bitcoin system is that it created the Public Credit Root. Bitcoin is an asset. The Bitcoin system is a credit root. An asset can be held; a credit root can be referenced by other systems. An asset solves value storage; a credit root solves final credibility. An asset can resemble gold; a credit root has almost no precedent in human history. Gold has scarcity, but it cannot provide timestamp proofs for other ledgers. Gold has historical consensus, but cannot verify digital states. Gold has a store-of-value function, but cannot serve as a public witness layer for machine systems. The Bitcoin system can. To understand Satoshi only from the perspective of the bitcoin asset is to underestimate him. Satoshi did not create a system that makes the world trust him. He created a system that no longer needs to trust him. This is one of the highest forms of institutional creation. The greatest achievement of a creator is not to make everyone depend on him forever, but to create a system that even he himself cannot control at will. Satoshi's greatness lies precisely here.

IX. From Human Credit to Machine Credit: The True Historical Turning Point of Cryptocurrency

The history of human finance is a history of credit, long built on the credit of people, institutions, and states: trusting kings, governments, central banks, banks, courts, auditors, companies, experts, key developers, and security teams. These forms of credit are not without value. They form an important foundation of modern civilization. But they all have boundaries: they ultimately depend on whether people, organizations, power, morality, and institutions remain effective.

The Bitcoin system proved for the first time that credit no longer needs to rest ultimately on any single person. It can rest on a machine structure formed jointly by public rules, open verification, proof-of-work competition, multi-party checks and balances, and long-term history. Not because there are no people involved, but because it does not require us ultimately to trust any one person.

Not because it has no risk, but because it places risk into structures of public verification and multi-party checks and balances. Not because it will never make mistakes, but because the cost of transaction rollback rises as the number of block confirmations increases, thereby forming a quantifiable expectation of finality. This is the historical transition from human credit to machine credit, and the reason Satoshi's Bitcoin system can become a Public Credit Root.

Conclusion: Satoshi's Greatness Is That He Created a System That Does Not Require Trust in Satoshi A credit root is not an organization, but the lowest-level basis by which results are ultimately recognized as valid. A human credit root ultimately rests on key people. An organizational credit root ultimately rests on key teams and check-and-balance processes. A power credit root ultimately rests on coercive power and policy choice. A machine credit root ultimately rests on verification and checks and balances that cannot be controlled by any single party.

The Bitcoin system placed programmers, miners, nodes, users, markets, and the historical ledger into a mutually checking machine structure. This is Satoshi's true creation. He did not make the world trust him; he created a system that no longer needs to trust him. He did not create a new center; he created a public structure in which no single center can become the final credit root. He did not merely create Bitcoin; he created the public machine credit root. This is Satoshi's historical position, and it is also the fundamental reason the Bitcoin system is irreplaceable.

Chapter Twelve
Satoshi Nakamoto's Withdrawal Made Bitcoin Possible, but May Also Limit Bitcoin's Second Half

— From the Advantage of Ownerlessness to a Transparent Coordination Mechanism

The problem of Bitcoin's first half was whether it could survive without a central issuer, a corporate body, or traditional financial guarantees. Satoshi's withdrawal played a decisive role at this stage: it helped Bitcoin escape founder control, form ownerlessness, and establish the spiritual foundation that rules stand above individuals. The problem of Bitcoin's second half has changed. Bitcoin is no longer merely an open issuance system asking whether it can survive. It may become the Public Credit Root of Verifiable Finance and enter modern finance, institutional assets, regulatory frameworks, Transparent Banks, AI security, and machine-credit systems. At this point, the loose technical coordination mechanisms formed in the first half may not be sufficient to handle more complex uncertainty. Therefore, we need to discuss more seriously how, after Bitcoin enters its second half as a Public Credit Root, a transparent, limited, term-bound, bounded, and backstopped coordination mechanism can be established without destroying ownerlessness or creating a coercive center. A common concern is that any coordination mechanism may bring factual authority, interest capture, and responsibility-shifting risks. This concern is not unreasonable, but it cannot become a reason to reject coordination. The real question is not whether coordination is needed, but how coordination can be institutionalized, made transparent, temporary, and exit-enabled. What we ultimately need is not avoidance of the problem, but a solution.

I. Withdrawal Does Not Mean Intellectual Absence

After Satoshi's withdrawal, the industry gradually formed a series of misunderstandings: since Satoshi is absent, Bitcoin does not need to understand Satoshi; since Bitcoin is ownerless, the intellectual source is unimportant; since the protocol can run, theoretical explanation can be absent; since decentralization is the objective, any coordination should be suspected; since Satoshi should not control Bitcoin, he can only remain forever in myth. Withdrawal is not intellectual absence. Ownerlessness is not absence of history; decentralization is not absence of theory; anti-centralization is not opposition to all explanation and all coordination. A system can be ownerless at the operational level, but it must have a source in intellectual history. A protocol can be free from founder control, but cannot therefore lose theoretical explanation. A Public Credit Root may belong to no person, but it must be understood by society, absorbed by institutions, and applied by future finance. Bitcoin is not a natural object, not gold dug from the earth, and not a network phenomenon formed by accident. It is a carefully designed financial system with clear problem consciousness, design tradeoffs, historical sources, and institutional logic. Without understanding these things, the industry easily misreads Bitcoin as "blockchain technology," "digital gold," "decentralized currency," or an "anti-inflation asset," and fails to see the most valuable thing it truly created: The Public Credit Root. Satoshi withdrew to free Bitcoin from personal control. But this does not mean that cryptocurrency can abandon the study of Satoshi's thought. On the contrary, the more Bitcoin enters its second half, the more it needs to understand Satoshi's thought from a financial perspective.

II. Why Withdrawal May Create a Governance Vacuum in the Second Half

The objective of Bitcoin's second half is no longer mere survival, but entry into a more complex financial world. At this point, the problems become fundamentally different. Quantum-computing risk is far from ordinary market volatility. Early coins and old-address security have already moved beyond ordinary technical disputes. The application of Bitcoin as a Public Credit Root is not an ordinary payment problem. Institutional capital entering is not ordinary user adoption. Global regulatory games are not a single community discussion. The security risks of the AI era cannot be fully covered by traditional open-source audits. Transparent Banks and Verifiable Finance are not problems solved by simple on-chain transfers. All of these problems require more mature

The problem of Bitcoin's first half was whether it could survive without a central issuer, a corporate body, or traditional financial guarantees. Satoshi's withdrawal played a decisive role at this stage: it helped Bitcoin escape founder control, form owner lessness, and establish the spiritual foundation that rules stand above individuals. The problem of Bitcoin's second half has changed. Bitcoin is no longer merely an open issuance system asking whether it can survive. It may become the Public Credit Root of Verifiable Finance and enter modern finance, institutional assets, regulatory frameworks, Transparent Banks, AI security, and machine-credit systems. At this point, the loose technical coordination mechanisms formed in the first half may not be sufficient to handle more complex uncertainty. Therefore, we need to discuss more seriously how, after Bitcoin enters its second half as a Public Credit Root, a transparent, limited, term-bound, bounded, and backstopped coordination mechanism can be established without destroying ownerlessness or creating a coercive center. A common concern is that any coordination mechanism may bring factual authority, interest capture, and responsibility-shifting risks. This concern is not unreasonable, but it cannot become a reason to reject coordination. The real question is not whether coordination is needed, but how coordination can be institutionalized, made transparent, temporary, and exit-enabled. What we ultimately need is not avoidance of the problem, but a solution.

I. Withdrawal Does Not Mean Intellectual Absence

After Satoshi's withdrawal, the industry gradually formed a series of misunderstandings: since Satoshi is absent, Bitcoin does not need to understand Satoshi; since Bitcoin is ownerless, the intellectual source is unimportant; since the protocol can run, theoretical explanation can be absent; since decentralization is the objective, any coordination should be suspected; since Satoshi should not control Bitcoin, he can only remain forever in myth. Withdrawal is not intellectual absence. Ownerlessness is not absence of history; decentralization is not absence of theory; anti-centralization is not opposition to all explanation and all coordination. A system can be ownerless at the operational level, but it must have a source in intellectual history. A protocol can be free from founder control, but cannot therefore lose theoretical explanation. A Public Credit Root may belong to no person, but it must be understood by society, absorbed by institutions, and applied by future finance. Bitcoin is not a natural object, not gold dug from the earth, and not a network phenomenon formed by accident. It is a carefully designed financial system with clear problem consciousness, design tradeoffs, historical sources, and institutional logic. Without understanding these things, the industry easily misreads Bitcoin as "blockchain technology," "digital gold," "decentralized currency," or an "anti-inflation asset," and fails to see the most valuable thing it truly created: The Public Credit Root. Satoshi withdrew to free Bitcoin from personal control. But this does not mean that cryptocurrency can abandon the study of Satoshi's thought.

On the contrary, the more Bitcoin enters its second half, the more it needs to understand Satoshi's thought from a financial perspective.

II. Why Withdrawal May Create a Governance Vacuum in the Second Half

The objective of Bitcoin's second half is no longer mere survival, but entry into a more complex financial world. At this point, the problems become fundamentally different. Quantum-computing risk is far from ordinary market volatility. Early coins and old-address security have already moved beyond ordinary technical disputes. The application of Bitcoin as a Public Credit Root is not an ordinary payment problem. Institutional capital entering is not ordinary user adoption. Global regulatory games are not a single community discussion. The security risks of the AI era cannot be fully covered by traditional open-source audits. Transparent Banks and Verifiable Finance are not problems solved by simple on-chain transfers. All of these problems require more mature public discussion, a more transparent coordination mechanism, and a higher-level theoretical framework. However, the Bitcoin community has long maintained natural vigilance toward "coordination." Mention coordination and it is easily understood as centralization. Mention governance and it is easily seen as betrayal of Bitcoin's spirit. Mention Satoshi and it is easily understood as creating authority. As a result, the industry may fall into a governance vacuum: problems truly exist, but no one can propose a strong signal on behalf of the system; risks gradually approach, but coordination mechanisms are insufficient; theory needs upgrading, but myth still occupies the center; financial applications need implementation, but the industry is still repeating technical slogans; regulatory pressure continues to grow, but cryptocurrency lacks mature financial theory with which to respond. This is the limitation that Satoshi's withdrawal may create in the second half: the withdrawal itself was not wrong, but the industry has misread withdrawal as "never needing an intellectual source or a coordination layer." If the importance of the Bitcoin system as a Public Credit Root remains misunderstood for a long time, and if major risks still lack a clear coordination route, Bitcoin may be marginalized in key financial applications. That Bitcoin's price has not only failed to catch up with leading AI assets but has at times underperformed gold shows that the current narrative is clearly insufficient. This itself shows that the market still has not fully understood the Public Credit Root value of the Bitcoin system, nor has it seen the institutional path for strengthening that value. Bitcoin's second half needs a new narrative: not only explaining bitcoin as digital gold, but explaining the Bitcoin system as the Public Credit Root of Verifiable Finance.

III. Ownerlessness Cannot Substitute for Coordination Capacity

Bitcoin's ownerlessness is an advantage, but it cannot substitute for all coordination capacity.

Gold is also ownerless. But gold has no protocol upgrades, no quantum migration, no address-security issues, no node consensus, no miner incentives, no software vulnerabilities, and no global network-governance problems. Bitcoin is far more complex than gold. Bitcoin is both an asset and a system; both money and a network; both a ledger and a Public Credit Root. It needs resistance to centralization, but it also needs long-term maintenance. It must keep rules stable, but it must also face external technological risks. Therefore, Bitcoin cannot be explained simply through the logic of gold. Gold does not need developers; Bitcoin does. Gold does not need miners, nodes, and markets to jointly maintain the continuity of a protocol; Bitcoin does. Gold does not need to face quantum-signature migration; Bitcoin must. Gold does not need to handle early-address security; Bitcoin must. Gold does not need to respond to the AI-era open-source attack model; Bitcoin and Ethereum both must. Therefore, Bitcoin's ownerlessness cannot be understood as "no need for coordination." The real question is how to establish a transparent, limited, non-coercive, verifiable coordination mechanism without destroying ownerlessness. This is the true question Bitcoin's second half needs to discuss.

IV. Coordination Risk Cannot Negate Coordination; the Key Is to Institutionally Limit Coordination Power

One of the most important objections is that coordination mechanisms may bring factual authority and interest capture. This concern is reasonable. Any coordination layer, if it loses boundaries, can move from a "strong-signal proposal layer" to a "factual power center." Any long-occupied coordination institution may be captured by capital, miners, exchanges, political forces, or developer cliques. Any arrangement that shifts responsibility to "the community" or "the protocol" may also allow financial institutions to evade their own responsibility.

But these problems show not that "coordination is impossible," but that "coordination must be designed." The institutional experience of the real world is similar. Washington's importance did not lie in establishing permanent authority, but in assuming the responsibility of founding coordination at a critical turning point, and then limiting power itself through terms, exit, and institutional arrangements. Leaders are often very important at historical turning points, but mature institutions do not make leaders permanent. They restrict leaders through terms, procedures, publicity, and boundaries of power. Bitcoin's second half should be the same. In the face of quantum risk, early-coin issues, Public Credit Root applications, institutional entry, and global regulation, having no strong-signal coordination layer at all may lead to delay, misunderstanding, and division. But a coordination layer without boundaries may damage owner lessness. Therefore, the truly feasible direction is not rejection of coordination, but establishment of transparent coordination. Transparent coordination should follow these principles: it may propose strong signals, but cannot enforce execution; it must conduct public discussion, not black-box decision-making; it must accept questioning and cannot become an authoritative oracle; it must preserve the final choice of nodes, miners, markets, and users; it must aim at the security and long-term credibility of the Public Credit Root, not the interest of any particular group; it must treat UASF as the ultimate backstop, not as a replacement for the choice of the economic majority; and the coordination institution must have a term, boundaries, and an exit mechanism. Such coordination is not destroying Bitcoin. On the contrary, it may become the next-stage tool for protecting Bitcoin's owner lessness.

V. The Real Meaning of Satoshi's Participation: Not the Return of Authority, but Strong-Signal Coordination with a Limited Term

If Satoshi could participate in second-half coordination in a public, limited, non-coercive, term-bound way, this may be the optimal strong-signal solution at the present stage. Satoshi's participation here cannot be understood as letting Satoshi take power again, still less as allowing Satoshi to stand above the protocol. Its real meaning is that when the Public Credit Root faces major uncertainty, the person with the greatest meaning as intellectual source and historical legitimacy provides strong-signal coordination within a limited term. The so-called return of thought means re-understanding why Satoshi created Bitcoin, re-explaining Bitcoin's financial meaning, re-answering how the Public Credit Root should enter future finance, bringing cryptocurrency back from technical narrative to financial essence, and changing the first-half phenomenon in which even "bitcoin" and the "Bitcoin system" were not clearly distinguished and everything was explained technologically. Of course, the practical experience of the first half must be respected: Satoshi should not stand above the protocol, should not make decisions for the market, should not become Bitcoin's ruler, should not have coercive power, and should not return Bitcoin to the structure of a founder project. But Satoshi can be an intellectual source, a historical interpreter, and a catalyst for theoretical reconstruction and public coordination in the second half. He can help the industry understand that Bitcoin is not an ordinary technical system, but a Public Credit Root; he can also help the industry understand Transparent Banks, Verifiable Finance, AI security, quantum risk, and public coordination. Therefore, the reasonable form of Satoshi's participation in coordination is not permanent authority, but a limited term; not administrative control, but strong-signal proposal; not unilateral decision, but public discussion; not replacement of UASF, but respect for the final choices of nodes, miners, markets, and users. The term system itself is a limiting device: it lets a leader play a role during a critical transition while preventing the coordination mechanism from becoming a permanent power center.

VI. Withdrawal Protected the Bitcoin Asset, but Intellectual Absence Limits Credit-Root Application

Bitcoin as an asset has already been seen by the world. ETFs, institutional allocation, global liquidity, non-sovereign store-of-value narratives, and the digital-gold narrative all show that Bitcoin's value at the asset level has entered mainstream view.

But the Bitcoin system as a Public Credit Root is still far from fully understood. Many people still view Bitcoin as an asset rather than a system; as digital gold rather than a machine credit root; as a store of value rather than external verification infrastructure; as an investment target rather than a credit anchor for future finance. This is precisely the result of intellectual absence. Satoshi's withdrawal protected the Bitcoin asset, but the long-term absence of Satoshi's thought caused the meaning of the Public Credit Root to be underestimated. If the industry understands only the bitcoin asset, it will talk only about price, ETFs, halving's, miners, and macro liquidity. If it understands the Bitcoin system, it will begin to discuss the Public Credit Root, lowest ledgering cost, Transparent Banks, Verifiable Finance, hash anchoring, machine credit, and future financial infrastructure. This is the difference between Bitcoin's first half and second half: in the first half, the world discovered bitcoin; in the second half, the world must understand the Bitcoin system, and on that basis explore how it can jointly build trustworthy, transparent, and verifiable future financial infrastructure together with technologies such as AI.

VII. Bitcoin's Second Half Needs "Owner lessness + Transparent Coordination + Term Constraints"

Bitcoin's first half proved one thing: without a center, a monetary issuance and ledgering system can still run. Bitcoin's second half needs to prove another thing: without a center, it can still remain credible, verifiable, coordinatable, and sustainable in the complex financial era. It needs owner lessness, and it also needs transparent coordination; it needs the Public Credit Root, and it also needs Verifiable Finance; it needs the final choice of nodes, and it also needs a strong-signal proposal layer; it needs free market choice, and it also needs public risk discussion; it needs developer expertise, and it also needs the economic majority as backstop; it needs the return of Satoshi's thought, and it also needs Satoshi's personal influence not to exceed its boundary. It does not need personal dictatorship or permanent authority. Coordination must be voluntary, must respect the interests of the majority, and must form majority consensus through public discussion. How is consensus formed? It must allow people to see clear benefits. The Public Credit Root is Bitcoin's unique institutional value and the social new anchor most likely to form broader consensus. This is the direction of the second half: not to replace owner lessness with coordination, but to protect owner lessness through transparent coordination; not to replace rules with a leader, but to use term-limited leadership during a critical transition to help rules enter a new historical stage; not to turn Bitcoin into a centralized system, but to make Bitcoin better understood, applied, and protected as a Public Credit Root.

VIII. Conclusion: Understanding and Coordination Can Open the Second Half

Satoshi's withdrawal was an arrangement of history. But Satoshi's withdrawal should not be misread as "the intellectual source is unimportant." Ownerlessness should not be misread as "no need for historical explanation." Decentralization should not be misread as "rejecting all coordination." In Bitcoin's first half, withdrawal was an advantage, because Bitcoin first had to survive as an asset and a monetary issuance system. In Bitcoin's second half, we need to re-understand the Bitcoin system. The Bitcoin system is a Public Credit Root; the Public Credit Root needs to enter Transparent Banks and Verifiable Finance; Verifiable Finance needs a new financial theory; and this new financial theory needs to re-understand Satoshi and also face transparent coordination when real risks arise. If Satoshi can participate in second-half coordination through a limited term, without coercive power, with public procedures and UASF as the backstop, that is not a destruction of Bitcoin's owner lessness. It may be one of the optimal solutions for strengthening the certainty of the Public Credit Root. Understanding is what can open the second half. Coordination is what can handle the complex risks of the second half. Terms and institutional boundaries are what can prevent coordination from becoming a new power center. How to guarantee the certainty of the Public Credit Root cannot remain only at the level of problem consciousness. It must form an institutional proposal that can be discussed, tested, and constrained.

Chapter Thirteen
The Transparent Coordination Institution in Bitcoin's Second Half Is an Institutionalized Path

— From the Advantage of Owner lessness to Strong-Signal Coordination with a Limited Term

Introduction: We Must Answer "What Should Be Done"

Chapters Nine through Twelve have basically clarified the theoretical boundaries of the Satoshi Nakamoto question: the Satoshi question is not gossip, but a question about the source of the Public Credit Root; Satoshi must be restored from "god" to "human," because myth cannot replace theory; the Bitcoin system created by Satoshi established a public machine credit root that no longer requires trust in any person; Satoshi's withdrawal made Bitcoin's first half possible, but after Bitcoin enters its second half, intellectual absence and insufficient coordination may also limit the application of the Public Credit Root. Therefore, this chapter must answer a more concrete and difficult question: since Bitcoin cannot return to personal authority, why does the second half still need coordination? In what form should such coordination exist? How can it avoid centralized rule while also avoiding governance vacuum?

This is the question of a transparent coordination institution.

A real risk must be faced: any coordination institution may form factual authority, interest capture, responsibility transfer, and damage to protocol neutrality. But if this chapter is changed merely into a discussion of risks, it would evade the real problem. Bitcoin's second half ultimately needs a solution. Risk cannot be a reason to reject coordination; risk shows precisely that coordination must be institutionally limited. If "inviting Satoshi" is understood as letting a person return to power, it is not appropriate. If it is understood as manufacturing identity news, it is not enough. If it remains only at the level of intellectual history, it still cannot complete the second-half task. A more mature understanding should be this: Bitcoin needs a transparent coordination layer that can carry Satoshi's thought, serve the application of the Public Credit Root, and at the same time be constrained by terms and institutional boundaries.

I. Why Governance Vacuum Appears in Bitcoin's Second Half

The core task of Bitcoin's first half was issuance, ledgering, and survival verification. It therefore most needed institutional neutrality. Bitcoin's most valuable quality is avoiding control by any single subject. Satoshi's withdrawal, node consensus, miner competition, open-source code, and market choice jointly helped Bitcoin complete its first half. The problems of the second half have changed. Bitcoin is no longer only an asset; it is being understood as a Public Credit Root. Its value lies not only in issuance and ledgering, but also in the possibility that other financial systems may reference, anchor to, audit, and verify through it. At this point it must face new questions: how quantum risk should be handled, how early-address security should be discussed, how institutional funds can enter without distorting neutrality, how AI-era open-source code risks should be governed, how global regulation can understand that Bitcoin is not an ordinary financial product, and how the Bitcoin system can move from an "asset narrative" to a "financial-infrastructure narrative." These questions are not merely technical or market questions. They also involve finance, law, politics, regulation, security, accounting, auditing, applications, and social consensus. In this situation, complete reliance on loose coordination will inevitably produce a governance vacuum: problems truly exist but lack a high-level public discussion framework; risks gradually approach but there is no strong-signal roadmap; developers can discuss code but cannot represent the economic majority; miners can express hash power but cannot represent all holders; regulators need a communication object but Bitcoin has no formal explanatory mechanism; ordinary holders are the economic majority but lack

institutionalized channels of expression. Thus the industry easily falls into a state in which it can argue but cannot form a direction; it can oppose but cannot put forward mature proposals; it can maintain owner lessness but has difficulty forming a public roadmap for the second half. This is governance vacuum.

II. Solving Governance Vacuum Must Never Move Toward Personal Authority

This is the bottom line. Solving governance vacuum absolutely does not mean letting Satoshi make final decisions for the protocol, make final judgments for the market, possess power above nodes, miners, and the economic majority, become the governor of a Bitcoin central bank, or allow Bitcoin to regress from an ownerless system into a founder system. If this occurred, the ownerlessness established in Bitcoin's first half would be destroyed. Bitcoin's greatness lies precisely in the fact that Satoshi created a system that no longer needs to trust Satoshi. The greatest achievement of a creator is not to make the world depend on him forever, but to create a public system that even he himself cannot control at will. Satoshi can be an intellectual source, historical interpreter, and catalyst for second-half theoretical reconstruction. He can help the industry understand the financial meaning of the Bitcoin system, and help the outside world understand the Public Credit Root, Transparent Banks, and Verifiable Finance. But Satoshi cannot become the final judge. Bitcoin must still insist that rules stand above individuals, verification above authority, nodes and markets above slogans, the economic majority above the founder, and UASF remains the ultimate backstop. Therefore, what the second half needs is not "Satoshi taking power," but "the institutionalization of Satoshi's thought."

III. The Necessity of a Transparent Coordination Institution

Since Bitcoin cannot return to personal authority, does it therefore need no coordination? The answer is no. Bitcoin's second half needs coordination, but this coordination must be transparent, limited, non-coercive, challengeable, exit-enabled, and in service of the economic majority. It is not a ruling institution, but a strong-signal institution; not a protocol sovereign, but a public discussion platform; not an administrative center, but a mechanism for forming roadmaps; not a replacement for UASF, but a service to public judgment before UASF; not a way for a minority to control Bitcoin, but a way for the majority to understand major issues more clearly. The complexity of second-half problems determines this necessity. Quantum migration cannot be solved merely by spontaneous market behavior; it involves cryptography, wallet migration, early addresses, user education, exchange support, miner upgrades, node versions, time windows, and legal risks. Early-coin security cannot rely only on emotional debate; it involves the principle of immutability, property-right boundaries, quantum risk, dormant addresses, community belief, market expectations, and institutional legitimacy. Public Credit Root applications cannot be advanced by a single developer; they require banks, auditors, regulators, stable coin issuers, custodians, exchanges, and corporate ledgers to jointly understand the external anchoring value of the Bitcoin system.

Without a transparent coordination institution, these issues will be discussed in fragments. Fragmented discussion can produce voices, but it is difficult to form strong signals. Without strong signals, the second half is difficult to advance.

IV. What the Transparent Coordination Institution Can and Cannot Do

The boundaries of the transparent coordination institution must be very clear. It provides only strong signals, not coercive orders; it proposes roadmaps, but does not control the protocol; it organizes public discussion, but does not create black-box decisions; it serves the economic majority, but does not replace the economic majority. The things it can do include: identifying major issues such as quantum risk, early-address risk, Public Credit Root applications, AI security, long-term protocol maintenance, institutional entry, and regulatory misunderstanding; transforming chaotic disputes into clear questions; summarizing different proposals and listing their advantages, disadvantages, costs, risks, scope of impact, and objections; inviting developers, miners, holders, financial application parties, security experts, legal experts, audit experts, and regulatory observers to participate in public review; using multi-model AI audits and human expert review for risk simulation; issuing non-coercive coordination suggestions or roadmaps after sufficient discussion; accepting public questioning, rebuttal, and competition from alternative proposals; and tracking ecosystem adoption. The things it cannot do must also be written clearly: it cannot acquire protocol sovereignty, cannot represent all holders, cannot replace node choice, cannot force miners and users to upgrade, cannot freeze or dispose of assets, cannot become a regulatory authorization subject, cannot assume compliance responsibility for financial institutions, cannot treat AI tool outputs as final decisions, and cannot turn the Public Credit Root into the private interpretive right of any institution. This is the reasonable position of the transparent coordination institution: not a power center, but a center of public reason; not a protocol controller, but a generator of strong signals; not a substitute for Satoshi, but a discussion field for institutionalizing Satoshi's thought.

V. Why Satoshi May Be the Optimal Strong-Signal Candidate in the First Stage

At historical turning points, leaders are often very important. The question is not whether leadership is needed, but whether leadership is institutionally limited. Washington's importance did not lie in establishing permanent authority, but in assuming the

responsibility of founding coordination at a critical turning point and then limiting power itself through terms, exit, and institutional arrangements.

Bitcoin's second half faces a similar problem. In the face of quantum risk, early-coin issues, Public Credit Root applications, institutional entry, and global regulation, having no strong-signal coordination layer at all may lead to delay, misunderstanding, and division; but if the coordination layer has no boundaries, it may damage ownerlessness. Therefore, the truly feasible direction is not to reject leadership, but to limit leadership within a transparent, temporary, non-coercive, and exit-enabled institutional structure. If Satoshi can participate in second-half coordination in a public, limited, non-coercive, term-bound way, this may be the optimal strong-signal solution at the current stage. The reason is that Satoshi has a meaning as intellectual source and historical legitimacy that no one else possesses. His role is not to make decisions for Bitcoin, but to help the industry re-understand the Bitcoin system, re-explain the Public Credit Root, and reorganize theory and public discussion for the second half when the Public Credit Root faces major uncertainty. Satoshi may become a first-stage coordinator, but cannot become permanent authority. He may provide an intellectual source, but cannot substitute for institutions. He may help establish a transparent coordination layer, but cannot let it become centered on one person. He may provide strong signals, but cannot force nodes and markets to accept them. The highest objective of Satoshi's participation in transparent coordination should be to help Bitcoin's second half establish a coordination mechanism that ultimately does not depend on him.

VI. Who Should Participate in the Transparent Coordination Institution

If the coordination institution is composed only of developers, it will be too technical; only of miners, it will become an expression of hash-power interests; only of exchanges, it will be captured by market liquidity; only of large holders, it will become a capital club; only with regulators, it will lose Bitcoin's neutrality; only led by Satoshi personally, it will recreate founder authority. Therefore, the transparent coordination institution must embody multi-party checks and balances. It should at least include the following subjects: developers, who understand the protocol, code, security boundaries, and technical feasibility; miners or hash-power representatives, who bear network security and block-production competition; holders and economic-node representatives, who express the core interests of the economic majority; node and user representatives who do not participate in hash power, reflecting the position of users of the public verification network; financial application parties, including custodians, stable coin institutions, Transparent Banks, audit institutions, and enterprise application parties, representing second-half application needs for the Public Credit Root; security and cryptography experts, who study quantum risk, signature migration, wallet security, formal verification, and AI attack models; legal and regulatory observers, who do not control Bitcoin but help the industry understand real-world law, property-right boundaries, compliance paths, and regulatory misunderstandings; and AI audit systems, which are not voting subjects but tools for continuous auditing, risk simulation, and comparison of proposals. Among these, the most important mechanism is the expression of holders, nodes, and the economic majority. Transparent coordination in the second half must give the economic majority a clear position. Otherwise, coordination can easily become an internal discussion among a small technical circle, capital circle, or institutional circle.

VII. Weighting and Voting: They Can Form Only Public Signals, Not Protocol Commands

If a clearer coordination structure is needed in the future, a multi-party weighting model can be considered. But the design of weights must serve one objective: no single group can monopolize interpretive power. Developers have expertise, but cannot monopolize direction. Miners contribute security, but cannot monopolize rules. Holders have economic weight, but cannot ignore technical boundaries. Institutions have application capacity, but cannot sacrifice publicness. Regulators have real-world influence, but cannot replace the economic majority. Satoshi has significance as intellectual source, but cannot possess final power. It must be stated especially clearly here: any vote can only form a public signal, not a protocol command. It cannot change Bitcoin consensus rules, cannot replace the choices of nodes running software, cannot represent all holders, and cannot become a basis for regulators or financial institutions to shift responsibility. This distinction is extremely important. A transparent coordination institution is not a protocol-sovereign institution, nor an asset-representation institution. The votes, recommendations, roadmaps, and risk reports it forms are only public information that helps markets, nodes, developers, and application parties make judgments. What truly determines whether a proposal becomes effective remains the actual choice of nodes, miners, users, markets, and the economic majority.

VIII. Coordination Risks Must Be Faced and Institutionally Managed

These risks cannot be ignored. A transparent coordination institution must write these risks into its institutional boundaries from the beginning. First, representation risk. No coordination institution can claim to represent all of Bitcoin, nor all holders, nodes, or users. It can only represent the non-coercive public signals formed by participants under public procedures. Second, the risk of concentration in coin holdings and voting power. If voting is simply based on holdings, large holders and institutions may form factual control. Therefore, the holder expression mechanism must consider time weighting, tiered limits, interest disclosure, and anti-concentration design. Capital weight cannot

be directly converted into protocol power. Third, developer or miner capture risk. Developers possess technical discourse power, and miners possess hash-power influence, but neither can monopolize the interpretive power of the Public Credit Root. The transparent coordination institution must prevent dominance by any single group through multi-party participation and public rebuttal mechanisms. Fourth, conflicts of interest among financial institutions. Application parties such as custodians, exchanges, stable coin institutions, and Transparent Banks may participate in discussion, but they cannot package their own commercial routes as Bitcoin's public route, nor shift business responsibility to the coordination institution. Fifth, regulatory misrecognition risk. Regulators may mistakenly believe that the transparent coordination institution has legal duties or represents Bitcoin in bearing responsibility. Therefore, the coordination institution must continuously state its nature as non-regulatory, non-custodial, non-asset-representative, and non-compliance-guaranteeing. Sixth, misuse of AI tools. AI can be used for auditing, simulation, and comparison of multiple proposals, but AI outputs cannot be mistaken for decision opinions, and still less can they replace human responsibility and public discussion. Seventh, damage to protocol neutrality. If the coordination institution favors a commercial group, technical route, or regulatory interest in the name of the public, it will in turn damage the neutrality of the public verification network. Therefore, it must adhere to the principle that the Public Credit Root comes first and avoid becoming a tool of interest groups. These risks are not reasons to negate the transparent coordination institution. They are reasons why it must limit itself. Precisely because these risks exist, coordination must be public, limited, challengeable, term-bound, and exit-enabled.

IX. UASF Is the Ultimate Backstop

Any transparent coordination institution must recognize the ultimate backstop status of UASF. The meaning of UASF is that economic nodes and users, in extreme circumstances, can refuse blocks or upgrades that do not conform to the rules they recognize. It embodies the deepest security mechanism of the Bitcoin system: final choice does not belong to the founder, miners, developers, exchanges, or a coordination institution. It belongs to the economic majority as expressed through nodes and markets. A transparent coordination institution cannot replace UASF. It can only function before UASF: identifying problems in advance, organizing discussion, proposing solutions, explaining risks, forming strong signals, reducing the probability of forks, reducing misunderstanding and panic, and helping the economic majority make judgments. If a proposal from the coordination institution cannot gain recognition from the economic majority, it has no vitality. If nodes and markets reject it, it cannot be forced forward. If a major disagreement arises, UASF remains the ultimate backstop. The relationship between the two should be: the transparent coordination institution is responsible for forming public reason, while UASF preserves the final veto. This is precisely where Satoshi is needed now. In the early stage of the second half, public and limited Satoshi participation may be the shortest path to legitimacy and public understanding, while the existence of UASF ensures that no strong signal can become coercive power.

X. Why the Transparent Coordination Institution Can Serve Public Credit Root Applications

The key to Bitcoin's second half is the application of the Public Credit Root. If Bitcoin were only an asset, loose coordination might be enough. But if the Bitcoin system is to become the Public Credit Root of future Verifiable Finance, it must face more complex external connections. Banks need to know how to anchor key-state hashes to Bitcoin. Stable coin institutions need to know how to prove reserves and liabilities. Exchanges need to know how to prove asset-liability consistency. Corporate ledgers need to know how to use public timestamps. Audit institutions need to know how to verify hash anchors. Regulators need to know how to understand Verifiable Finance. AI financial systems need to know how to prevent models and data from being tampered with. Transparent Banks need to know how to embed the Public Credit Root into business processes. These things are not automatically completed by the Bitcoin protocol. They require theory, standards, interfaces, demonstrations, and coordination. A transparent coordination institution can play an important role here: it does not need to control the Bitcoin protocol, but can advance application standards for the Public Credit Root; it does not need to rewrite Bitcoin rules, but can help external financial systems use the Bitcoin system correctly; it does not need to become a regulator, but can help regulators understand Verifiable Finance; it does not need to replace the market, but can reduce misunderstanding and cost in Public Credit Root applications. The true meaning of the transparent coordination institution is not to govern the bitcoin asset, but to release the application capability of the Bitcoin system as a Public Credit Root.

XI. Basic Constitutional Principles of a Transparent Coordination Institution

The minimum constitutional principles for a transparent coordination institution should include at least the following ten. First, the principle of non-coercion: it may not force any node, miner, user, or institution to accept its recommendations. Second, the principle of openness: major issues, discussion processes, proposal texts, objections, and audit reports must be public. Third, the principle of challenge ability: any recommendation must allow public questioning, rebuttal, and competition from alternative proposals. Fourth, the principle of multi-party checks and balances: no single group may monopolize the coordination institution. Fifth, the principle of the economic majority: major recommendations must respect the economic majority and cannot let a minority technical or capital

subject replace market consensus. Sixth, the UASF backstop principle: the final veto power of economic nodes must be preserved. Seventh, the limited-term principle: coordinators cannot harden into a long-term power class. Eighth, the AI audit principle: major proposals must be reviewed jointly by multiple independent AI models and human experts. Ninth, the interest-disclosure principle: participants must disclose major interests related to the issue. Tenth, the Public Credit Root priority principle: the goal of the coordination institution is not to serve a group, but to protect the long-term credibility of the Bitcoin system as a Public Credit Root. The core of these principles is to restrict coordination to the level of "public signal," rather than allowing coordination to evolve into rule.

XII. Why Transparent Coordination Is Not Centralization

Many people will say: as long as an institution is created, it is centralization. This judgment is too simple. The key to centralization is not whether an institution exists, but whether the institution possesses unchallengeable coercive power. If an institution can force nodes to upgrade, freeze assets, change rules, decide which chain is the true chain, and replace user choice, it is of course centralized. But if an institution can only publicly make recommendations, must accept challenge, has no coercive power, cannot replace nodes and markets, and ultimately must be tested by the economic majority, then it is not centralized rule, but a public coordination tool. In fact, Bitcoin has always had coordination, only it has been dispersed, informal, and weakly institutionalized: developer code maintenance is not centralization, BIP proposals are not centralization, security-vulnerability disclosure is not centralization, miner signaling is not centralization, and UASF mobilization is not centralization. Therefore, the question is not "whether coordination exists," but "whether coordination is made transparent, institutionalized, and bounded." The goal of transparent coordination is not to increase centralization, but to reduce the risks of black-box coordination, interest-based coordination, and misunderstood coordination. Without transparent coordination, coordination will still exist, but it will move into the shadows - private coordination among major exchanges, private coordination among large mining pools, private coordination among major developers, private coordination by capital and regulators, and temporary coordination by media and market sentiment. That is more dangerous. The value of a transparent coordination institution is to bring unavoidable coordination into the sunlight.

XIII. Conclusion: Inviting Satoshi Is to Establish a Coordination System That Does Not Require Satoshi to Hold Power

Bitcoin does not need a Satoshi who returns to power - this point must be emphasized repeatedly. But Bitcoin's second half needs Satoshi's thought to be re-understood, the Public Credit Root to

be correctly defined, and problems such as quantum risk, early coins, financial applications, regulatory communication, and Verifiable Finance to enter mature discussion. These tasks cannot be completed by personal authority, nor by loose dispute. They require a transparent coordination institution. The true meaning of "inviting Satoshi" is not to make Satoshi the new center of Bitcoin, but to take Satoshi's thought as a source and promote the creation of a public mechanism that does not allow any person to monopolize interpretive power, any group to monopolize direction, or any coordination to become a black box. In Bitcoin's first half, Satoshi withdrew and made owner lessness possible. In Bitcoin's second half, Satoshi's thought returns and promotes transparent coordination. The ultimate goal is to establish a transparent coordination layer that can continue to serve the Public Credit Root even if Satoshi withdraws again.

What is invited is not authority, but the intellectual source. What is built is not a center, but transparent coordination. What is welcomed is not the return of an individual, but institutional maturity. Satoshi is not a necessary condition for Verifiable Finance to be established, but he may be the strongest catalytic condition for the Bitcoin system to complete the institutionalization of the Public Credit Root. A highly certain Public Credit Root will become a reliable foundation for Verifiable A and push modern finance into the age of Verifiable Finance.

Part IV
The Challenge of Verifiable Finance to the United States

Chapter Fourteen
Why the United States Needs to Understand Cryptocurrency at a Higher Level

—From Digital Asset Regulation to a Verifiable Finance Strategy

The Problem: The United States Has the Strongest Resources, but Has Not Yet Grasped the Greatest Value of Cryptocurrency

The United States has the world's strongest financial system, the deepest capital markets, the leading technology companies, the most active venture capital, the strongest AI companies, and the most mature global dollar network. It is also one of the most important participants in the global cryptocurrency market. Bitcoin ETFs have already been recognized. Stable coins are mainly denominated in dollars. Technology and AI giants are concentrated in the United States. Wall Street is accelerating its entry into the digital asset market. Regulators, Congress, courts, and state governments continue to discuss crypto policy. More and more political figures are also beginning to realize that cryptocurrency is no longer merely fringe speculation, but part of national competitiveness. It should be acknowledged that the United States has already done a great deal of work in the cryptocurrency field and remains one of the most important leaders in this field. Yet a deeper problem still exists: the United States has not yet truly understood the greatest value of cryptocurrency. The United States has already seen Bitcoin's potential as a strategic asset, but it has not yet fully understood the potential of the Bitcoin system to change the future of finance. The United States has already seen the function of stable coins in expanding the dollar's influence, but it has not yet fully grasped the strategic meaning of the Bitcoin system as a Public Credit Root. In short, a Public Credit Root is like a mathematical axiom: it is the starting point of the theorem and the anchor of the theory. The fundamental anchor of Verifiable Finance theory is precisely the Public Credit Root provided by the Bitcoin system. Bitcoin and gold are both extremely important, but they are not anchors at the same level. Gold is a static asset. The bitcoin asset is a digital scarce good. The Bitcoin system, however, is a Public Credit Root that can be referenced, anchored, and verified by external systems. The United States currently treats cryptocurrency more as a regulatory object and asset class, but it has not yet fully recognized that the starting point of the next-generation financial system lies here. There is a seemingly contradictory phenomenon here: if the Public Credit Root is so important, why do many institutions still tend to build their own chains, consortium chains, or closed ledgers, rather than directly referencing the Bitcoin system? The reason is not merely technical bias or institutional inertia. More fundamentally, the certainty of the Public Credit Root has not yet been sufficiently explained, institutionalized, and accepted. Major finance will not incorporate a system into core infrastructure merely because that system is technologically advanced. It must first confirm that this credit root is sufficiently stable, explainable, coordinable, that its responsibility boundaries are sufficiently clear, and that it can be absorbed by institutions over the long term. In this sense, if the United States wants to truly grasp the strategic value of cryptocurrency, it cannot merely regulate digital assets; it must participate in building the certainty of the Public Credit Root. If viewed only from the perspective of financial regulation, cryptocurrency is easily misread as a new asset class. If viewed only from the perspective of technological innovation, it may be seen as financial technology. If viewed only from the perspective of monetary competition, it will be treated as a tool for dollar stable coins. If viewed only from the perspective of investment markets, it is merely another risk asset. If viewed only from the perspective of national reserves, it is no more than digital gold. All of these understandings contain partial truth, but all are only partial observations. This book has repeatedly explained around Verifiable Finance that the core concept being severely underestimated is the Public Credit Root. After more than ten years of exploration, and with the rise of AI technology, Satoshi Nakamoto's forward-looking vision now has more realistic conditions for implementation. Cryptocurrency is standing at a historical threshold. It will push the financial system based on double-entry bookkeeping since the Industrial Revolution from internal institutional constraints toward externally verifiable constraints based on the Public Credit Root. Only through the Bitcoin system as a Public Credit Root Can

Transparent Banks and Transparent Finance obtain a real foundation. Once the Public Credit Root is widely adopted, the Bitcoin system will no longer be merely a digital asset network, but may become the base layer of a new finance. The core theme of this book is this: how can the future financial credit system move from institutional promises to verifiable facts? This is precisely the fundamental reason why the United States must re-understand cryptocurrency at a higher level.

I. The United States Currently Treats Cryptocurrency Mainly as a Regulatory Object

The American discussion of cryptocurrency has long revolved around specific regulatory issues: Is Bitcoin a commodity? Do certain tokens constitute securities? Do exchanges need to register? Do stable coins require reserve regulation? Does DeFi create money-laundering and fraud risks? How should taxation apply? How should ETFs enter traditional markets? How should custodians protect assets? How should KYC/AML apply? All of these questions are critically important, but in essence they still belong to a regulatory-object mindset. This mindset treats cryptocurrency as an emerging industry and then asks: What risks does it create? Who should regulate it? What laws should apply? How can compliance be achieved? How can investors be protected? This thinking is necessary in the short term, but it has a fundamental limitation: it treats cryptocurrency only as an object to be regulated, rather than elevating cryptocurrency into a new financial infrastructure that may reconstruct the logic of regulation itself. Traditional regulation relies on institutional reporting, licensing, after-the-fact audits, enforcement penalties, and internal control examinations. Regulators must believe that the data submitted by institutions is basically true, that audits can discover problems, that internal controls can constrain risks, and that misconduct can be effectively held accountable after it occurs. The new possibility brought by cryptocurrency is that certain key financial facts can be continuously verified through technical structures. Whether reserves exist, whether liabilities are real, whether transactions occurred, whether assets were misappropriated, whether ledgers were tampered with, whether clearing results are valid, whether permissions were abused, and whether risk states have changed can all be verified in real time or periodically. If these facts can be continuously proven through technical structures, regulation can move from checking institutional statements after the fact to continuously verifying whether facts hold. This is the real regulatory lesson of cryptocurrency. The current problem in the United States is precisely that it is still mainly handling cryptocurrency within the old regulatory framework, and has not yet raised it to the level of next-generation financial regulation and financial transparency infrastructure.

II. Cryptocurrency Is Not Only a New Asset Class, but a Tool for Reconstructing the Credit System

Many people understand cryptocurrency simply as a new asset class. This perspective is useful for investment markets, but it remains insufficient for financial institutional transformation. Bitcoin, Ethereum, stablecoins, tokenized Treasuries, on-chain funds, NFTs, RWA, and other instruments can all be viewed as assets. But if the analysis stops there, their far-reaching institutional meaning will be missed. What cryptocurrency truly changes is the way credit is generated. Traditional financial credit comes from institutional trust: trusting banks to keep accounts correctly, central banks to maintain monetary order, exchanges not to misappropriate assets, auditors to perform their duties carefully, custodians to safeguard assets properly, regulators to discover problems in time, and courts to handle disputes fairly. This system has supported modern finance, but its core remains institutional credit. Satoshi Nakamoto proposed another credit structure: trust is no longer built only by believing institutions, but by verifying rules, ledgers, signatures, hashes, states, and history. What he created was not merely a digital asset, but a public machine credit root that does not require trust in any individual, company, or central bank. Ethereum further extended this capability into a programmable rule platform. This means that cryptocurrency has opened a new credit paradigm: from trusting institutions to verifying facts. If the United States treats cryptocurrency only as an asset market, it will continue to focus on price, ETFs, custody, exchanges, and investor protection. If it understands cryptocurrency as a tool for reconstructing the credit system, it will begin to build new frameworks for reserve verification, liability verification, clearing verification, bank transparency, stable coin credibility, exchange proof of assets and liabilities, and AI continuous auditing. The former is regulating a market; the latter is defining the next financial order.

III. Stable coins Are Not the End Point, but the Transitional Interface Through Which the Dollar Enters Verifiable Finance

Stable coins are the most accessible strategic entry point for the United States to understand cryptocurrency. They are denominated in dollars and naturally connect the dollar system, payment systems, exchanges, cross-border settlement, and on-chain finance. Their strategic value in expanding the dollar's influence in the digital world is obvious. But if stable coins are understood only as tools for dollar expansion, the essence is still missed. Stable coins are not the end point, but the transitional interface through which the dollar moves toward the era of Verifiable Finance. The core question is not whether they are denominated in dollars, but whether they are truly verifiable: Are the reserves real? Are the assets sufficient? Is there maturity mismatch or collateral reuse? Are there undisclosed liabilities? Can redemption be honored under stress? Is continuous auditing accepted? Can machine-verifiable proof of reserves be provided?

If these questions cannot be continuously verified, a stable coin is merely an on-chain extension of traditional dollar credit. It may be more efficient, but it is not truly transparent.

It may expand the dollar's influence, but it still preserves the financial black box. The next step should be to advance stable coins from dollar tokens to verifiable dollars: make proof of reserves real-time, make liability scale clear, make custody structures transparent, make clearing and redemption traceable, anchor key states to the Public Credit Root, use AI audits to continuously monitor anomalies, and move regulation from periodic reports toward continuous verification. If the United States takes the lead in establishing such standards, the dollar will gain a new institutional advantage. The old advantage came from American national strength, fiscal credit, military power, capital markets, and global clearing networks. The new advantage can come from transparency, verifiability, technical standards, and globally trusted infrastructure. This is the true strategic meaning of stable coins for the United States: stable coins bring the dollar on-chain; Verifiable Finance brings the dollar out of the black box.

IV. AI Is Changing the Logic of Financial Security and Regulation

Another important reason the United States has not yet fully understood cryptocurrency is that it has not placed AI and cryptocurrency within the same framework of financial security.

AI is profoundly changing the offensive and defensive structure of financial systems. In the past, financial attacks required professional hackers and high technical thresholds. In the future, AI can automatically read code, discover vulnerabilities, generate phishing content, simulate attack paths, analyze smart-contract composability risks, induce users to sign, and even attack front ends and wallets at scale. This will overturn old security assumptions: open source is no longer naturally secure, manual audit and periodic compliance inspection are no longer sufficient, and after-the-fact punishment and static risk-control models are no longer enough. Attackers are continuously online, and defenders must also be continuously online. Financial security is moving from periodic audit to continuous verification. AI is also a powerful defensive tool. It can be used for code auditing, transaction monitoring, anomaly detection, reserve verification, liability analysis, compliance screening, attack simulation, and risk warning. The real challenge is this: who can organically combine AI, the Public Credit Root, and financial regulation to build a new system of continuous verification? The United States has the world's strongest AI and the strongest finance. If the two remain separate, it will miss an opportunity for institutional innovation. The next generation of financial security is likely to come from the following combination: the Public Credit Root provides final anchoring, Verifiable Finance provides factual proofs, AI auditing provides continuous inspection, the regulatory system provides legal boundaries, and the Transparent Bank provides the commercial form. If the United States can integrate these elements first, it will no longer merely regulate cryptocurrency; it will define the financial security standards of the AI era. Although transparent and verifiable financial systems have long been difficult to implement because of engineering complexity, the emergence of AI is significantly reducing this obstacle. Taking the Transparent Bank as an example, its theoretical design has already shown feasibility with AI assistance. At current technological levels, building a transparent banking system that can be piloted, iterated, and operated stably is no longer a distant idea, but an engineering objective that can be advanced in the near term.

V. If the United States Only Regulates Cryptocurrency, It Will Miss the Opportunity to Lead Verifiable Finance

Regulation is necessary, but regulation alone is far from enough. The true challenge for the United States is not whether to regulate cryptocurrency, but whether to lead Verifiable Finance. The two are fundamentally different. Regulating cryptocurrency treats it as a risk object, focusing on preventing fraud, money laundering, market manipulation, asset misappropriation, and systemic risk. Leading Verifiable Finance transforms the Public Credit Root, cryptographic proofs, and verifiable ledger capabilities into the next generation of financial institutional advantages, focusing on new standards for making reserves, liabilities, clearing, permissions, risks, and responsibility traceable. Regulation addresses current risks. Leadership competes for the future financial order. If the United States only regulates without building, only punishes without defining, only prevents risks without creating standards, treats stable coins merely as tools without advancing verifiable dollars, treats Bitcoin merely as a reserve without understanding the Public Credit Root, and treats blockchain merely as financial technology without grasping credit reconstruction, it may lose leadership in the theory and infrastructure of the next generation of finance. The strength of the dollar system comes not only from issuance power, but also from the fact that the United States once defined global financial rules, clearing rules, audit rules, accounting rules, securities rules, and international order. In the next era, the United States must define rules again. The core of these new rules should not be merely who may issue tokens, but should focus on: Which financial facts must be verifiable? How should reserves be verified? How should liabilities be verified? How should exchanges prove that they have not misappropriated assets? How should stable coins prove redeemability? How should banks prove key ledger states? How should AI audits enter regulatory processes? How should the Public Credit Root become an external proof layer? How should customer privacy and regulatory penetration be balanced? How should centralized institutions continue to operate while accepting verification? This is the meaning of a Verifiable Finance strategy.

VI. The United States Should Establish a Verifiable Finance Strategy

What the United States needs is not scattered cryptocurrency policies, but a complete Verifiable Finance strategy. It should include at least the following eight directions.

1. Establish recognition of the Public Credit Root: make clear that the core value of a small number of public networks such as Bitcoin and Ethereum lies in Public Credit Roots and Verifiable Finance infrastructure, not merely in assets or application platforms.

2. Actively participate in building the certainty of the Public Credit Root: promote open, transparent, and non-coercive international discussion around quantum risk, early addresses, long-term security, standard interfaces, and public coordination, so as to stabilize the foundational anchor of Verifiable Finance.

3. Promote verifiable stable coin standards: move from periodic audits toward higher-frequency, more transparent, and more verifiable proofs of reserves and liabilities.

4. Establish exchange asset-liability verification standards: break the black-box custody model so that customer assets, platform liabilities, cold-wallet reserves, and risk exposures are gradually incorporated into a verifiable framework.

5. Promote pilots for verifiable bank ledgers: without disclosing all customer data, anchor key state summaries, reserve proofs, clearing results, and audit logs to the Public Credit Root.

6. Establish an AI continuous-audit framework: continuously monitor code, transactions, reserves, liabilities, permissions, risks, abnormal behavior, and compliance status.

7. Formulate principles of layered disclosure: facts must be verifiable, while disclosure may be layered; customer privacy should be protected, but key facts must be provable.

8. Promote state-level and federal-level experiments: allow some states to pilot institutional innovations such as Transparent Banks, verifiable stable coins, AI financial auditing, and Public Credit Root anchoring.

This is not an ordinary fintech policy, but a next-generation financial infrastructure strategy for the United States.

Conclusion: The United States Needs to Redefine Financial Transparency The United States currently has significant advantages, but in the era of Verifiable Finance, Europe, Japan, and even China also have their own advantages. The financial ledgers of any country or any organization need transparency. This can solve not only cryptocurrency problems, but also the pain points of the fiat system. The speed of this competition will be determined by AI.

The United States needs to redefine the meaning of financial transparency: from institutional promises to verifiable facts, from black boxes to auditability, from trusting institutions to verifying facts. This is the true strategic meaning of cryptocurrency for the United States.

Cryptocurrency is not the enemy of the American financial system, but an opportunity for the United States to redefine financial transparency. What the United States truly needs to do is not merely regulate cryptocurrency, but lead Verifiable Finance. This is the best opportunity for the United States.

Chapter Fifteen
Using Stablecoins to Explain the Importance of Verifiable Finance

—*From Dollar Tokens to Verifiable Stablecoins*

Introduction: Stablecoins Are the Practical Entry Point for the United States to Understand Verifiable Finance

If the Bitcoin system provides the Public Credit Root for Verifiable Finance, then stablecoins are the most direct and realistic entry point for the United States to enter the era of Verifiable Finance. The reason is simple: stablecoins are no longer a marginal experiment. They have become an important unit of account, medium of exchange, cross-border payment tool, and on-chain dollar carrier in the cryptocurrency market. A large number of stablecoins are denominated in dollars, and behind them stand U.S. Treasuries, dollar deposits, the banking system, payment networks, custodians, exchanges, and global users. For the United States, stablecoins are both a bridge through which the dollar enters the digital world and an opportunity to redefine financial transparency. The problem is that if stablecoins are understood only as tools for dollar expansion, their true institutional value will be underestimated. The value of stablecoins is not merely to bring the dollar on-chain. The future of stablecoins is to bring the dollar into the era of Verifiable Finance.

A verifiable stablecoin does not mean simply issuing more dollar stablecoins, nor does it mean having more exchanges price in USDT, USDC, or other dollar tokens. What it truly seeks to solve is a deeper set of questions: Are the reserves real? Are the liabilities clear? Can redeemability be proven? Is the custody structure transparent? Is the redemption process traceable? Can risk exposure be continuously monitored? Can key states be anchored to a Public Credit Root? Can regulation move from periodic reports to continuous verification? If these questions cannot be solved, stablecoins are merely an on-chain extension of traditional dollar credit: more efficient, but still preserving a black box; expanding the dollar's influence, but not truly improving the credibility of the dollar system. Therefore, the core question of this chapter is this: stablecoins are not the end point, but the transitional interface through which the dollar enters the era of Verifiable Finance. What the United States should truly pursue is not merely the expansion of dollar stablecoin scale, but verifiable stablecoin standards.

I. What Is a Verifiable Stablecoin?

A verifiable stablecoin is a stablecoin whose reserves, liabilities, redeemability, and key risk states can be independently, continuously, and tamper-resistently verified. It no longer relies mainly on users' unilateral trust in the issuer, but uses cryptographic proofs, anchoring to a Public Credit Root, and AI continuous auditing to turn key financial facts into a reviewable evidentiary structure. In other words, an ordinary stablecoin asks users to believe that it has reserves; a verifiable stablecoin allows users, auditors, regulators, and the market to prove that it has reserves. This distinction is extremely important. If a stablecoin is only a dollar token, it is still essentially the on-chain expression of traditional financial credit. Only when a stablecoin enters a verifiable structure can it become a realistic entry point for Verifiable Finance. The following sections begin from the verifiability problems of current stablecoins and explain how dollar tokens can be upgraded into verifiable stablecoins.

II. The Core Question for Stablecoins Is Not Whether They Are Dollar-Denominated, but Whether They Are Verifiable

When people hear the term stablecoin, they often think the core issue is price stability: as long as one stablecoin is roughly equal to one dollar, the mission has been accomplished. But this is only the surface. The real core issue of a stablecoin is not whether it claims to equal one dollar, but whether it can prove that it truly has the capacity to maintain that promise. In other words, the core is not price anchoring, but credit anchoring. A dollar stablecoin must answer the following questions: Where are the reserves? What are the reserves? Are they sufficient? Can they be liquidated in time? Have they been pledged or reused? Does the issuer have undisclosed liabilities? Can it redeem under concentrated redemption pressure? Is the custodian bank reliable? Is the audit timely? Is on-chain issuance consistent with off-chain reserves? If these questions cannot be verified, the stablecoin remains institutional credit. Users trust the issuer, the market trusts reserve reports, regulators trust disclosures, and the

III. Current Stablecoins Still Preserve the Black Box of Traditional Finance

On the surface, stablecoins are on-chain assets, but their credit foundation depends heavily on the off-chain financial system.

On-chain, one can see issuance volume, transfer records, and address balances. But ordinary users cannot directly verify where the off-chain reserves are, what their structure is, how they are custodied, or what redemption pressure exists. This creates the fundamental contradiction of stablecoins: on-chain transparency is high, while off-chain systems remain black boxes. This black box includes at least five layers. First, the reserve black box. Users find it difficult to confirm in real time the authenticity, completeness, liquidity, and legal ownership of reserve assets.

Second, the liability black box. The issuer's overall liabilities, undisclosed obligations, and related-party risks may not be fully transparent. Third, the custody black box. Reserve assets are held in banks or custodians, but users cannot directly verify asset segregation status or priority rights in emergencies. Fourth, the redemption black box. Redemption capacity depends not only on reserve size, but also on processes, banking channels, and liquidity management. Users usually discover whether the system is robust only after risk is exposed. Fifth, the regulatory black box. Regulation still relies on materials submitted by institutions and periodic inspections, making continuous verification difficult. This shows that stablecoins have improved the circulation efficiency of the dollar, but they have not yet solved the black-box problem of traditional finance. If the United States wants stablecoins to become a new advantage of the dollar system, it cannot be satisfied with regulation, disclosure, and audit. It must push stablecoins into a Verifiable Finance framework.

IV. From Dollar Tokens to Verifiable Stablecoins

Dollar tokens and verifiable stablecoins are not the same thing. A dollar token maps a dollar claim or dollar value onto a blockchain, and its core is circulation efficiency. A verifiable stablecoin brings reserves, liabilities, redeemability, and key risk states into a verifiable structure, and its core is financial credibility. A dollar token answers: Can the dollar circulate on-chain? A verifiable stablecoin answers: Is the on-chain dollar promise real and reliable? The former solves payment and trading problems. The latter solves credit and regulatory problems. To advance stablecoins into verifiable stablecoins, at least six key transitions are required. First, from periodic disclosure to continuous proof. Higher-frequency, more automated, and more machine-readable reserve and liability proofs must be introduced. Second, from unilateral statements to multi-party verification. Issuers, banks, custodians, auditors, Public Credit Roots, and AI audit systems together form a verification network. Third, from on-chain transparency to on-chain/off-chain proof consistency verification. It is not enough to see on-chain circulation volume; the correspondence between off-chain reserves and on-chain liabilities must be verified through reference chains and proof structures. Fourth, from institutional credit to structural credit. Credit comes from a verifiable structure, not merely from brand, license, and reputation. Fifth, from compliance reports to computable regulation. Regulatory materials must gradually become computable, traceable, and automatically comparable data structures. Sixth, from single audits to AI continuous audits. AI helps detect abnormal flows, reserve fluctuations, redemption pressure, maturity mismatch, and related-party risks. Only after these transitions are completed can stablecoins truly become verifiable stablecoins.

V. The Role of Public Credit Roots in Stablecoins

For stablecoins to enter the era of Verifiable Finance, the Public Credit Root must be introduced. The meaning of the Public Credit Root is not to replace issuers, banks, custodians, auditors, or regulators, but to provide an external tamper-resistant proof layer. A stablecoin system can form hash values from key state summaries and anchor them to the Bitcoin system or another highly trusted Public Credit Root. These summaries may include total issuance summaries, reserve proof summaries, liability structure summaries, custody confirmation summaries, redemption state summaries, audit log summaries, and risk indicator summaries. These summaries do not need to expose all commercial data or customer privacy, but they can form a tamper-resistant time series. Any auditor, regulator, or properly authorized subject can verify whether the key state at a certain point in time is consistent with later disclosure, whether it has been modified, whether it has been deleted, or whether it has been rewritten after the fact. The problem of traditional finance is this: ledgers are inside institutions, audits happen after the fact, disclosures are delayed, and users can only trust. The direction of verifiable stablecoins is this: key facts form summaries, summaries are anchored to the Public Credit Root, and audit and regulation can continuously verify them. The role of the Bitcoin system here is not to serve as a reserve asset, but as a proof layer. This is precisely why the United States cannot only discuss whether to hold Bitcoin; it must understand how to use the Bitcoin system as a Public Credit Root.

VI. AI Auditing Will Become Critical Infrastructure for Stablecoin Security

Once stablecoins expand in scale, their risks are not merely technical risks, but may become systemic financial risks. Traditional manual audits cannot meet this speed and complexity. AI auditing can undertake multiple functions in future stablecoin systems: continuously monitoring on-chain circulation and address distribution; detecting abnormal minting, burning, concentrated transfers, and redemption pressure; continuously analyzing reserve structures, including asset maturity, liquidity, concentration, and interest-rate risk; continuously comparing on-chain liabilities with off-chain reserves to detect inconsistencies, lags, or abnormal changes;

continuously monitoring custody and banking risks and dynamically evaluating them together with market data; continuously simulating stress scenarios, including concentrated redemption, market panic, and banking-channel interruption; and continuously generating regulatory alerts that turn complex risks into accountable risk signals. But AI auditing cannot independently constitute a credit root. AI can also make errors, be attacked, or draw wrong conclusions from wrong data. Therefore, the most reasonable structure is this: AI provides continuous analysis, the Public Credit Root provides tamper-resistant evidence, and law and regulation provide responsibility boundaries. Only the combination of the three forms the security foundation for stablecoins entering the era of Verifiable Finance.

VII. Stablecoin Regulation Should Be Upgraded from Reserve Regulation to Verification Regulation

Stablecoins of course require reserve regulation, but reserve regulation alone is not enough. The next stage should be upgraded into verification regulation. Its core question is no longer merely whether an institution has submitted a report, but whether key financial facts can be independently verified. Stablecoin verification regulation should include at least seven aspects. First, issuance verification. On-chain total supply must remain consistent with the issuer's liability records. Second, reserve verification. Reserve assets should be cross-proven through banks, custodians, auditors, and regulatory interfaces. Third, liability verification. Liability scale, outstanding obligations, and potential risks must be proven. Fourth, redemption verification. Redemption requests, speed, failure rates, and stress states should enter the scope of regulatory visibility. Fifth, custody verification. It must be proven whether assets are segregated, pledged, or reused, and whether the relevant legal relationships are clear. Sixth, risk verification. Maturity mismatch, liquidity risk, concentration risk, and similar issues should be continuously monitored. Seventh, historical verification. Key state summaries should be anchored to the Public Credit Root to form a tamper-resistant history. This is the upgrade direction of stablecoin regulation: from examining institutions to verifying facts, from periodic disclosure to continuous proof, from manual audits to AI-assisted audits, from report-based regulation to computable regulation, and from dollar tokens to verifiable stablecoins.

VIII. Verifiable Stablecoins Will Strengthen, Not Weaken, the Dollar's Position

Some people worry that if stablecoins enter a Verifiable Finance framework, the dollar system may be weakened. This worry remains trapped in old thinking. The real question is not whether the dollar will be constrained, but whether the dollar system can continue to earn global trust in the era of AI and cryptocurrency.
If dollar stablecoins can take the lead in achieving verifiable reserves, verifiable liabilities, verifiable redemption, and verifiable risks, the international position of the dollar will instead be strengthened. The reason is simple: global users will be more willing to use a dollar stablecoin that not only has strong liquidity, but whose key facts are also verifiable. A verifiable stablecoin does not weaken the dollar; it upgrades dollar credit. It moves the dollar from trusting the American system toward verifying dollar facts, making the on-chain dollar not merely a unit of circulation, but a standard for trustworthy financial facts. This will be an important path for the United States to maintain financial leadership in the era of the Public Credit Root.

IX. The United States Should Take the Lead in Establishing Verifiable Stablecoin Standards

If the United States wants to lead the stablecoin era, it should not be satisfied with passive regulation. It should actively establish verifiable stablecoin standards. This set of standards may include eight aspects. First, standards for reserve asset layering. The risk levels, liquidity requirements, and disclosure methods for assets such as cash, bank deposits, and short-term Treasuries should be clearly defined. Second, standards for proof-of-reserve frequency. Proof should move gradually from monthly or quarterly toward higher-frequency and automated proof. Third, standards for on-chain liability synchronization. Issuance volume and internal liability systems should remain verifiably consistent. Fourth, standards for Public Credit Root anchoring. Key state summaries should be anchored to a Public Credit Root according to rules. Fifth, standards for AI audit interfaces. Machine-readable data interfaces should be provided for compliance AI, audit AI, and regulatory systems to conduct continuous analysis. Sixth, standards for proof of custody segregation. Legal ownership of assets, bankruptcy remoteness, and priority arrangements should be structurally disclosed and verifiable.
Seventh, standards for stress-scenario disclosure. Verifiable liquidity stress-test results should be continuously queryable and reviewable. Eighth, standards for balancing user privacy and regulatory penetration. All user privacy must not be exposed, but stablecoins must not become unauditable black boxes. If these standards are established by the United States first, they will form global influence. The stablecoin market is naturally linked to the dollar. Whoever defines verifiable stablecoins may define the next generation of the digital dollar order.

X. The Future Competition of Stablecoins Is a Competition for Greater Credibility

Stablecoins will certainly continue to grow, but scale is not the final standard. A very large stablecoin with opaque reserves and unverifiable risks may become a source of systemic risk. A more mature stablecoin system should pursue credibility, verifiability, and resilience. Stablecoin competition will ultimately become competition between credit structures: whose reserves are more verifiable, whose liabilities are more transparent, whose redemption is more reliable, whose risks are more monitorable,

whose audits are more continuous, and whose key states are harder to tamper with. The first half of stablecoins brought the dollar on-chain. The second half of stablecoins will make on-chain dollar promises verifiable.

Conclusion: Dollar Stablecoins Are Only the Beginning; Verifiable Stablecoins Are the Direction Stablecoins are important not merely because they already have market scale, but because they are the first type of financial product through which Verifiable Finance is easiest to implement. Through stablecoins, reserves, liabilities, redemption, custody, and risk states can be verified first. As these mechanisms mature, exchanges, custodians, and banks can further be pushed into verifiable structures. Therefore, verifiable stablecoins are not isolated products, but the preliminary testing ground for Transparent Banks and the Transparent Dollar.

Stablecoins are not the endpoint of cryptocurrency, nor the endpoint of dollar strategy. They are only the transitional interface through which the dollar enters the era of Verifiable Finance.

If the United States treats stablecoins only as tools for dollar expansion, it will gain a short-term advantage but miss an institutional upgrade. If the United States advances stablecoins into verifiable stablecoins, it may redefine financial transparency in the digital age.

The future competitiveness of the dollar depends not only on American national strength, capital markets, and clearing networks, but also on whether the dollar system can become more transparent, more verifiable, and more trustworthy.

The meaning of verifiable stablecoins is this: reserves are no longer merely statements, but proofs; liabilities are no longer merely reports, but verifiable states; clearing is no longer merely an internal process, but a verifiable result; regulation is no longer merely after-the-fact inspection, but continuous verification; and the on-chain dollar is no longer merely a unit of circulation, but a core standard for Verifiable Finance in the AI era. Stablecoins bring the dollar on-chain.

Verifiable Finance brings the dollar out of the black box.
This is the historical opportunity the United States should seize.

Chapter Sixteen
The United States Needs Cryptocurrency Regulation, but It Needs a Verifiable Finance Strategy Even More

—From Regulating New Assets to Defining a New Financial Paradigm

Introduction: Regulation and Strategy Must Advance Together

Chapter Fourteen discussed why the United States must re-understand cryptocurrency at a higher level. This chapter further discusses how that understanding can be transformed into a regulatory framework, infrastructure standards, and national strategy. The former answers why; this chapter answers how. Exchanges, stablecoins, and custodians need regulation. Fraudulent projects, money-laundering risks, and market manipulation need to be combated. Customer assets, tax rules, and financial attributes also need to be protected and defined. Such regulation is of course necessary and urgent, but it mainly addresses current risks and cannot automatically define the future financial order. The true transformation brought by cryptocurrency is not that financial markets have gained a new class of digital assets, but that the structure of financial credit is undergoing fundamental change: traditional finance relies on institutional credit, while cryptocurrency opens machine credit; traditional regulation relies on institutional reports and after-the-fact audits, while Verifiable Finance requires key facts to be independently verifiable; the core question of traditional finance is whether institutions are trustworthy, while the core question of Verifiable Finance is whether facts are provable. If the United States only regulates cryptocurrency, at most it is defending against risks. If the United States can lead Verifiable Finance, it will have the opportunity to establish the future financial paradigm. This chapter discusses a Verifiable Finance strategy from the regulatory perspective: it does not mean relaxing regulation, nor does it mean putting all financial activity on-chain. It means combining the Public Credit Root, the Chainless system, Transparent Banks, AI continuous auditing, and legal responsibility to establish next-generation standards for financial transparency.

I. The Old Model Is After-the-Fact Regulation; the New Strategy Is Continuous Verification

The current primary task of regulation is to handle risks. But if policy stops there, the United States will miss a larger institutional opportunity. Cryptocurrency not only brings new risks; it also provides new governance tools: ledgers, asset states, issuance rules, reserve summaries, historical records, and permission changes can all be verified, and key facts can obtain external proof through the Public Credit Root. The old model is this: institutions submit reports, auditors inspect after the fact, regulators conduct periodic reviews, and enforcement penalties occur after problems are exposed. The new model is this: key facts are continuously proven, important states are anchored to the Public Credit Root, AI auditing continuously monitors them, and regulators observe changes in risk through computable interfaces. Therefore, regulating cryptocurrency is only the first step. Leading Verifiable Finance is the next step. Risk regulation asks: How can cryptocurrency be prevented from harming the existing financial system? A Verifiable Finance strategy asks: How can the new capabilities provided by cryptocurrency be used to upgrade the existing financial system? The former is defense; the latter is construction. The United States cannot merely be a defender.

II. From Regulating Institutions to Verifying Facts: The Regulatory Paradigm Is Different

Traditional financial regulation is built on mature systems such as licensing, capital requirements, audits, disclosure, and enforcement. It has supported the modern financial system and cannot simply be denied. But its natural limitation is that regulatory attention mainly falls on institutions, rather than directly on key facts. Institutions can lie, reports can be falsified, audits can lag, and risks can be hidden. Verifiable Finance does not abolish regulation; it upgrades regulation. It moves the regulatory object from whether institutions are trustworthy

toward whether key facts are verifiable. Regulatory agencies remain important. Law remains important. Licensing and compliance remain important. But they should be built on a more verifiable factual foundation. This is the transformation of the regulatory paradigm: not using technology to replace regulation, but using verifiable facts to strengthen regulation; not asking regulators to give up judgment, but giving regulatory judgment a more reliable, more continuous, and more reviewable factual basis.

III. Which Key Facts Should Be Verified?

Verifiable Finance does not require all data to be public. It requires key financial facts to be independently verifiable under authorized conditions. At a minimum, it should include the following seven categories of facts. Whether reserves exist: stablecoins, banks, custodians, and similar institutions must provide verifiable evidence for the existence, ownership, and state of reserves.

Whether liabilities are clear: institutions should not only prove assets, but also prove liability boundaries and redemption obligations.

Whether assets have been misappropriated: exchanges, custodians, and platform enterprises must prove that customer assets have not been misappropriated, pledged, or reused.

Whether clearing has been completed: payment, settlement, delivery, and redemption should have traceable and verifiable evidence.

Whether permissions have been abused: key operations, signing permissions, system upgrades, and fund transfers should have logs and verification mechanisms.

Whether risks have been hidden: maturity mismatch, leverage, liquidity, concentration, and related-party risks should be continuously monitored.

Whether history has been tampered with: key state summaries should be anchored to the Public Credit Root to form a tamper-resistant external time series.

These facts cannot be solved by traditional reports alone. They require new technical structures. Regulation should be upgraded from self-reporting plus audit plus enforcement to factual proof plus public anchoring plus AI continuous auditing plus legal responsibility.

IV. The Foundational Layers of a Verifiable Finance Strategy

Verifiable Finance is not a single technology, but a structure. It includes at least five foundational layers. Public Credit Root: a small number of highly trusted public networks such as Bitcoin and Ethereum provide an external tamper-resistant evidence layer. They do not replace banks, law, or regulators, but provide public anchors that institutions cannot unilaterally tamper with.

Connecting bridge: the Chainless system. The Chainless system here is not another public chain, but an intermediate layer that converts off-chain financial facts into verifiable structures. Through designs such as transparent general ledgers, sub-ledgers, hash indexes, Bitcoin anchoring, and TSS/MPC cross-chain mechanisms, the Chainless system builds a Web3 operating-system kernel suitable for financial business, allowing facts to enter verifiable structures as they are formed. Transparent Bank: a Transparent Bank does not simply put a bank on-chain. It brings the bank into a verifiable structure, preventing the bank from operating for long periods outside structures of truthfulness and forming a financial base of verification plus constraint. AI continuous auditing: AI continuously monitors code, ledgers, transactions, reserves, liabilities, permissions, and risks, helping discover problems that human audits may not catch in time. But AI cannot independently constitute a credit root. It must be built upon the Public Credit Root, the Chainless system, and legal responsibility. Legal responsibility: Verifiable Finance cannot use code to replace law. Instead, it allows law to be built on more verifiable facts. The reasonable structure is this: the Public Credit Root provides evidence, AI auditing identifies risk, law defines responsibility, and financial institutions accept verification constraints.

V. Establishing Verifiable Finance Infrastructure Standards

Standards should begin from practice and gradually become standardized. They should include at least eight directions. Public Credit Root anchoring standards: define anchoring frequency, failure handling, re-verification mechanisms, and evidence preservation methods.

Proof-of-reserve standards: replace simple periodic reports with verifiable proof of reserves. Proof-of-liability standards: assets and liabilities must be verified at the same time, avoiding a situation in which assets are proven but obligations are not. Customer asset segregation proof standards: prove that customer assets have not been misappropriated, pledged, or reused. AI audit interface standards: establish machine-readable risk-data interfaces. Layered disclosure standards: facts must be verifiable, while disclosure can be layered, balancing privacy, trade secrets, and regulatory penetration. Permission and operation log standards: key operation logs must be auditable, traceable, and difficult to tamper with. Legal responsibility mapping standards: every verifiable fact should correspond to real-world legal responsibility. Once these standards are formed, the United States will not merely be regulating cryptocurrency; it will be defining the next generation of financial infrastructure.

VI. Three Testing Grounds: Stablecoins, Exchanges, and Banks

A Verifiable Finance strategy should begin with the areas easiest to implement. It should not cover all financial business from the beginning. Three testing grounds are most suitable for early trials. Stablecoins: large in scale, clear in risk, and directly related to the dollar strategy, they are suitable for first establishing verification of reserves, liabilities, redemption, and risk. Centralized exchanges: whether customer assets have been misappropriated, whether platform liabilities are real, and whether cold-wallet reserves are sufficient should be incorporated into a verifiable framework. Banks: all data need not be made public, but key states, including reserves, liabilities, clearing, audit logs, and risk indicators, should be verifiable in layers. This path is gradual: begin with stablecoins, then move to exchanges, and eventually enter banks. It neither destroys the existing financial order nor prevents that order from being upgraded through verification.

VII. Clarifying a Misunderstanding: Transparency Does Not Mean Full Public Disclosure

Verifiable Finance is often misunderstood as making all data public. This is wrong. Finance requires transparency, but it also requires privacy. It requires regulatory penetration, but also customer protection. It requires auditability, but also trade secrets. The correct principle is: facts must be verifiable, while disclosure can be layered. Bank customer data, trade secrets, trading strategies, and personal privacy do not need to be disclosed to the whole world. But key facts must be verifiable under authorized conditions. Reserves, liabilities, clearing, whether assets have been misappropriated, and whether the system has tampered with key states must all be provable. This is structured transparency, not naked transparency. If the United States understands this point, Verifiable Finance will have a realistic path to implementation.

VIII. Policy Framework: From Regulatory Checklist to National Strategy

A United States Verifiable Finance strategy can form a basic policy framework. First, recognize the institutional significance of the Public Credit Root. Second, establish verifiable stablecoin standards. Third, promote verification of assets and liabilities for centralized exchanges. Fourth, pilot Transparent Banks.
Fifth, establish AI audit standards. Sixth, develop computable regulatory interfaces. Seventh, protect privacy and trade secrets, and implement layered disclosure. Eighth, establish legal responsibility mapping. The core of this framework is not to make finance completely decentralized, but to make finance verifiable. It is not to weaken regulation, but to place regulation on a more solid factual foundation. It is not to treat cryptocurrency as a new asset that must be tamed, but to turn the Public Credit Root, machine verification, and transparent constraint capabilities created by cryptocurrency into institutional advantages for the next generation of finance.

Conclusion: The United States Needs Cryptocurrency Regulation, but It Needs to Lead Verifiable Finance Even More

The United States of course needs cryptocurrency regulation. Without regulation, fraud, misappropriation, money laundering, market manipulation, and systemic risk will all damage market trust. But if there is only regulation, the United States can only handle new assets within an old framework; it cannot define new finance.

The meaning of a Verifiable Finance strategy is that it elevates cryptocurrency from a risk object into an institutional tool: using the Public Credit Root to strengthen external proof, using the Chainless system to connect on-chain and off-chain facts, using Transparent Banks to transform centralized finance, using AI auditing to improve continuous supervision, and using legal responsibility to absorb real-world institutional boundaries.

The next generation of financial competition is not only about who has more assets, more exchanges, or a larger stablecoin scale. It is about who can first establish institutional standards under which key financial facts are verifiable. If the United States only regulates cryptocurrency, it is still chasing risks. If the United States leads Verifiable Finance, it can redefine financial transparency, financial regulation, and the foundation of financial credit.

Therefore, the United States needs cryptocurrency regulation, but it needs a Verifiable Finance strategy even more. This is not a narrow policy issue for the cryptocurrency industry. It is a financial infrastructure issue for the AI era and the machine-credit era.

Chapter Seventeen
The Future of the Dollar Requires Greater Transparency

—From the Transparent Dollar to a New Paradigm of Fiat Transparency

Introduction: Dollar Transparency Is Not Merely a Dollar Problem, but a Question of the Dollar System Entering the Era of Verifiable Finance

The dollar has long stood at the center of the global financial order. Over the past several decades, relying on American national strength, capital markets, the legal system, financial institutions, and the global clearing network, the dollar has become the core currency for global trade, reserves, debt, payment, and financial asset pricing. But a new era is arriving. AI is reshaping productive forces and the structure of financial security. Cryptocurrency has already created the Public Credit Root. Stablecoins are bringing the dollar into the on-chain world. Verifiable Finance is moving financial trust from institutional promises toward factual proof. Against this background, the deeper question facing the dollar is no longer merely whether it can continue to dominate global settlement, nor merely how cryptocurrency should be regulated, but whether the dollar system can upgrade from power-based credit into transparency-based credit. This is the core argument of this chapter: the future of the dollar requires greater transparency. The Transparent Dollar, as used here, does not mean abolishing the dollar, weakening American financial power, or requiring all dollar transactions to be made public. Its true meaning is to gradually bring the key financial facts of the dollar system--stablecoin reserves, bank liabilities, clearing states, asset custody, risk exposures, and key operational records--into verifiable structures. The meaning of the Transparent Dollar first lies in the dollar itself. The dollar is the fiat system most capable of taking the lead in completing this transformation: it has the deepest capital markets, the strongest financial technology capability, the broadest global usage scenarios, and the most realistic stablecoin entry point. If the dollar completes a transparency upgrade first, it will not only protect the dollar's status, but also define the fiat transparency standard for the era of Verifiable Finance. Therefore, the Transparent Dollar is not a retreat of dollar hegemony, but an evolution of dollar credit. It is not a weakening of American financial power, but a rebuilding of American financial credibility. It is not the end of the old order, but the starting point for fiat systems entering the era of Verifiable Finance.

I. Dollar Hegemony Faces Structural Pressure

Dollar hegemony did not arise from nothing. It comes from the combined structure of American national strength, deep capital markets, a mature legal system, powerful financial institutions, and a global clearing network. This system has been extremely successful over the past several decades and has also provided the basic order for global finance. But this system is facing new structural pressures. U.S. debt and fiscal pressure continue to rise, and markets keep asking where the boundaries of dollar credit lie. Monetary expansion weakens long-term purchasing power. Geopolitics pushes discussions of de-dollarization. Stablecoins change the way the dollar spreads, but also expose insufficient transparency of off-chain reserves. AI reconstructs the logic of financial security, making old audit and compliance models increasingly inadequate. The Public Credit Root proves that financial trust no longer needs to depend entirely on a single institution. These pressures do not mean that the dollar must decline. The dollar system remains large, deep, complex, and strongly institutionally inertial. The real question is this: the dollar must evolve. In the past, the dollar's advantages mainly came from power, markets, and networks. In the future, the dollar's advantages must also come from transparency, verification, and trusted infrastructure. If the dollar continues to rely only on traditional power structures, it will remain strong, but it will face accumulating trust erosion. If the dollar enters verifiable structures first, it can transform its existing advantages into next-generation institutional advantages.

II. Stablecoins Bring the Dollar On-Chain, but Have Not Yet Brought It Out of the Black Box

Stablecoins are an important form by which the dollar enters the digital world. They expand the dollar's use, making the dollar an important unit of account, medium of exchange, cross-border payment tool, and on-chain dollar carrier in the cryptocurrency market. This is of course a major opportunity for the United States. Stablecoins strengthen the dollar's pricing position in the digital asset market, may increase demand for short-term dollar assets and U.S. Treasuries, and bring the dollar into new financial scenarios outside the traditional banking system. But stablecoins also expose the black-box problem of traditional finance: on-chain tokens are transparent, but off-chain reserves may not be transparent; on-chain issuance is visible, but off-chain liabilities may not be clear; on-chain transfers are rapid, but off-chain redemption capacity may not be verifiable in real time. Users can see address balances, but find it difficult to verify reserve structure, custody relationships, maturity mismatch, undisclosed obligations, and redemption capacity under extreme stress. Therefore, stablecoins only bring the dollar on-chain; they have not truly brought the dollar out of the black box. The first half of stablecoins is dollar tokenization. The second half of stablecoins is stablecoin verifiability. The first step toward the Transparent Dollar is not issuing more stablecoins, but establishing verifiable stablecoin standards.

III. What Is the Transparent Dollar?

The Transparent Dollar is not a new currency name, nor a single product. It is an upgrade direction for the dollar system. Its core meaning is this: key financial facts within the dollar system should gradually become verifiable. First, reserve transparency. Stablecoins, banks, payment institutions, custodians, and other dollar financial intermediaries should be able, under authorized conditions, to provide verifiable evidence for the existence, ownership, and state of key reserves. Second, liability transparency. Financial institutions should not only prove that they have assets, but should also prove liability boundaries, redemption obligations, customer rights, and potential risks. Third, clearing transparency. Payment, redemption, delivery, settlement, and custody states should have traceable and verifiable evidence. Fourth, permission transparency. Key operations, fund transfers, system upgrades, custody signatures, and internal authorizations should have tamper-resistant logs and responsibility mapping. Fifth, risk transparency. Maturity mismatch, concentration risk, liquidity risk, leverage risk, and related-party risk should be subject to continuous monitoring and AI auditing. Sixth, historical transparency. Key state summaries should be anchored to the Public Credit Root to form a tamper-resistant time series and prevent after-the-fact tampering, deletion, and rewriting. The principle of the Transparent Dollar is not full public disclosure, but facts must be verifiable while disclosure can be layered. Customer privacy can be protected, trade secrets can be protected, regulatory access can be authorized in layers, but key financial facts must be provable.

IV. The Transparent Dollar Is a Credit Upgrade, Not a Retreat of Power

Some may worry that the Transparent Dollar will weaken the dollar. This worry comes from the old logic of power. That old logic holds that the stronger financial power is, the less it should be subject to external constraints; the more advantage the dollar has, the less it needs transparency. But the era of AI and cryptocurrency is changing this logic. Future global trust will not come only from power itself; it will increasingly come from verifiability. If the dollar system can take the lead in making key facts verifiable, its global credit will instead be strengthened. Verifiable reserves will increase the credibility of dollar stablecoins. Verifiable liabilities will increase market trust in financial institutions. Verifiable clearing will reduce cross-border payment and settlement risks. Verifiable custody will improve the safety of customer assets. Verifiable risks will help regulators discover systemic problems earlier. Verifiable history will reduce after-the-fact fraud and disputes. The Transparent Dollar does not hand the dollar over to the Bitcoin system, nor does it make the dollar subject to public chains, nor does it require the United States to give up financial sovereignty. The Transparent Dollar uses the Public Credit Root, AI auditing, and legal responsibility to strengthen the credibility of the dollar system. In the past, the dollar earned trust through American strength. In the future, the dollar can continue to earn trust through transparent structures. This does not weaken the dollar; it upgrades dollar credit.

V. The Universal Meaning of the Transparent Dollar: Providing a Starting Point for Fiat Transparency

The true meaning of the Transparent Dollar does not lie only in the dollar itself. It reveals a more universal proposition: if fiat systems want to continue earning trust in the era of AI and Verifiable Finance, they must also gradually increase the verifiability of key financial facts. Fiat currency is not naturally trustworthy. Fiat credit depends on the state, central banks, fiscal systems, banks, law, and payment and clearing systems. The advantages of traditional fiat systems are strong organizational capacity, high execution efficiency, and clear legal responsibility. Their weakness is that key facts often remain inside institutions, while external participants can only rely on reports, audits, and after-the-fact regulation. Therefore, fiat systems should not reject Verifiable Finance. On the contrary, fiat systems need Verifiable Finance the most. The institutional conditions and implementation paths of different countries and different currencies may differ, but the direction should be consistent: key financial facts should become more verifiable. The dollar is important because it is the currency most capable of defining this standard first. Whoever first completes fiat transparency may gain a new institutional advantage in the era of AI and Verifiable Finance.

VI. From Dollar Hegemony to the Transparent Dollar: Redefining Financial Advantage

Dollar hegemony belongs to the financial advantage of the old era. It answers the question: who has the largest market, the deepest liquidity, the strongest clearing network, the strongest financial institutions, the strongest national capacity, and the strongest rule-making power? The Transparent Dollar belongs to the financial advantage of the new era. It answers the question: who can make reserves more verifiable, liabilities clearer, clearing more transparent, risks exposed earlier, AI auditing enter regulation, the Public Credit Root become a financial proof layer, and key facts verifiable while protecting privacy? Past competition was competition in monetary strength. Future competition will increasingly be competition in financial transparency standards. If the United States only maintains dollar hegemony without establishing the Transparent Dollar, it will remain strong but gradually face trust erosion. If the United States establishes the Transparent Dollar first, it can transform existing dollar advantages into next-generation institutional advantages. Dollar hegemony makes the world use dollars. The Transparent Dollar makes the world continue to trust dollars.

VII. The Transparent Dollar Requires Transparent Banks and Regulatory Upgrades

Stablecoins are only the entry point. Banks are the core of the dollar system. A Transparent Bank does not put the entire bank on-chain, disclose all customer data, or eliminate banks. Its core is this: banks continue to provide centralized services, but key financial facts must be verifiable. Banks can preserve customer privacy, preserve trade secrets, and continue risk control, compliance, payment, lending, and asset management. But they must gradually prove key facts: whether reserves are real, whether liabilities are clear, whether clearing has been completed, whether customer assets have been misappropriated, whether key permissions have been abused, whether risks have been hidden, and whether audit logs have been tampered with.

Without Transparent Banks, the Transparent Dollar can only remain at the stablecoin level. With Transparent Banks, the core financial institutions of the dollar system truly enter verifiable structures. Regulation must also be upgraded accordingly. Traditional regulation mainly relies on reports, audits, and enforcement. The Transparent Dollar requires regulation to enter a mode of continuous verification. Regulators should not only ask whether an institution has a license, whether reports have been submitted, and whether auditors have signed off. They should also ask whether reserves, liabilities, clearing, risks, and key histories are verifiable. This is not a loosening of regulation. It makes regulation closer to facts.

VIII. The Transparent Dollar Requires AI, Public Credit Roots, and Legal Responsibility

Implementing the Transparent Dollar is not simple. It requires complex engineering systems, continuous auditing capability, layered disclosure mechanisms, Public Credit Root anchoring, and legal responsibility mapping. In the past, such systems were difficult to implement, with engineering complexity as an important reason. The emergence of AI makes this complex structure realistically feasible for the first time. AI can continuously monitor on-chain issuance and circulation, analyze reserve asset structures and liquidity risks, compare on-chain liabilities with off-chain reserves, detect abnormal fund flows, simulate concentrated redemptions and market stress, identify permission abuse and internal risks, and turn complex data into regulatory alerts. But AI cannot independently become a credit root. AI can be attacked, manipulated, or trained incorrectly, and it can also make wrong judgments. Therefore, the Transparent Dollar must combine AI auditing, the Public Credit Root, and legal responsibility. AI provides continuous analysis. The Public Credit Root provides tamper-resistant evidence. Law and regulation provide responsibility boundaries. Only their combination forms the security structure of the Transparent Dollar.

IX. If the United States Does Not Define Standards, the Market Will Form Fragmented Rules

Financial standards never remain blank for long. If the United States does not define standards for the Transparent Dollar and Verifiable Finance, the market will spontaneously form various fragmented standards. If the United States does not define verifiable stablecoin standards, different issuers will each define their own. If the United States does not define AI audit standards, large platforms and private institutions will each define their own. If the United States does not define Public Credit Root anchoring rules, the market will form incompatible technical paths. If the United States does not define the Transparent Bank framework, banks, exchanges, custodians, and payment companies may each build closed systems. If the United States does not define principles of layered disclosure, the balance between transparency and privacy will be formed passively without unified standards. Future competition is not only monetary competition, technological competition, and capital competition. It will also be competition over financial transparency standards. The United States cannot be absent. Dollar hegemony belongs to the advantages of the past several decades. The Transparent Dollar belongs to the standards competition of the next several decades. If the United States continues to define rules, it must define the Transparent Dollar.

Conclusion: The Transparent Dollar Is the Starting Point of Fiat Transparency Dollar hegemony once supported the modern global financial order. But the future advantage of the dollar cannot rely only on the hegemonic structure of the past. It must adapt to the new realities of AI, cryptocurrency, Public Credit Roots, stablecoins, and Verifiable Finance. The Transparent Dollar does not abolish the dollar, oppose dollar hegemony, put the dollar fully on-chain, or expose financial data nakedly to the

to the public. The Transparent Dollar is an upgrade of dollar credit. It makes reserves no longer merely statements, but proofs; liabilities no longer merely reports, but verifiable states; clearing no longer merely internal processes, but verifiable results; regulation no longer merely after-the-fact inspection, but continuous verification; and the dollar no longer merely a currency of power, but a core standard of Verifiable Finance in the AI era.

More broadly, the Transparent Dollar should become the starting point of fiat transparency. Future major fiat systems should, while protecting privacy and trade secrets, make key financial facts more verifiable.

Dollar hegemony makes the world use dollars. The Transparent Dollar makes the world continue to trust dollars.

From dollar hegemony to the Transparent Dollar is not a retreat of the dollar, but an evolution of the dollar. It is not a weakening of American financial power, but the rebuilding of American financial credit. It is not the end of the old order, but the beginning of a new order of fiat transparency.

From double-entry accounting to Verifiable Finance, the structure of financial constraint is undergoing a deep transformation: double-entry accounting established the internal constraints of modern finance, the Public Credit Root provides an externally verifiable anchor, the Transparent Bank brings centralized finance into a verifiable structure, and the Transparent Dollar may allow the fiat system to enter the era of Verifiable Finance. In this sense, a financial revolution is approaching its point of eruption, and the place most likely to complete the institutional breakthrough first remains the United States.

Appendix - Glossary

Verifiable Finance: a theoretical system that studies how key facts, key states, key rights, key responsibilities, and key accounting results in financial relationships can, through institutional rules, accounting records, cryptographic proofs, responsibility records, layered disclosure, and regulatory-audit acceptance, form structures that are verifiable, traceable, replayable, and institutionally absorbable.

Public Credit Root: a foundational credit structure that is open, long-running, difficult to tamper with, globally verifiable in real time, and able to serve as the final anchoring point for other financial systems. The Bitcoin system is the most typical Public Credit Root.
Bitcoin Asset and Bitcoin System: the Bitcoin asset refers to BTC as a non-sovereign digital asset. The Bitcoin system refers to the overall institutional structure that includes the network, nodes, miners, rules, ledger, incentives, and social consensus.

Machine Credit: not blind trust in machines, but credit built on verifiable structures through cryptography, public rules, competitive mechanisms, economic incentives, and historical sedimentation.

Transparent Bank: a new type of financial institution in which centralized services still exist, but key financial facts must be verifiable. It does not eliminate banks; it makes it impossible for banks to lie.

Transparent Finance: a new financial paradigm represented by Transparent Banks and based on the Public Credit Root and verifiable proofs. It emphasizes the verifiability of key facts, not the public disclosure of all data.

Lowest Ledgering Cost: separating the cost of daily ledgering from the cost of final credit proof. Institutions can keep accounts internally at low cost, but key ledger states need to be anchored to a Public Credit Root. Verification Above Open Source: open source is one means of achieving verification, but it is not the final objective. What financial systems truly need to prove are reserves, liabilities, clearing, permissions, risks, and historical states.

Verifiable Stablecoin: a stablecoin whose reserves, liabilities, redeemability, and key risk states can be independently, continuously, and tamper-resistently verified. Transparent Dollar: the upgrade direction in which key financial facts of the dollar system gradually become verifiable. Its significance lies not only in the dollar, but in opening a new paradigm of fiat transparency.
Layered Disclosure: facts must be verifiable, but the subjects and depth of disclosure can be layered in order to balance transparency, privacy, trade secrets, and regulatory penetration.

AI Continuous Auditing: using AI to continuously monitor and analyze code, ledgers, transactions, reserves, liabilities, permissions, risks, and abnormal states. Transparent Coordination Institution: a non-coercive, public, challengeable coordination layer that may be needed in Bitcoin's second half and that serves the economic majority. It provides strong signals and does not replace UASF.
UASF: User Activated Soft Fork. It expresses the final choice and veto power of economic nodes over protocol rules under extreme conditions.

CAPITOL TIMES
MEDIA • MAGAZINE

ADVERTISING THAT BUILDS

BRANDS. DRIVES GROWTH.

At Capitol Times Magazine we turn bold ideas into powerful campaigns that connect, convert, and create lasting impact.

STRATEGIC. IMPACTFUL. RESULTS-DRIVEN.

We are your strategic ally—arming you with bold strategy, digital power, and the enduring force of print. Together, we conquer challenges, crush weak competition, and build lasting prosperity for our people and economy.

STRATEGIC TARGETING

Reach the right audience with precision, every time.

POWERFUL ADVERTISING

Impactful print and digital solutions that get noticed.

MAXIMUM VISIBILITY

Boost brand awareness and drive measurable results.

LET'S GROW TOGETHER
ads@capitoltimesmedia.com

YOUR MESSAGE.
OUR PLATFORM.
REAL RESULTS.

CAPITOL TIMES MAGAZINE

LEADERS. VISIONARIES. FRIENDS.

A Special

THANKS TO WEISHA ZHU

FOUNDER OF

CHAINLESS.HK

"Anyone who becomes associated with him will be the beneficiary of meeting an *extraordinary* person."

Scott Shields

SCOTT SHIELDS

Stephanie Li

STEPHANIE LI

INTEGRITY. TRUST. PARTNERSHIP. IMPACT.