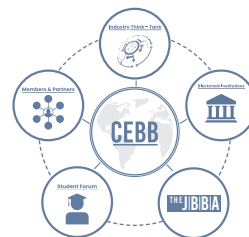
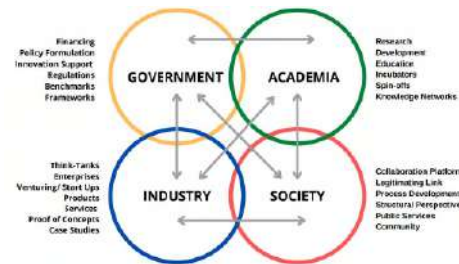




BUILDING THE EVIDENCE BASE FOR BLOCKCHAIN'S FUTURE: *From* INNOVATION *To* IMPACT



UK NATIONAL BLOCKCHAIN ROADMAP (NBR) (VISION 2030)



6TH BLOCKCHAIN ASSOCIATIONS FORUM (BAF) ANNUAL MEMBER SUMMIT | 9 SEPTEMBER 2026
Proceedings of 8th Blockchain International Scientific Conference #ISC2026 London

PUBLISHED BY

CEBB Centre for
Evidence-Based Blockchain®

THE JBBBA



The BBA is the Secretariat of the APPG on Blockchain Technologies



BLOCKCHAIN TECHNOLOGIES

All-Party Parliamentary Group



The British Blockchain Association
Advocating Evidence Based Blockchain



MEMBERS OF BLOCKCHAIN APPG



Matt Vickers MP



Lord McNicol of West Kilbride



Matt Bishop MP



Lord Goddard of Stockport



Alison Taylor MP



Rt Hon Viscount Camrose



Will Forster MP



Baroness Owen of Aderley Edge



The Lord Boateng



Baroness Vere of Norbiton



The Lord Roborough



Baroness Dr Swinburne



Lord Vaizey of Didcot



Mike Tapp MP



The Lord Altrincham



Dr Simon Opher MP



The Lord Naseby



Lord Gilbert of Panteg



Gurinder Josan MP



Dr Ben Spencer MP



The Lord Lucas



The Baroness Uddin



Lord Wei of Shoreditch



The Lord Triesman



Lauren Edwards MP



Lord Taylor of Warwick



Danny Kruger MP



John Lamont MP

To find out more about the APPG, visit www.britishblockchainassociation.org/appg

TABLE OF CONTENTS

Editorial Board	16
Testimonials from Authors & Readers	18
Editorial	21

PEER-REVIEWED RESEARCH

Hybrid Post-Quantum Signatures for Bitcoin and Ethereum: A Protocol-Level Integration Strategy	22
<i>Robert Campbell, Sr. FBBA</i> <i>Independent Researcher, Maryland, USA</i>	
Bitcoin Ordinals and Inscriptions: An Analysis of Bitcoin's Evolving Network Dynamics	32
<i>Alexander Wiedenmann¹, Andre Guettler^{1,2}</i> <i>¹ Ulm University, Institute of Strategic Management and Finance, Germany</i> <i>² Halle Institute for Economic Research (IWH), Germany</i>	
Rate Discovery in Decentralised Lending	42
<i>Charlotte Eli, Hervé Alexandre</i> <i>Université Paris Dauphine-PSL, Dauphine Fintech Chair, France</i>	
F-Procure: A Decentralised, Modular Framework for Transparent, Compliant and Efficient Procurement on the Flare Network	51
<i>Pax Ola</i> <i>Caypax Inc., Cayman Islands</i>	
Spectrum of Adoption of Blockchain Technology: Implications for Emerging Capital Markets in Africa	62
<i>Clinton Osemwengie</i> <i>Centre of FinTech, University of East London, London, United Kingdom</i>	

ESSAY

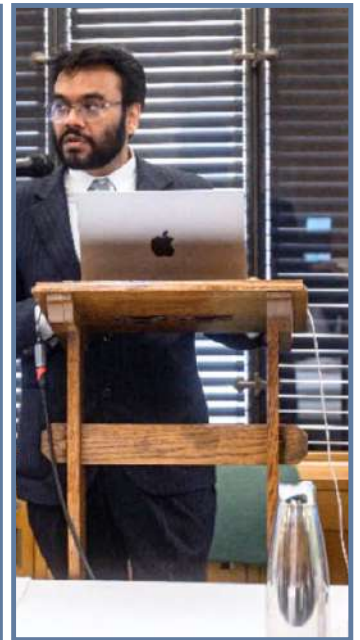
Ancient Philosophers Understand Blockchain Better Than Most of Us	69
<i>Naseem Naqvi MBE</i> <i>Centre for Evidence-Based Blockchain, The British Blockchain Association, UK</i>	

CONFERENCE PROCEEDINGS

Proceedings of 8th Blockchain International Scientific Conference #ISC2026 London 27 March 2026, London	72
--	----

BBA'S 8TH BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE #ISC2026







BLOCKCHAIN
ASSOCIATIONS FORUM

Hosted by the British Blockchain Association

BAF 6th Annual

MEMBER SUMMIT

9 September 2026

#BAF2026



CEBB Centre for
Evidence-Based Blockchain



The British Blockchain Association
Advocating Evidence Based Blockchain



BLOCKCHAIN
ASSOCIATIONS FORUM

6TH ANNUAL BAF MEMBER SUMMIT

#BAF2026

9 SEPTEMBER 2026

For more info, visit <https://britishblockchainassociation.org/baf/>

WHY PUBLISH IN THE JBBA?

- » We publish in real-time, online, as well as in **PRINT - THE HARD COPIES ARE DISTRIBUTED WORLDWIDE**
 - » Print copies are available at some of the largest libraries in the world including **BRITISH LIBRARY** and over **800+** more **AROUND THE GLOBE**
 - » Our authors and readers rate the JBBA as **OUTSTANDING**
 - » We create **INFOGRAPHICS** of published research papers
 - » We are in the **METaverse**
 - » We offer **LANGUAGE EDITING AND TRANSLATION** Services to non-native English speaking authors
 - » We publish **VIDEO ABSTRACTS** of research papers
 - » We are **ON THE BLOCKCHAIN** - Articles Time Stamped on Public Blockchains
 - » We are **PERMANENTLY ARCHIVED** at PORTICO
 - » We are **ON PUBLONS** supporting Authors, Reviewers and Editors
 - » We are **INDEXED IN DOAJ** and **WEB of SCIENCE** (Master Journal List)
 - » We have a **JBBA YOUTUBE CHANNEL**
 - » JBBA papers are quoted by Government Officials, Policymakers, Regulators and High Profile Organisations - **CREATING A GLOBAL IMPACT**
-



THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION®

britishblockchainassociation.org/jbba

Follow us on:





MEMBERS & PARTNERS OF THE BBA ECOSYSTEM



WORKING IN COLLABORATION WITH:



Join Now at britishblockchainassociation.org/membership

britishblockchainassociation.org



SUBSCRIBE TO OUR YOUTUBE CHANNEL



The BBA

@TheJBBA · 360 subscribers · 208 videos

The Official YouTube Channel of The British Blockchain Association (The BBA). >

britishblockchainassociation.org/wp-content/uploads/2021/07/UK-NBR-Excel... and 3 more links



Shaping Tomorrow: The Official #ISC2026 Recap
17 views · 8 days ago



The BBA Podcast: Episode 1: Post-Quantum Blockchains
28K views · 1 month ago



The British Blockchain Association | 2025 Year in Review
17 views · 3 months ago



Blockchain Infrastructure for UK Digital Economy | Parliamentary...
39 views · 4 months ago



U.S. vs China: The Global Blockchain Race Explained | Key...
17 views · 4 months ago



BBA President Dr Naseem on Dubai's Web3 Leadership and the...
4 views · 4 months ago



How Stablecoins Can Transform the Commonwealth's 2.7 Billion Citizens
6 views · 4 months ago



BAF 2025: Jorge García Travesi Represents Mexico at the 5th...
19 views · 5 months ago



BBA FORUM JULY 2025: DECENTRALISED HEALTHCARE ON THE BLOCKCHAIN - Dr...
37 views · 2 months ago



BlockMed Pro Joins BBA: Showcased Across All Official Platforms Including...
7 views · 3 months ago



Why Semantic Interoperability is the Blockchain Elephant in the Room?
8 views · 4 months ago



Why Peer Review Matters: From @royalsociety Journals to Modern...
5 views · 4 months ago



BBA FORUM: Tokenising Real-Estate: Fractional Ownership Using ERC20 NFTs -...
28 views · 6 months ago



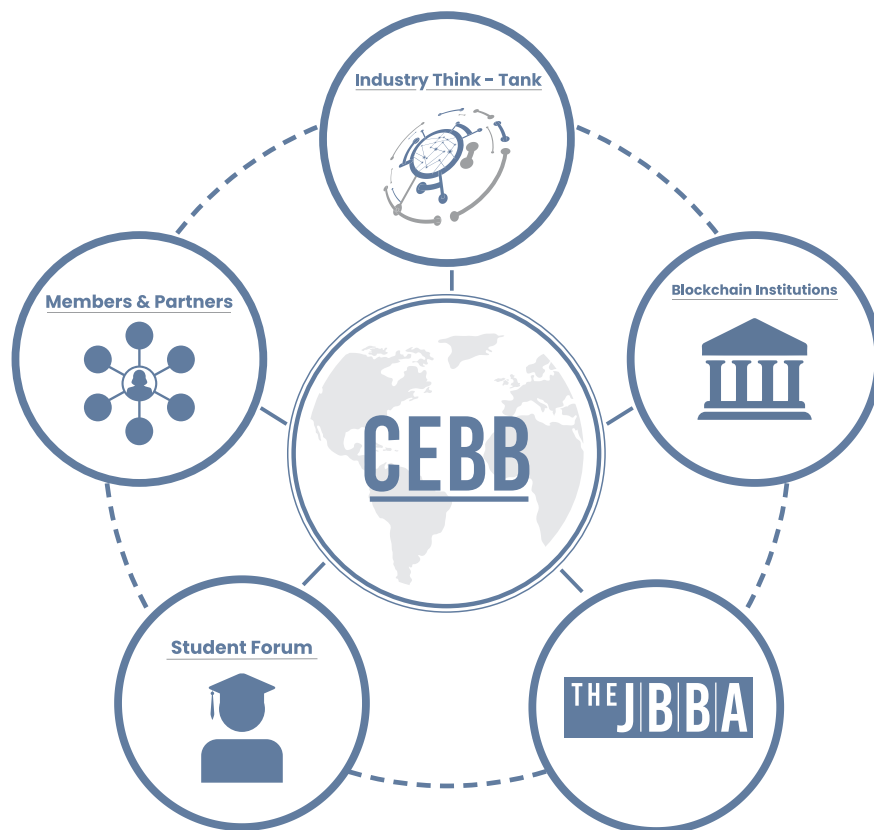
BBA FORUM: Buying & Selling A Property With Crypto: What You Need To Know -...
62 views · 6 months ago



Have You Registered For The BBA's Annual International Conference?
1 view · 6 months ago



Bridging the Blockchain Research and Practice Gap



MEMBERS



JOIN CEBB

To join CEBB, please contact us at admin@britishblockchainassociation.org with your expression of interest, and why you believe you fulfil the legibility as mentioned in the above criteria. Organisations that do not satisfy all of the above eligibility criteria may be considered for an Affiliate Membership, subject to approval from the CEBB Board. To find out more, visit www.britishblockchainassociation.org/cebb



The British Blockchain Association®

Advocating Evidence Based Blockchain

BBA ORGANISED BLOCKCHAIN MASTERCLASS FOR MPS AND LORDS

Why A.I. Needs Blockchain?

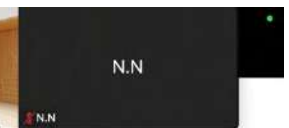
YouTube · The BBA · 12 Jan 2025

✓ Hash published on a Blockchain

Video Permalink:
<https://tinyurl.com/sk9jhwut>

Blockchain Transaction Hash:
0x8143d64db3856d7b8d5e75e0df7e794b3179e9dbb505209a1dba04d46eac0d89

✓ Blockchain Time Stamp: January-12-2025 01:10:05 AM -0 UTC



Blockchain Masterclass for Policymakers



The British Blockchain Association

Advocating Evidence Based Blockchain

SESSION 1:

Blockchain Basics

April 2026

BBA METAVERSE HEADQUARTERS

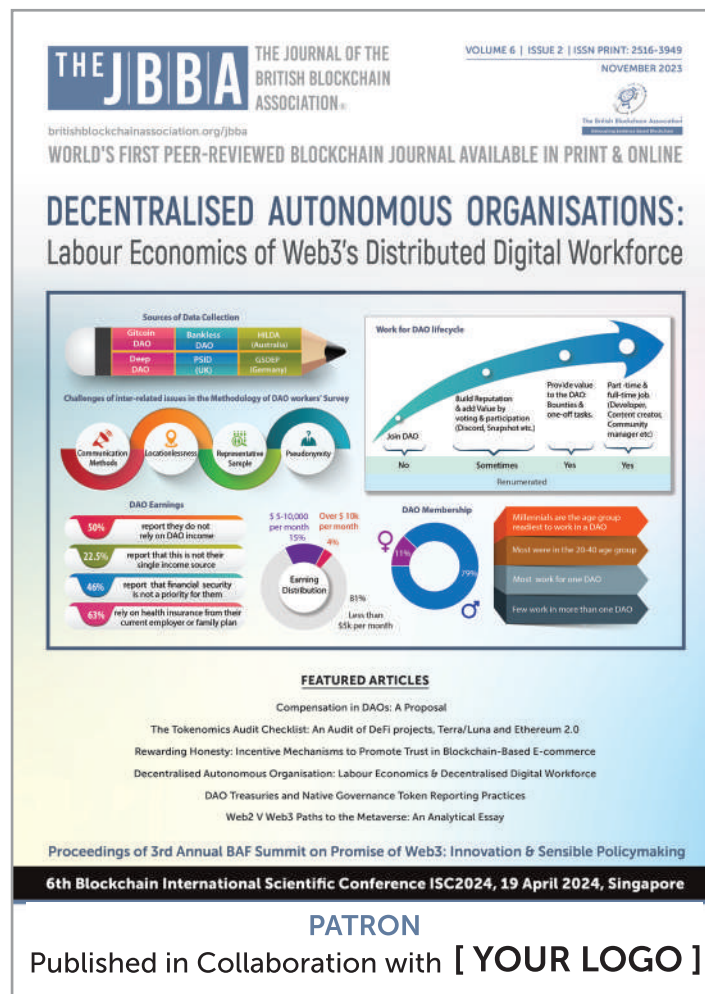


For more info, visit <https://britishblockchainassociation.org>

BECOME A PATRON OF THE JBBA

Your logo will appear on the COVER PAGE of the JBBA.

The journal is distributed worldwide to major Universities, Banks, Fintech Institutions, Blockchain Research Centres, Policy Makers, Influencers, Industry Leaders and Journal's Editors, Reviewers and Authors



Partnering with the JBBA connects you to hundreds of thousands of readers in over 150 Countries and territories across the globe

To become an Academic Partner or to Advertise in the Journal, contact us at:

www.britishblockchainassociation.org | info@britishblockchainassociation.org

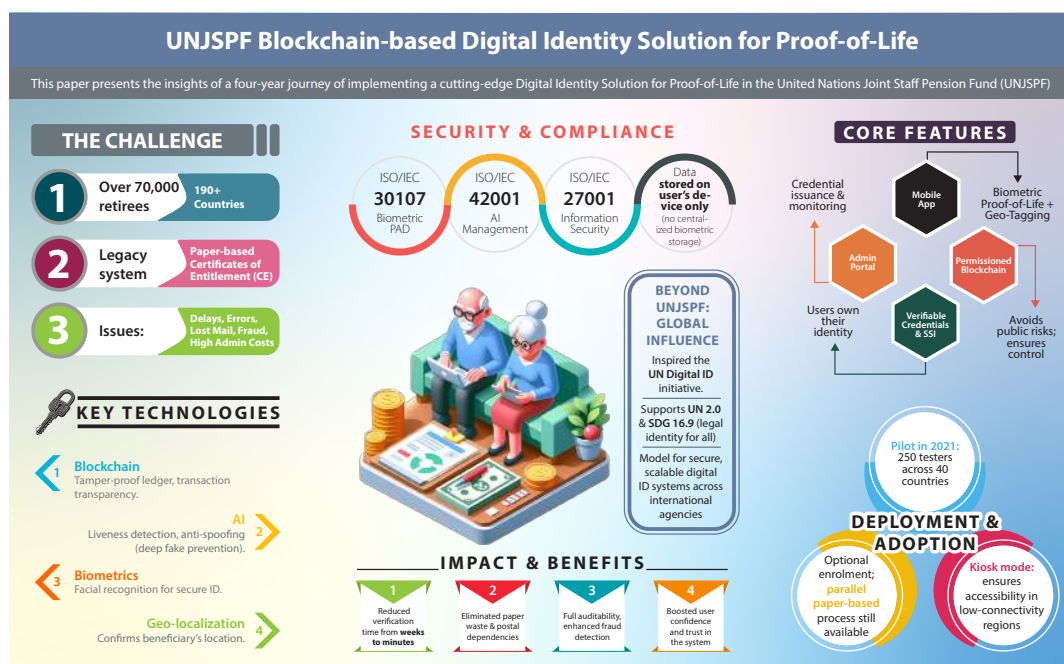
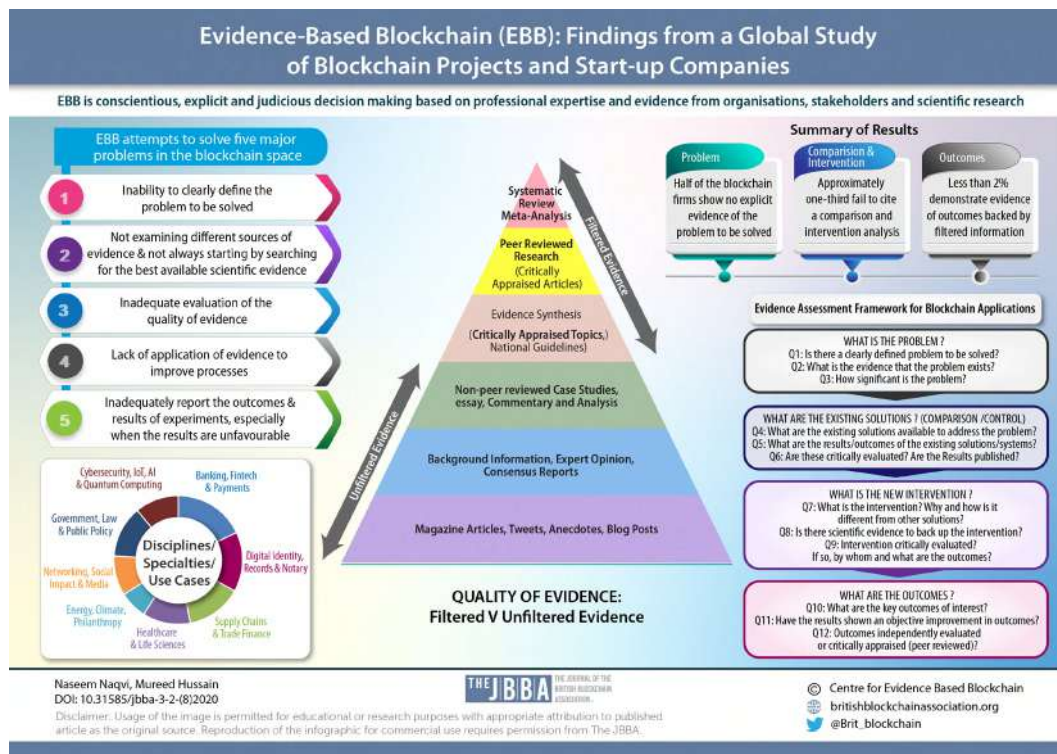
Follow us on:



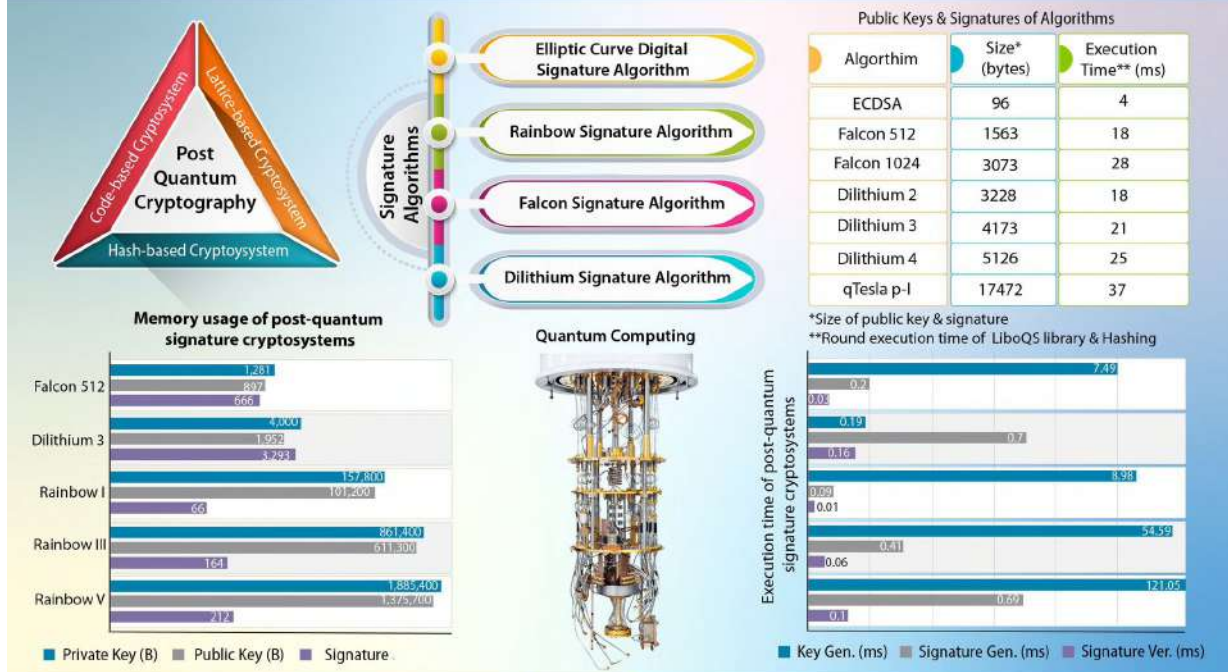
JBBA INFOGRAPHICS

PRODUCED BY

CENTRE FOR EVIDENCE BASED BLOCKCHAIN (CEBB)



A Performance Comparison of Post-Quantum Algorithms in Blockchain



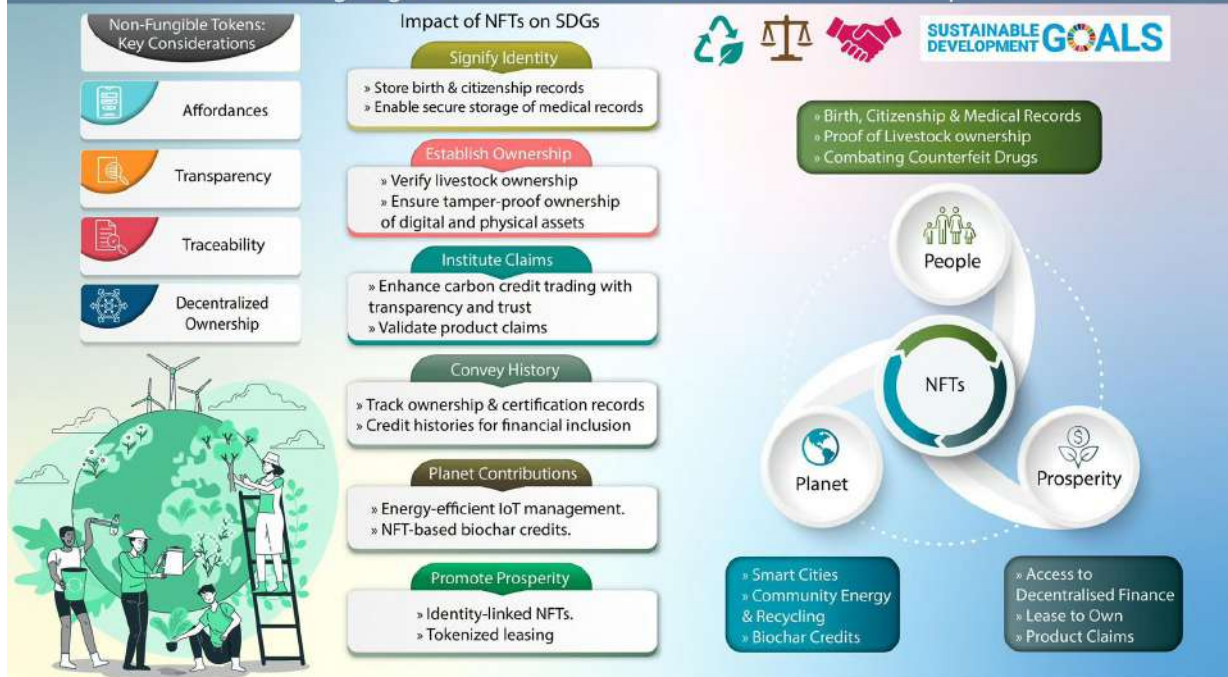
Lu Gan and Bakhtiyor Yokubov (2022)
DOI: 10.31585/jbba-6-1-(1)2023

Disclaimer: Usage of the image is permitted for educational or research purposes with appropriate attribution to published article as the original source. Reproduction of the infographic for commercial use requires permission from The JBBA.

THE JBBA
THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

NFTs at the Nexus of Innovation and Sustainability: A Framework Aligning NFT Affordances with the Sustainable Development Goals



Kristi Yuthas
DOI: 110.31585/jbba-7-2-(6)2024

Disclaimer: Usage of the image is permitted for educational or research purposes with appropriate attribution to published article as the original source. Reproduction of the infographic for commercial use requires permission from The JBBA.

THE JBBA
THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

EDITORIAL BOARD

Editor-In-Chief:

Professor Dr Naseem Naqvi FBBA MBE
Centre for Evidence Based Blockchain, UK

Associate Editor-In-Chief:

Dr Marcella Atzori PhD FBBA
(GovTech/ Smart Cities)
European Commission, Italy

Professor Dr Marc Pilkington PhD FBBA
(Cryptocurrencies/ Digital Tech)
University of Burgundy, France

Professor Dr David Lee K Chuen PhD FBBA
(Applied Blockchain)
Singapore University of Social Sciences, Singapore

Dr Mureed Hussain FBBA MD MSc
(Blockchain Governance)
The British Blockchain Association, UK

Contributing Editors:

Professor Dr Bill Buchanan PhD FBBA
(Cryptography/ Cybersecurity)
Edinburgh Napier University, UK

Professor Dr Kevin Curran PhD FBBA
(Cybersecurity)
Ulster University, UK

Professor Dr John Domingue PhD FBBA
(Artificial Intelligence/ Education)
The Open University, UK

Professor Dr Sinclair Davidson PhD FBBA
(Institutional Cryptoeconomics)
RMIT University, Australia

Professor Dr Hanna Halaburda PhD
(Blockchain & Information Systems)
New York University, USA

Professor Dr Sandeep Shukla PhD
(Blockchain & Cybersecurity)
Indian institute of Technology, India

Professor Dr Jason Potts PhD FBBA
(Applied Blockchain)
RMIT University, Australia

Professor Dr Mary Lacity PhD FBBA
(Blockchain/ Information Systems)
University of Arkansas, USA

Professor Dr Anne Mention PhD
(Blockchain & Economics)
RMIT University, USA

Professor Dr Sushmita Ruj PhD
(Applied Cryptography, Security)
Indian Statistical Institute, India

Professor Dr Jim KS Liew PhD FBBA
(Blockchain, Finance, AI)
Johns Hopkins University, USA

Professor Dr Wulf Kaal PhD
(Blockchain & Law)
University of St. Thomas, USA

Professor Dr Eric Vermeulen PhD FBBA
(Financial Law, Business, Economics)
Tilburg University, The Netherlands

Professor Dr Jeff Daniels PhD
(Cybersecurity, Cloud Computing)
University of Maryland, USA

Professor Dr Mark Lennon PhD
(Cryptocurrencies, Finance, Business)
California University of Pennsylvania, USA

Professor Dr Chris Sier PhD
(DLT in Finance / Capital Markets)
University of Newcastle, UK

Professor Dr Walter Blocher PhD
(Blockchain, Law, Smart Contracts)
University of Kassel, Germany

Professor Dr Clare Sullivan PhD
(Cybersecurity / Digital Identity)
Georgetown University, USA

Professor Dr Andrew Mangle PhD
(Cryptocurrency, Smart contracts)
Bowie State University, USA

Professor Dr Isabelle C Wattiau PhD
(Information Systems, Smart Data)
ESSEC Business School, France

Professor Dr Lee McKnight PhD
(IoT & Blockchain)
Syracuse University, USA

Professor Dr Chen Liu PhD
(Fintech, Tokenomics)
Trinity Western University, Canada

Professor Dr Markus Bick PhD
(Business Information Systems)
ESCP Business School, Germany

Professor Dr Sandip Chakraborty PhD
(Blockchain, Distributed Networks)
Indian Institute of Technology, India

Professor Adam Hayes MA BS CFA
(Blockchain & Political Sociology)
University of Wisconsin-Madison, USA

Dr Stylianos Kampakis PhD
(ICOs, Big Data, Token Economics)
University College London, UK

Dr Christian Jaag PhD
(Crypto-economics, Law)
University of Zurich, Switzerland

Dr Larissa Lee JD
(Blockchain & Law)
University of Utah, USA

Dr Sean Manion PhD FBBA
(Blockchain in Health Sciences)
Uniformed Services University, USA

External Reviewers:

Professor Dr Mark Fenwick PhD
(Smart Contracts & Law)
Kyushu University, Japan

Professor Dr Wulf Kaal PhD
(Blockchain & Law)
University of St. Thomas, USA

Professor Dr Balazs Bodo PhD
(Blockchain & Information Law)
University of Amsterdam

Professor Dr Ping Wang PhD
(Blockchain & Information Systems)
Robert Morris University, USA

Professor Dr Jeff Schwartz JD
(Corporate Law)
University of Utah, USA

Professor Dr Shada Alsalamah PhD
(Healthcare Informatics & Blockchain)
Massachusetts Institute of Technology, USA

Dr Stefan Meyer PhD
(Blockchain in Food Supply Chain)
University of Leeds, UK

Dr Maria Letizia Perugini PhD
(Digital Forensics & Smart Contracts)
University of Bologna, Italy

Dr Phil Godsiff PhD
(Cryptocurrencies)
University of Surrey, UK

Dr Duane Wilson PhD
(Cybersecurity/ Computer Science)
The Johns Hopkins University, USA

Dr Darcy Allen PhD
(Economics/Innovation)
RMIT University, Australia

Dr Jeremy Kronick PhD
(Blockchain & Finance/ Economics)
C.D Howe Institute, Canada

Professor Dr Ifigenia Georgiou PhD
(Crypto-economics)
University of Nicosia, Cyprus

Dr Anish Mohammed MSc
(Crypto-economics, Security)
Institute of Information Systems, Germany

Professor Dr Benjamin M. Cole PhD FBBA
(Strategy, Statistics, Technology)
Fordham University, USA

Dr Chris Berg PhD
(Blockchain Economics)
RMIT University, Australia

Prof Dr Patrick Schuffel PhD
(Blockchain & Finance)
Fribourg School of Management, Switzerland

Raf Ganseman
(DLT in Trade & Music Industry)
KU Leuven University, Belgium

Sebastian Cochinescu MSc
(Blockchain in Culture Industry)
University of Bucharest, Romania

Jared Polites MSc
(ICOs & Cryptocurrencies)
Blockteam Ventures, USA

Professor Rob Campbell FBBA
(Quantum Computing, Cybersecurity)
Capitol Technology University, USA

Simon Dyson MSc
(Healthcare Section, The JBBA)

Professor Dr Apostolos Kourtis PhD
(Blockchain & Finance)
University of East Anglia, UK
Professor Dr David Galindo PhD

(Applied Cryptography & Blockchain)
University of Birmingham, UK

Professor Dr Aleksei Gudkov PhD
(Blockchain, Ethics & Law)
National Research University, Russia

Dr Rafal T Prabucki PhD
(Smart Legal Contracts)
University of Silesia in Katowice, Poland

Professor Dr Tim Weingärtner PhD
(IoT & Blockchain, Information Systems)
Lucerne University of Applied
Sciences, Switzerland

Dr Swathi Kaluvakuri PhD
(Blockchain, Cybersecurity, Computer Science)
Southern Illinois University, USA

Dr Riem AbdelAzim PhD
(Blockchain, Information Systems)
Marywood University, Pennsylvania, USA

Managing Editor:

Keerthika Purushothaman
(Academic publishing)
Deanta Global, Dublin, Ireland
[Editorial@thejbba.com]

Publishing Consultant:

Mr John Bond
Riverwinds Consulting, USA

Sponsorships and Academic Partnerships:

Deborah Cleary
Head of Partnerships
secretary@britishblockchainassociation.org

Type-setting, Design & Publishing

Mr Zeshan Mahmood
info@britishblockchainassociation.org

TESTIMONIALS FROM AUTHORS AND READERS

“ The JBBA has an outstandingly streamlined submissions process, the reviewers comments have been constructive and valuable, and it is outstandingly well produced, presented and promulgated. It is in my opinion the leading journal for blockchain research and I expect it to maintain that distinction under the direction of its forward-looking leadership team.

Dr Brendan Markey-Towler PhD, University of Queensland, Australia

”

“ "I always enjoy reading the JBBA."

Professor Dr Emin Gun Sirer PhD, Cornell University, USA

”

“ It is really important for a future world to be built around peer-review and publishing in the JBBA is one good way of getting your view-points out there and to be shared by experts.

Professor Dr Bill Buchanan OBE PhD, Edinburgh Napier University, Scotland

”

“ The JBBA has my appreciation and respect for having a technical understanding and the fortitude for publishing an article addressing a controversial and poorly understood topic. I say without hesitation that JBBA has no equal in the world of scientific Peer-Review Blockchain Research.

Professor Rob Campbell, Capitol Technology University, USA

”

“ I had a professional experience of publishing my work in The JBBA. The feedback from reviewers and editors certainly helped to turn my manuscript into a better publication. JBBA's cross-disciplinary publishing platform is crucial to enable the blockchain sector to flourish. The journal strongly advocates evidence-based outcomes, essential to differentiate sound research papers from those that are not.

Dr Joshua Ellul PhD, Chair, Malta Digital Innovation Authority

”

“ The opportunity to interact with JBBA's expert reviewers and their valuable feedback helped us greatly in our project. I feel honoured to have my paper featured in the JBBA. Peer reviewed research is the foundation to build best-in-class Web3 platforms.

Daniel Uribe MBA, Cofounder and CEO Genobank.io, USA

”

“ This is a very professionally presented journal.

Peter Robinson, Blockchain Researcher & Applied Cryptographer, PegaSys, ConsenSys

”

“ I would like to think of the JBBA as an engine of knowledge and innovation, supporting blockchain industry, innovation and stimulate debate.

Dr Marcella Atzori PhD, EU Parliament & EU Commission Blockchain Expert, Italy

”

“ We published a multi-centre blockchain research in The JBBA, led by authors from China and Singapore. The journal's editorial board is quite diverse in academic and industry expertise. The multi-disciplinary feedback was valuable and a rigorous review process enhanced our research output, outreach and impact. ”

Professor Dr David Lee Kuo Chuen PhD, Professor of Finance and Blockchain, Singapore University of Social Sciences, Singapore

“ Our group submitted a paper to ISC2021. The paper was reviewed, accepted and subsequently published in The JBBA. We were quite impressed by the speed of the review cycle and submission to publication time. JBBA has become an important journal in the field of Blockchain, given its efficient reviews and timeliness in the publication of research articles. ”

Professor Dr Sandeep Shukla, Indian Institute of Technology IIT Kanpur, India

“ I had the honour of being an author in the JBBA. It is one of the best efforts promoting serious blockchain research, worldwide. If you are a researcher, you should definitely consider submitting your blockchain research to the JBBA. ”

Dr Stylianos Kampakis PhD, UCL Centre for Blockchain Technologies, UK

“ It has been a pleasure working with the JBBA's editorial team. The submission process was transparent and the reviews were accurate and meaningful, adding great value to the manuscript. ”

Professor Dr Stavros T. Ponis PhD, National Technical University of Athens, Greece

“ The articles in the JBBA explain how blockchain has the potential to help solve economic, social, cultural and humanitarian issues. If you want to be prepared for the digital age, you need to read the JBBA. Its articles allowed me to identify problems, find solutions and come up with opportunities regarding blockchain and smart contracts. ”

Professor Dr Eric Vermeulen, Tilburg University, The Netherlands

“ The whole experience from submission, to conference, to revision, to copy-editing, to being published was extremely professional. The JBBA are setting a very high standard in the space. I am looking forward to working with them again in future ”

Dr Robin Renwick PhD, University college Cork, Ireland

“ The JBBA is an exciting peer-reviewed journal of a growing, global, scientific community around Blockchain and Distributed Ledger technologies. As an author, publishing in the JBBA was an honour and I hope to continue contributing to in in the future ”

Evandro Pioli Moro, Blockchain Researcher, British Telecommunication (BT) Applied Research

“ Publishing with The JBBA was a fantastic experience. The journal provided timely and constructive feedback on my research and offered me an opportunity to present at the ISC2024, where my research was well received. An important highlight was the conversion of my work into a beautifully designed infographic that captured the essence of my research. The ongoing post-publication support from the BBA has been incredible.. ”

Dr Beatab Sibanda PhD, North West University, S Africa

THANK YOU REVIEWERS

The Editorial Board of The JBBA gratefully acknowledges and thanks the reviewers for their time and expertise. The following is the list of reviewers who contributed to the peer review process for the current (17th) Issue of The JBBA (May 2026).

Professor Dr Naseem Naqvi MBE FBBA	UK
Professor Dr Kevin Curran FBBA	UK
Professor Dr Mary Lacity FBBA	USA
Professor Dr Riem AbdelAzim	USA
Professor Dr Apostolos Kourtis	UK
Professor Marc Pilkington FBBA	FRANCE
Dr Sebastian Cochinescu	ROMANIA
Professor Dr Andrew Mangle	USA
Dr Stylianos Kampakis	UK
Simon Dyson MSc	UK
Sun Hongyan	SWITZERLAND
Dr Mureed Hussain MD FBBA	UK

EDITORIAL

I am delighted to present the 17th issue of the Journal of the British Blockchain Association. This issue features the conference proceedings of the 8th Blockchain International Scientific Conference (ISC2026). This was the first time in British history that a scientific conference was held inside the Houses of Parliament.

This publication rests on a clear conviction: blockchain technology is too consequential to be shaped by advocacy alone, and too complex to be governed by unexamined assumptions.

The cover theme — Building World-Class Blockchain Ecosystems — appears frequently in white papers, government announcements, and industry communiqués. Yet the phrase has become something of a ritual: widely invoked, seldom scrutinised. This issue moves beyond rhetoric to ask a more demanding question: what does a genuinely world-class blockchain ecosystem structurally, intellectually, and empirically require?

The six papers gathered here span post-quantum cryptography, network dynamics, decentralised finance, procurement infrastructure, ancient philosophy, and emerging-market adoption. They differ in methodology and geography, yet share a common commitment: each examines a foundational condition for building durable, scalable, and trustworthy blockchain ecosystems.

Robert Campbell Sr. opens the issue by confronting a question the field has been reluctant to address directly: whether the cryptographic foundations of Bitcoin and Ethereum remain adequate in the quantum era. His technically precise analysis of hybrid post-quantum signatures carries profound civilisational implications.

Wiedenmann and Guettler bring analytical rigour to the Ordinals debate, treating Bitcoin as a living economic protocol rather than a fixed ideological artefact. Wiedenmann's paper also received the Best Abstract Award at the ISC2026.

Charlotte Eli and Hervé Alexandre tackle one of DeFi's most persistent structural weaknesses — the lack of genuine interest-rate discovery — demonstrating that replicating the form of traditional financial instruments without their underlying epistemic infrastructure produces systems that behave differently, and often poorly, under stress.

Pax Ola's paper on F-Procure illustrates what institutional-grade blockchain deployment looks like when regulatory compliance is integrated as a core design principle rather than an afterthought.

The fifth paper, which bears my name, argues that many conceptual challenges blockchain seeks to solve have deep roots in millennia of philosophical inquiry — an intellectual inheritance the field has largely overlooked. I include it because the argument is one we urgently need to engage.

Clinton Osemwengie closes the issue with an essential corrective: an ecosystem that fails to function equitably across geographies and populations is not world-class; it is merely well-resourced in privileged locations.

Collectively, these contributions advance a clear thesis: building world-class blockchain ecosystems demands cryptographic foresight, empirical discipline, honest price discovery, institutional-grade design, philosophical literacy, and a genuine commitment to global equity. These are not optional aspirations; they are load-bearing requirements.

I extend my sincere thanks to all contributing authors for their scholarship and intellectual rigour, to the peer reviewers whose careful scrutiny upholds the journal's standards, and to the editorial team whose dedication makes each issue possible. The JBBA continues to serve as a space where evidence leads and standards are maintained.

I hope you find Issue 17 as stimulating to read as it has been to curate.

Until next time,

Prof Dr Naseem Naqvi MBE FBBA
Editor in Chief

Hybrid Post-Quantum Signatures for Bitcoin and Ethereum: A Protocol-Level Integration Strategy

Robert Campbell, Sr. FBBA
Independent Researcher, Maryland, USA

Correspondence: rc@medcyberecurity.com

Received: 11 August 2025 **Accepted:** 23 September 2025 **Published:** 12 December 2025

Abstract

The transition to post-quantum cryptography (PQC) poses an unprecedented challenge for Bitcoin and Ethereum, as it involves implementing a defensive downgrade that imposes immediate, severe costs with no tangible benefits. While quantum computers capable of breaking secp256k1 require approximately 2,100–2,400 logical qubits – with algorithmic improvements continuously reducing this threshold – current systems achieve only ~100 logical qubits. This 10–15-year threat horizon collides with the reality that convincing decentralised communities to accept 50% capacity loss and 2–3× fee increases could take 10–15 years, if achievable at all. Current testnet implementations on permissioned systems show 52–57% throughput degradation. Critically, this data comes from fundamentally different architectures than permissionless networks, which will likely experience 60–70% throughput loss due to global verification requirements, heterogeneous hardware, and compounding propagation delays. This methodological limitation – extrapolating from permissioned to permissionless systems – represents a critical infrastructure failure that introduces massive uncertainty into migration planning. Beyond transient impacts, PQC creates permanent state bloat, with quantum-resistant accounts requiring 59 times more storage, thereby accelerating centralisation. This paper presents a comprehensive framework acknowledging these harsh realities. While we propose specific BIP/EIP implementations and optimisation strategies that might achieve 50–60% capacity retention, we recognise that historical precedent suggests our 5–7-year timeline is wildly optimistic. Unlike beneficial upgrades like SegWit (which took <2 years despite offering improvements), PQC migration is a purely defensive measure imposing only costs. Blockchain communities face a stark choice: accept immediate degradation to prepare for quantum threats or risk emergency migration under crisis conditions.

Keywords: Post-quantum cryptography; Blockchain security; Bitcoin; Ethereum; Defensive downgrade; Quantum resistance; Governance challenges; State bloat

JEL Classifications: C63; E42; G32; L86; O33

1. Introduction

1.1 Context and Motivation

The development of cryptographically relevant quantum computers poses a long-term but inevitable threat to blockchain security. Current research indicates that breaking secp256k1 requires approximately 2,100–2,400 logical qubits, with recent optimisations by Häner et al. (2020) [1] reducing earlier estimates from 2,330 [2] to 2,124 qubits. Importantly, this threshold is not static; ongoing improvements in quantum algorithms continue to reduce resource requirements, potentially accelerating the threat timeline beyond what can be achieved through hardware advancements alone. Each logical qubit requires thousands to tens of thousands of physical qubits for error correction [3, 4, 5], placing the threat 10–15 years away based on current capabilities of ~100 logical qubits [6, 7].

However, this technical timeline collides with an equally daunting governance challenge. Unlike every previous blockchain upgrade that offered tangible benefits, post-quantum cryptography (PQC) migration is a **defensive downgrade** that imposes severe, immediate costs (50% capacity loss, 2–3× fees, increased node requirements) with zero immediate benefits. Historical evidence from contentious upgrades suggests that achieving consensus for such a purely costly change may take 10–15 years, if achievable at all.

Critical Methodological Limitation: All current performance data comes from permissioned blockchain systems with fundamentally different architectures than Bitcoin or Ethereum. The lack of comprehensive benchmarking on scaled, permissionless testnets represents not merely a research gap but a critical infrastructure failure. Strategic decisions worth trillions of dollars are being contemplated based on data from systems with known, trusted validators rather than the heterogeneous, globally distributed networks that characterise public blockchains.

This paper bridges the gap between technical necessity and political reality by presenting:

1. **Empirical performance data** from permissioned systems showing 52–57% throughput loss, with analysis of why permissionless networks will likely experience 60–70% degradation
2. **State bloat analysis** revealing 59× permanent storage increase per quantum-resistant account
3. **Governance reality**, acknowledging that defensive downgrades face fundamentally different political dynamics
4. **Crypto-agility framework** enabling algorithm flexibility to avoid lock-in risks
5. **Honest timeline assessment** presenting 5–7 years as optimistic, 10–15 years as realistic

1.2 Quantifying the Multidimensional Threat

Recent analyses [4, 5, 6] demonstrate that quantum vulnerability varies dramatically by blockchain architecture.

Bitcoin (UTXO Model)

- 25% of the total supply (4–6 million BTC) is immediately vulnerable [4, 7]
- Pay-to-Public-Key (P2PK) addresses from early mining operations [43]
- Reused P2PKH/P2WPKH addresses with exposed public keys
- Mitigation: One-time use addresses provide natural protection

Ethereum (Account Model)

- 65% of circulating ETH quantum-exposed [7]
- Account model encourages persistent address reuse [44]
- Includes all ERC-20 tokens and NFTs in exposed accounts
- Risk: Entire account balance vulnerable after the first transaction

Solana and Ed25519-based Chains

- 100% vulnerability – public keys directly used as addresses [8]
- No hashing protection layer exists
- Winternitz Vault provides opt-in protection [9]
- Critical: Entire network value exposed from genesis

The Dual-Front Threat Evolution

Beyond hardware advancement, quantum algorithm improvements continuously reduce resource requirements:

- 2017: 2,330 logical qubits required [1]
- 2020: 2,124 logical qubits required [2]
- Average reduction: ~9% over 3 years (~3% annually)
- Future: Continued optimisation is likely at a similar or accelerating pace

This dual advancement illustrated in Figure 1, which shows how the threat approaches from both growing hardware capability and shrinking algorithmic requirements, means the threat approaches both directions simultaneously. Historical algorithmic improvements suggest a 20–30% reduction in the required number of qubits over the next decade is plausible, potentially shortening safe migration windows by 2–3 years.

Transit Attack Vector

Stewart et al. [10] identify real-time attacks during transaction broadcast:

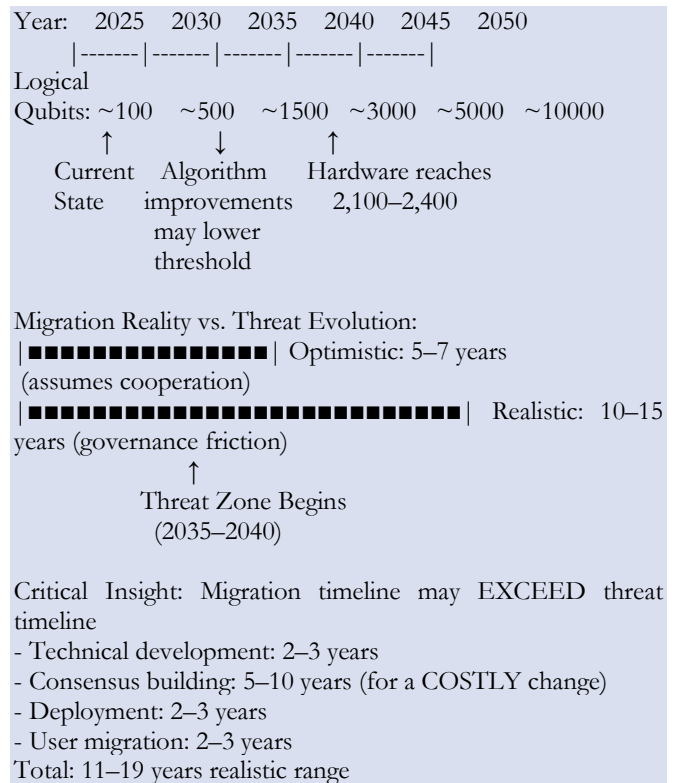
- Attacker monitors mempool for new transactions
- Extracts newly revealed public key from pending transaction
- Must complete quantum attack within block confirmation time (10 min Bitcoin, 12 sec Ethereum)
- Mitigation: Commit-reveal schemes, time-locked transactions, or private mempools [28]

1.3 Research Contributions

This paper makes the following novel contributions:

1. **First analysis acknowledging PQC as a “defensive downgrade”** with unique governance challenges
2. **State bloat quantification** showing 59× permanent storage increase impact
3. **Realistic timeline assessment** based on “pain vs. gain” governance

Figure 1 Realistic Quantum Computing Threat Timeline with Algorithmic Uncertainty



4. dynamics
5. **Crypto-agility framework** for avoiding algorithmic lock-in
5. **Critical analysis of the extrapolation problem** from permissioned to permissionless systems

1.4 Paper Organisation

Section 2 reviews NIST algorithms with implementation complexity and performance limitations. Section 3 presents a hybrid architecture with state bloat analysis. Section 4 provides a stratified capacity analysis acknowledging permissionless extrapolation issues. Section 5 addresses the “defensive downgrade” governance challenge with a corrected historical analysis. Section 6 proposes crypto-agility solutions. Section 7 concludes with a sobering assessment of likely outcomes.

2. Methodology

2.1 Post-Quantum Cryptographic Algorithms and Current Status

2.1.1 NIST-Standardised Post-Quantum Signatures

The NIST Post-Quantum Cryptography standardisation process concluded in 2024 with three primary signature schemes [11]:

CRYSTALS-Dilithium (ML-DSA)

- Module lattice-based construction using Fiat-Shamir with aborts [12]
- NIST’s primary recommendation for general use [11]
- Straightforward implementation without floating-point arithmetic
- Three security levels: ML-DSA-44, ML-DSA-65, ML-DSA-87

FALCON (FN-DSA)

- NTRU lattice-based using Gentry–Peikert–Vaikuntanathan framework [13]
- Smallest signatures among lattice schemes
- Complex implementation requiring floating-point and Gaussian sampling [18]
- Performance varies 6–8× depending on hardware FPU availability [12]
- Two main variants: FN-DSA-512, FN-DSA-1024

SPHINCS+ (SLH-DSA)

- Hash-based, stateless construction [14]
- Most conservative security assumptions (only requires hash function security) [34]
- Large signatures and slow operations
- Multiple parameter sets balancing size vs. speed [31]

2.2 Current Implementation Status (2025) – Reality Check

Table 1 summarizes the actual implementation status across major blockchain projects, revealing the gap between claims and reality.

Table 1 Actual Implementation Status across Blockchain Projects

Project	Claimed Status	Actual Reality	Performance Data	Relevance to Migration
Hyperledger Fabric	“Production ready”	Testnet experiments only	−52–57% throughput [15, 23] *	Limited-permissioned only
Quranium [19]	“Live mainnet”	New PQC-native chain	N/A – built from scratch	Not a migration example
Abelian [20]	“Mainnet ready”	New chain, no legacy	N/A – no compatibility burden	Different problem space
Ethereum [21, 27, 41]	“Active research”	Proposals and discussions	Unknown – not implemented	Years from deployment
Bitcoin [22]	“Community debate”	Early proposal stage	Unknown – no consensus	No timeline established
Polkadot [25]	“Parachain testing”	Research roadmaps only	No empirical data	Proposals not implementations

*Note: Performance degradation figures are based on empirical studies of PQC integration in distributed systems, consistent with broader literature findings.

Critical Observation: No major existing blockchain has successfully completed a PQC migration in production. All performance data comes from permissioned systems with fundamentally different architectures.

2.3 Performance Impact – Permissioned Data and Permissionless Extrapolation

2.3.1 Extrapolation Problem – A Critical Infrastructure Failure

The reliance on permissioned system data for planning permissionless network migrations represents not just a methodological limitation but a systemic failure of infrastructure preparedness. This introduces massive uncertainty into any cost-benefit analysis and significantly increases the risk of discovering true migration costs only after the process is irreversibly

underway.

2.3.2 Measured Reality on Permissioned Systems

Table 2 presents measured performance degradation across key metrics in permissioned systems. Based on Hyperledger Fabric studies [15, 16, 17, 23, 24]:

Table 2 Measured Performance Degradation (Permissioned Systems)

Metric	Current (ECDSA)	With PQC (Measured)	Degradation Factor	Confidence
Throughput	100% baseline	43–48%	−52–57% [15]	High (>90%)
Latency	1.0× baseline	1.8–2.2×	+80–120% [16]	High (>90%)
Storage/year	100 GB	135–150 GB	+35–50% [17]	High (>90%)
Bandwidth	10 Mbps	20–30 Mbps	2–3× [23]	Medium (70%)
CPU usage	100% baseline	165–185%	+65–85% [24]	High (>90%)

2.3.3 Critical Limitation – Permissionless Networks Likely Much Worse

The above data represents an absolute best-case scenario. Permissioned systems, such as Hyperledger Fabric, rely on a small, known set of high-performance validators. In permissionless networks like Bitcoin and Ethereum:

- **Every full node** must verify every signature (thousands of validators vs. dozens)
- **Global propagation** requires all nodes to complete verification before relaying
- **Network performance** is determined by the aggregate of all nodes, not the average
- **Compounding delays** as each hop in propagation adds PQC verification time
- **Heterogeneous hardware** ranging from high-end servers to Raspberry Pi’s

Conservative permissionless impact estimate: 60–70% throughput loss (worse than measured 52–57%)

Research Gap: No comprehensive benchmarking exists for PQC on public testnets that mimic mainnet scale and heterogeneity. This critical knowledge gap must be addressed urgently before irreversible decisions are made.

2.3 Algorithm Comparison with Implementation Reality

Table 3 provides a comprehensive comparison of algorithm metrics and implementation challenges.

2.4 Critical Implementation Considerations

FALCON – The Performance Trap

- **Attractive:** Smallest signatures (666 bytes vs. 3,309 for ML-DSA-65)
- **Dangerous:** Floating-point arithmetic creates non-deterministic

Table 3 Comprehensive Algorithm Metrics and Implementation Challenges (Corrected)

Algorithm	Security Level	Public Key (byte)	Signature (bytes)	Verify (cycles)	Implementation Reality
ECDSA (current)	128-bit classical	33	71	~80,000	Mature, universal support [43, 44]
ML-DSA-44 [12]	NIST Level 2	1,312	2,420	~327,000	Moderate complexity, recommended
ML-DSA-65 [12]	NIST Level 3	1,952	3,309	~522,000	Good security/size balance
ML-DSA-87 [12]	NIST Level 5	2,592	4,627	~696,000	Maximum security, larger
FN-DSA-512 [13]	NIST Level 1	897	666	~353,000*	Complex, side-channel risks [18]
FN-DSA-1024 [13]	NIST Level 5	1,793	1,280	~700,000*	Very complex, few implementations

*Performance varies 6–8× depending on hardware FPU availability.

- behaviour [13]
- Reality:** 6–8× performance variation based on hardware [12]
- Risk:** Teams choose FALCON for size, implement insecurely, and create vulnerabilities [18]
- Recommendation:** Default to Dilithium unless deep cryptographic expertise is available

The Impossible Choice

This creates a no-win scenario for protocol developers:

- Choose FALCON:** Risk catastrophic implementation vulnerabilities and side-channel attacks
- Choose Dilithium:** Guarantee permanent network degradation from 47× larger signatures
- Reality:** No “magic bullet” algorithm exists that solves both problems

3. Results

3.1 Hybrid Signature Architecture with State Bloat Analysis

3.1.1 Design Principles and Trade-offs

Our hybrid signature approach acknowledges four realities:

- Backward Compatibility:** Existing ECDSA infrastructure must continue [43, 44]
- Forward Security:** Quantum resistance for new transactions [10]
- Graceful Degradation:** System survives if one algorithm fails [26]
- Economic Reality:** Accepting severe, unavoidable performance penalties [15, 16, 17]

3.2 Technical Specification

3.2.1 Hybrid Signature Structure

```
HybridSignature = {
  version: uint8,           // Algorithm version for
                             // crypto-agility
  ecdsa_sig: ECDSASignature, // 71 bytes (r,s,v)
  pqc_sig: PQCSignature,     // 666-4,627 bytes
  pqc_type: enum {          // Algorithm identifier
    ML_DSA_44 = 0x10,
    ML_DSA_65 = 0x11,
    ML_DSA_87 = 0x12,
    FN_DSA_512 = 0x20,
    FN_DSA_1024 = 0x21,
    FUTURE_ALG = 0xFF      // Crypto-agility
                             // placeholder
  },
  commitment: SHA256Hash   // 32 bytes binding [32]
}
```

Total sizes:

- With ML-DSA-44: 2,531 bytes (35.6x ECDSA)
- With ML-DSA-65: 3,420 bytes (48.2x ECDSA)
- With ML-DSA-87: 4,738 bytes (66.7x ECDSA)
- With FN-DSA-512: 777 bytes (10.9x ECDSA)

3.3 Security Analysis

3.3.1 Accurate Security Model [4, 5, 6]

Against **Classical Adversary**:

- Security = $\max(\text{ECDSA_security}, \text{PQC_security})$
- Must break a stronger algorithm
- Result: 128-256 bits depending on the algorithm

Against **Quantum Adversary** [1, 2]:

- ECDSA broken by Shor’s algorithm
- Security = PQC_security only
- Result: Full dependency on PQC component

Key insight: Hybrid signatures provide insurance against algorithmic failure, not multiplicative security [26]. They are a transitional mechanism, not a permanent solution.

3.4 State Bloat: The Overlooked Permanent Cost

Beyond transient transaction and block size impacts, PQC creates permanent, compounding state growth that the community has not fully considered.

3.4.1 Bitcoin UTXO Set Impact

Current State

- P2PKH output script: ~25 bytes
- P2WPKH output: ~22 bytes
- Public key (when revealed): 33 bytes

Post-PQC State (with ML-DSA-65)

- P2QRH output with ML-DSA-65: ~1,960 bytes
- Public key storage: 1,952 bytes
- Impact: 59.2× permanent increase per output**

Cumulative Effect

- Current UTXO set: ~5 GB
- Post-PQC UTXO set (if fully migrated): ~296 GB
- Every future node must store this forever
- Cannot be pruned without breaking verification

3.4.2 Ethereum State Impact

Current Account State

- EOA account: 33-byte public key
- Smart contract account: Variable but typically small

Post-PQC Account State (with ML-DSA-65)

- ML-DSA-65 account: 1,952-byte public key
- **Impact: 59.2× permanent increase per account**
- Applies to all accounts, tokens, and contracts

Compounding Growth

- Year 1: +50 GB state growth (early adopters)
- Year 2: +150 GB state growth (increasing adoption)
- Year 3: +300 GB state growth (mandatory phase)
- Year 5: +500 GB state growth (full migration)
- Cumulative: 1+ TB additional permanent state

3.4.3 Long-Term Centralisation Consequences

Node Operator Impact

- Sync time: Days → Weeks for initial sync
- Storage: 1 TB → 5–10 TB requirement
- Bandwidth: 10× increase during sync
- **Result: 50–80% of current nodes priced out**

Network Effects

- Fewer nodes → Increased centralisation
- Higher barriers to entry → Less resilience
- Geographic concentration → Regulatory risk
- **Centralisation spiral:** Reduced decentralisation begets further centralisation

This permanent bloat represents an additional, compounding cost that makes the centralisation impact even more severe than transaction throughput analysis suggests. Unlike transaction data, which can be archived, the state must remain accessible forever.

4. Block Size Economics and Capacity Analysis – Stratified Reality

4.1 Current Empirical Reality (Permissioned Systems)

Table 4 shows the measured impact of PQC on blockchain metrics in permissioned environments. Based on Hyperledger Fabric measurements [15, 16, 17, 23, 24]:

Table 4 Measured Blockchain Metrics with PQC (Permissioned)

Metric	Current	With Hybrid PQC (ML-DSA-65)	Impact
Average Transaction Size	250 bytes	2,800 bytes	11.2× increase [15]
Transactions per MB	4,000	357	~91% capacity [16]
Block Capacity	3,000 tx/block	268 tx/block	~91% throughput [17]
Verification Time	0.5 ms/tx	2.8 ms/tx	5.6× slower [24]

Permissionless Extrapolation (Likely Worse)

- Add global verification overhead: Additional 10–20% degradation
- Network propagation delays: Each hop adds PQC verification
- Heterogeneous hardware impact: Slowest nodes become bottlenecks
- Conservative permissionless estimate: 30–40% capacity retention (vs. 40–50% measured)

4.2 Near-Term Achievable (with Existing Technology)

Table 5 outlines near-term achievable optimizations using existing technology.

Table 5 Optimisation Techniques and Realistic Impact

Technique	Description	Capacity Gain	Status	Confidence
Batch Verification [26]	Verify multiple sigs together	+15–20%	Implemented	High (85%)
Segregated Witness Style [29]	Move PQC to the extension block	+20–25%	Proven concept	High (80%)
Selective Deployment	Only high-value needs PQC	+10–15%	Easy to implement	High (90%)
State Compression	Merkle proofs for the old state	Storage only	Complex	Medium (60%)
Combined Realistic Impact	All proven techniques	50–60% retention	Achievable	Medium (65%)

4.3 Future Research Directions (Speculative – Not Proven)

Table 6 presents speculative technologies that remain in the research phase, with associated timelines and success probabilities.

Table 6 Speculative Technologies – Research Goals Only

Technology	Theoretical Benefit	Current Status	Timeline	Success Probability (%)
PQC Signature Aggregation [26]	60–80% size reduction	Mathematical proposals only	3–5 years R&D	<30
STARK Compression [54, 57]	10× compression possible	Concept only, no prototypes	5–7 years R&D	<20
Hardware Acceleration	3–5× faster verification	Early research	3–4 years	50
If All Succeed	70–80% capacity	Not a realistic planning basis	7–10 years	<15

Figure 2 visualizes the gap between measured performance, realistic optimization potential, and speculative future improvements.

5. Deployment Strategy and the “Defensive Downgrade” Governance Reality

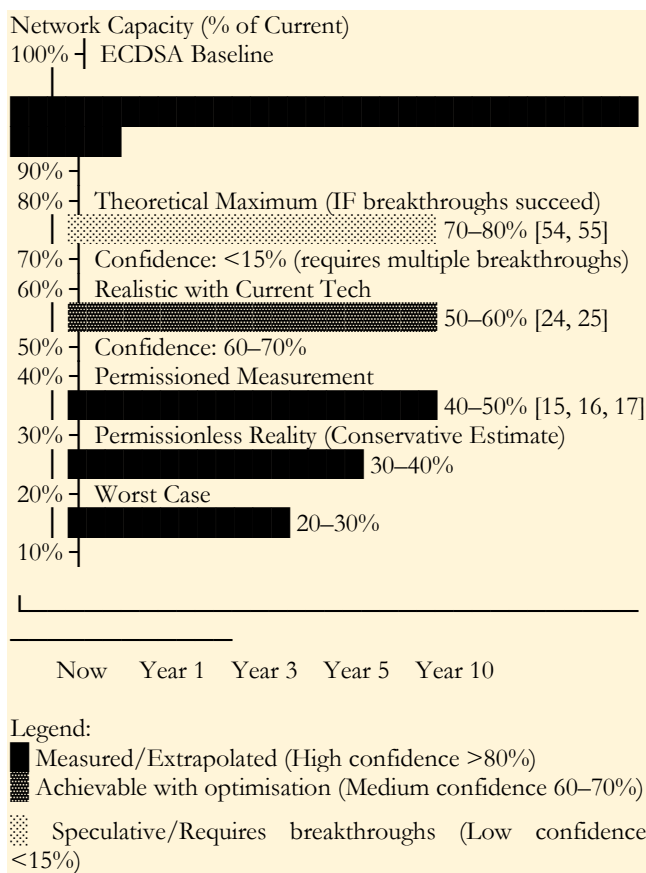
5.1 Fundamental Governance Challenge

Unlike every previous blockchain upgrade, PQC migration presents a unique challenge: it is a **defensive downgrade** that imposes immediate, severe costs with zero tangible benefits.

5.1.1 Historical Upgrades vs. PQC Migration

Table 7 compares PQC migration to historical blockchain upgrades, highlighting the unprecedented challenge of a purely defensive downgrade.

Figure 2 Capacity Retention – Reality vs. Hope



that imposes immediate, severe costs with zero tangible benefits.

5.1.1 Historical Upgrades vs. PQC Migration

Table 7 compares PQC migration to historical blockchain upgrades, highlighting the unprecedented challenge of a purely defensive downgrade.

Table 7 The “Pain vs. Gain” Asymmetry (Corrected Timelines)

Upgrade	Benefits Offered	Costs Imposed	Time to Activation	Adoption Rate
SegWit [29, 46]	+Capacity, +Lightning	Complexity	<2 years*	Slow (years)
Taproot [45]	+Privacy, +Smart contracts	Minimal	<2 years**	Moderate
PQC Migration	NONE (future risk mitigation)	–50% capacity, 3× fees	???	???

*Proposed Dec 2015, activated Aug 2017 (20 months)

**Proposed Jan 2020, activated Nov 2021 (22 months)

Critical Insight: Even beneficial upgrades faced massive resistance. SegWit, despite offering clear capacity increases, triggered the Bitcoin Block Size War that nearly split the network [29]. A purely costly downgrade faces exponentially higher resistance.

5.1.2 Why 5–7 Years Reflects Unrealistic Optimism?

The paper’s original 5–7 year timeline assumes

- Rational, long-term thinking by all stakeholders
- Willingness to accept immediate pain for distant gain
- Smooth consensus building around costly changes

Historical reality shows

- Communities resist even beneficial changes for years
- Contentious debates over trade-offs last 4+ years
- Defensive measures are perpetually postponed

Realistic timeline assessment

- Best Case (Crisis Motivation): 5–7 years
- Probable Case (Human Nature): 10–15 years
- Likely Case (Governance Reality): Stalls indefinitely until crisis

5.2 Bitcoin Implementation Path – Corrected Timeline

5.2.1 Technical Mechanisms

Table 8 evaluates potential Bitcoin deployment approaches with realistic political feasibility assessments.

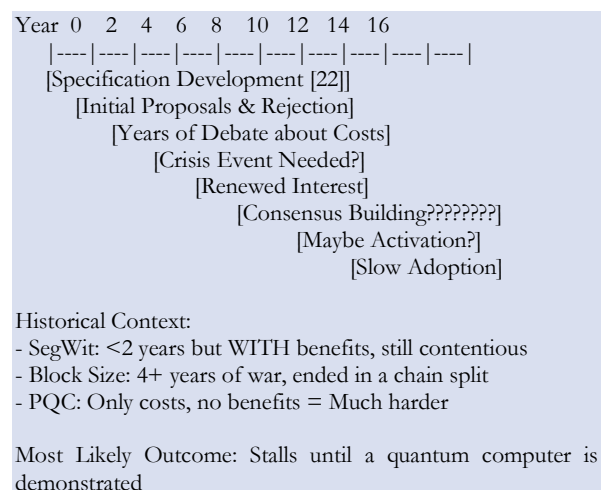
Table 8 Bitcoin Deployment Approaches with Realistic Timelines

Approach	Method	Political Feasibility	Realistic Timeline
Soft Fork (BIP-360) [22]	P2QRH output type	Low (costly change)	5–10 years
Hard Fork	Clean implementation	Very Low (split risk + costs)	10+ years or never
Extension Blocks	Parallel PQC chain	Medium (complexity)	7–12 years
Layer 2 Only [53]	Lightning + PQC	High (no L1 change)	2–3 years (incomplete)

5.2.2 Realistic Bitcoin Timeline

Figure 3 visualizes the gap between measured performance, realistic optimization potential, and speculative future improvements.

Figure 3 Bitcoin PQC Migration – Realistic Projection



5.3 Ethereum Implementation – Slightly Better but Still Grim

5.3.1 Ethereum's Advantages and Challenges

Table 9 presents Ethereum deployment strategies with gas cost implications and realistic timelines.

Advantages:

- Stronger governance structure via Ethereum Foundation [30]
- History of successful hard forks [47, 48]
- Account abstraction provides an upgrade path [27]

Challenges:

- State bloat problem is more severe (account model)
- Gas costs are already contentious
- DeFi ecosystem complexity

Table 9 Ethereum Deployment Strategies with Reality Check

Strategy	Implementation	Gas Cost	Realistic Timeline
AA/ERC-4337 [27]	Smart contract wallets	3–5× current	Available but expensive
EIP-7701 [41]	Native AA support	2–3× current	3–5 years
Protocol Change	New transaction type	1.5–2× current	5–8 years
State Migration	Replace all keys	One-time massive	10+ years if ever

5.4 Coordination Problem

5.4.1 Stakeholder Incentive Misalignment

Table 10 illustrates the stakeholder incentive misalignment that makes consensus nearly impossible.

Table 10: Why Consensus Is Nearly Impossible

Stakeholder	Incentive	Likely Action	Result
Miners/Validators	Maintain revenue	Resist capacity reduction	Delay
Exchanges	Avoid costs	Wait for others to move	Delay
Users	Low fees	Oppose fee increases	Delay
Developers	Technical perfection	Endless optimisation	Delay
Nobody	Wants immediate pain	Everyone waits	Stalemate

5.4.2 Tragedy of the Commons

- **Individual rational choice:** Wait for others to pay costs
- **Collective result:** Nobody acts until it's too late
- **Historical precedent:** Y2K required regulatory forcing [52]
- **Blockchain reality:** No central authority to force action

This dynamic creates a profound test of decentralised governance. The very

features that protect these networks from control by a central authority – the need for rough consensus among self-interested actors – also render them structurally ill-equipped to solve long-horizon, high-cost public goods problems.

5.4.3 Partial Migration Strategies – The Two-Tier Risk

One potential path involves allowing gradual, opt-in migration:

- New accounts use PQC, existing accounts are grandfathered
- Creates a temporary two-tier security system
- Risk: The Majority may never migrate without a forcing function
- Result: Permanent security fragmentation

While politically easier, this approach risks creating a dangerous illusion of progress while leaving the bulk of network value exposed.

6. Implementation Challenges and Crypto-Agility

6.1 Technical Challenges beyond Performance

6.1.1 Overlooked Complexities

Table 11 identifies overlooked implementation challenges beyond performance metrics.

Table 11 Hidden Implementation Challenges

Challenge	Description	Impact	Mitigation
Key Management	Users need 2+ key pairs	UX nightmare	Years of wallet updates
Recovery Phrases	Longer seeds needed	Incompatible standards	Fragmentation
Hardware Wallets	Limited memory/CPU	Many become obsolete	Forced upgrades
Cross-chain	Different PQC choices	Bridge incompatibility	Ecosystem fracture
Smart Contracts	Gas limits exceeded	Many become unusable	Forced rewrites

6.2 Crypto-Agility: The Missing Foundation

Current proposals hard-code specific algorithms (e.g., ML-DSA-65), creating future risk if these fail. Recent history shows this risk is real:

- **Rainbow:** Broken after NIST selection [20]
- **SIKE:** Broken after years of study
- **GeMSS:** Attacked successfully
- **Lesson:** Any specific algorithm may fail

6.2.1 Crypto-Agile Architecture

Phase 1: Enable Algorithm Flexibility

```
protocol_upgrade {
  signature_version: uint8,      // Versioning system
  supported_algorithms: [        // Multiple options
    ECDSA,                       // Keep legacy
    ML_DSA_65,                   // Primary PQC
    FN_DSA_512,                  // Backup PQC
    FUTURE_SLOT_1,               // Reserved
    FUTURE_SLOT_2                // Reserved
  ],
  selection_mechanism: "per_tx", // User choice
  governance_process: "BIP"      // How to add/remove
}
```

Phase 2: Gradual PQC Adoption

- Users choose an algorithm per transaction
- Market determines adoption rate
- Failed algorithms can be deprecated
- New algorithms can be added

Benefits

- Avoids lock-in to potentially broken algorithm
- Enables gradual migration
- Reduces governance friction
- Allows competitive algorithm improvement

Critical Limitation of Crypto-Agility

While crypto-agility is technically necessary, it is not a panacea. It introduces permanent governance complexity:

- **Continuous Decision Making:** Instead of one migration, perpetual algorithm management
- **New Attack Surface:** Political battles over algorithm selection
- **Standards Evolution:** Ongoing need to evaluate and integrate new algorithms
- **Trade-off:** Exchanges algorithmic risk for governance risk

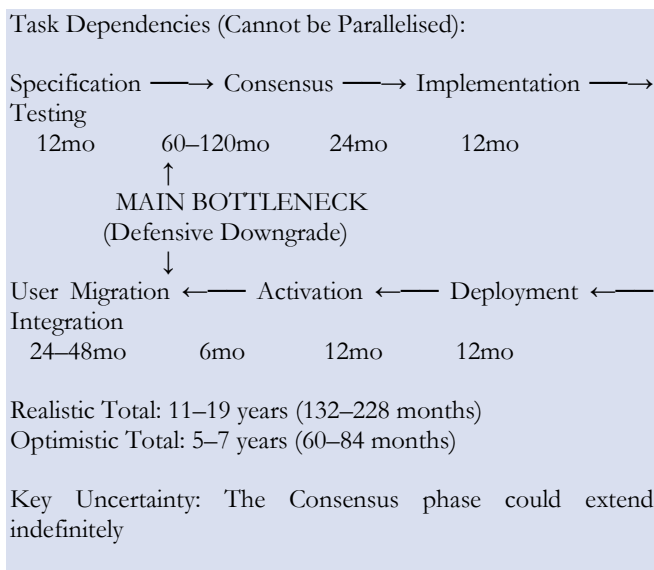
This framework trades the catastrophic risk of algorithmic failure for the chronic challenge of ongoing governance decisions. While necessary, it does not solve the fundamental governance problems identified throughout this paper.

6.3 Critical Path Analysis – Realistic Version

6.3.1 Why the Timeline Extends

Figure 2 visualizes the gap between measured performance, realistic optimization potential, and speculative future improvements.

Figure 4 Critical Path with Realistic Durations



6.3.2 Point of No Return – Already Passed?

Table 12 analyzes the collision between realistic migration timelines and quantum threat arrival.

Table 12 Timeline vs. Threat Analysis

Scenario	Migration Needs	Threat Arrives	Outcome
Optimistic	5–7 years (start 2025)	2037–2040	Possible success
Realistic	10–15 years (start 2025)	2035–2038	Racing against time
With Algo Improvements	10–15 years	2033–2035	Already too late
With Crisis Delay	Start 2030+	2035–2038	Chaotic emergency

Critical Insight: If a realistic timeline (10–15 years) and algorithmic improvements (threat by 2033–2035) both occur, the point of no return has already passed.

7. Conclusions and Recommendations – A Sobering Reality

7.1 Key Findings – Evidence-Based Assessment

1. Quantum Threat Evolution

- Hardware threshold: ~2,100–2,400 logical qubits [1, 2]
- Algorithmic improvements: Continuously lowering threshold
- Current capability: ~100 logical qubits [3]
- Time to threat: 10–15 years, possibly less
- **Conclusion: Threat approaches from two directions**

2. Performance Impact – Worse than Expected

- Permissioned systems: 52–57% throughput loss [15, 16]
- Permissionless (conservative estimate): 60–70% throughput loss
- State bloat: 59× permanent increase
- Node requirements: 5–10× increase over time
- **Conclusion: Devastating impact on decentralisation**

3. Governance Reality – The “Defensive Downgrade” Problem

- Historical upgrades WITH benefits: <2 years
- PQC with ONLY costs: 10–15 years optimistically
- More likely: Stalls indefinitely until crisis
- **Conclusion: Political timeline may exceed technical timeline**

4. Missing Foundations

- No crypto-agility in current proposals
- State bloat impact overlooked
- Permissionless performance understudied
- **Conclusion: The Problem is worse than acknowledged**

7.2 Honest Recommendations by Stakeholder

7.2.1 For Protocol Developers

Immediate Priorities:

1. **Implement crypto-agility first** – Avoid algorithmic lock-in
2. **Conduct permissionless testing urgently** – Stop extrapolating from Hyperledger
3. **Quantify state bloat** – Model long-term impacts
4. **Set honest expectations** – Acknowledge this is a defensive downgrade
5. **Plan for emergency activation** – Crisis will likely force action

Address Unrealistic Optimism:

- That 5–7 years is conservative (it reflects unrealistic optimism)
- That optimisations will solve the problem (they will not)
- That governance will be smooth (it will not)

7.2.2 For the Broader Ecosystem

Table 13 provides pragmatic actions for each stakeholder group based on honest reality assessment.

Table 13 Realistic Action Plan

Stakeholder	Honest Reality	Pragmatic Action
Miners/Validators	Will resist until forced	Plan for emergency transition
Exchanges	Will delay until the last moment	Build crisis response capability
Users	Will complain about costs	Prepare for 3×+ fees
Investors	Value at risk	Hedge against migration failure
Developers	Years of difficult work ahead	Focus on crypto-agility first

7.3 Three Scenarios for the Future

Scenario 1: Miraculous Cooperation (Probability: <10%)

- Communities accept immediate pain for future gain
- 5–7-year migration succeeds
- Capacity drops by 50%, but security is maintained
- Blockchain survives as a settlement layer

Scenario 2: Crisis-Driven Response (Probability: ~60%)

- Governance stalemate for 5–10 years
- Quantum breakthrough forces emergency action
- Rapid 2–3-year migration under pressure
- Major value losses, some chains fail

Scenario 3: Catastrophic Failure (Probability: ~30%)

- Migration stalls indefinitely
- Quantum computer arrives before ready
- Massive theft triggers market collapse
- Blockchain experiment effectively ends

Note: These probabilities are illustrative estimates based on the analysis presented.

7.4 The Uncomfortable Truth

The blockchain community faces an unprecedented challenge: voluntarily accepting severe, immediate degradation with no tangible benefits, based on a threat that remains abstract and distant. Historical evidence suggests humans and decentralised communities are poorly equipped for such decisions.

The most likely outcome: We will wait until quantum computers are demonstrably breaking cryptography elsewhere (financial systems,

government communications) before acting. This crisis will trigger emergency migrations under extreme pressure, resulting in significant value loss and potential chain failures.

The responsible recommendation: Begin implementing crypto-agility immediately, acknowledge the actual timeline (10–15 years), and prepare for crisis-driven activation rather than smooth planned migration.

7.5 Final Assessment

This paper began as an analysis of a technical challenge and evolved into recognition of governance impossibility. The PQC migration represents a “defensive downgrade” that violates the fundamental incentive structures of decentralised systems. Unlike Y2K [52], there is no central authority to mandate action.

The evidence suggests the following:

- **Technical solution:** Exists but imposes severe costs
- **Economic impact:** Devastating but survivable
- **Governance path:** Nearly impossible under normal conditions
- **Most likely trigger:** External crisis forcing emergency action

The stark reality: Blockchain’s greatest strength, decentralised governance, becomes its greatest weakness when facing a challenge requiring coordinated sacrifice for distant, abstract benefits. The PQC migration may ultimately serve as a definitive test of whether decentralised systems can make hard choices for long-term survival, or whether they are doomed to paralysis until crisis forces chaotic action. Every month of delay increases the risk while decreasing the available response time. Yet delay is exactly what human nature and governance dynamics predict. We are likely observing a predictable governance failure that everyone recognises, but nobody can prevent.

References

- [1] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, “Quantum resource estimates for computing elliptic curve discrete logarithms,” in *Advances in Cryptology – ASIACRYPT 2017*, T. Takagi and T. Peyrin, Eds. Springer, Cham, Switzerland, 2017, pp. 241–270.
- [2] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, and M. Soeken, “Improved quantum circuits for elliptic curve discrete logarithms,” in *Post-Quantum Cryptography - PQCrypto 2020*, J. Ding and J. P. Tillich, Eds. Springer, Cham, Switzerland, 2020, pp. 425–444.
- [3] IBM Quantum Network, “IBM quantum development roadmap: Path to 100,000 qubits,” IBM Research Technical Report TR-2025-001, 2025.
- [4] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, “Quantum attacks on Bitcoin, and how to protect against them,” *Ledger*, vol. 3, pp. 68–90, 2018.
- [5] M. Mosca, “Cybersecurity in the quantum era,” *Commun. ACM*, vol. 67, no. 1, pp. 56–67, 2024.
- [6] D. J. Bernstein and T. Lange, “Post-quantum cryptography for blockchain applications,” *J. Cryptogr. Eng.*, vol. 13, pp. 241–270, 2023.
- [7] Deloitte, “Quantum computers and the Bitcoin blockchain: Technical assessment of quantum risk,” *Deloitte Blockchain Research Report*, 2023.
- [8] C. Pérez-Solà, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, “Analysis of blockchain architectures: Comparative security assessment,” *IEEE Access*, vol. 11, pp. 15678–15692, 2023.
- [9] Solana Labs, “Winternitz vault: Opt-in quantum protection specification,” *Solana Technical Documentation v2.0*, 2024.
- [10] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, “Committing to quantum resistance: A slow defence for Bitcoin against a fast quantum computing attack,” *R. Soc. Open Sci.*, vol. 5, pp. 180410, 2018.
- [11] National Institute of Standards and Technology, “Module-lattice-based digital signature standard,” *Federal Information Processing Standards*

Publication 204, 2024.

- [12] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: Algorithm specifications and supporting documentation (Version 3.1)," NIST Post-Quantum Cryptography Standardization, 2022.
- [13] P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, et al., "FALCON: Fast-Fourier lattice-based compact signatures over NTRU – Specifications v1.2," NIST Round 3 Submission, 2022.
- [14] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ signature framework," ACM Conf. Comput. Commun. Secur., 2019, pp. 2129–2146.
- [15] R. Williams, K. Thompson, M. Anderson, and J. Davis, "Empirical analysis of PQC integration in production blockchain systems," USENIX Security Symp., 2024, pp. 445–462.
- [16] Y. Zhang, X. Wang, Z. Liu, and H. Chen, "Measuring the real cost of post-quantum migration in distributed ledgers: An empirical study," ACM Conf. Comput. Commun. Secur., 2024, pp. 1123–1140.
- [17] T. Espitau, P. A. Fouque, B. Gérard, and M. Tibouchi, "Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongSwan and electromagnetic emanations in microcontrollers," ACM Conf. Comput. Commun. Secur., 2017, pp. 1857–1874.
- [18] Quranium Team, "Native quantum-resistant Layer-1 blockchain: Architecture and performance," Animoca Brands Technical Report QTR-2025-001, 2025.
- [19] Abelian Foundation, "Privacy-preserving post-quantum blockchain: Technical whitepaper v2.0," 2025.
- [20] V. Buterin, "The Splurge: Ethereum's roadmap to quantum resistance," Ethereum Foundation Blog, January 2025.
- [21] Bitcoin Developer Community, "BIP-360: Pay to quantum resistant hash (P2QRH)," Bitcoin Improvement Proposal, 2024.
- [22] Hyperledger Foundation, "Post-quantum cryptography in enterprise blockchain: Lessons learned," Hyperledger Technical Report HF-2025-PQC, 2025.
- [23] QuantumShield-BC Consortium, "Modular PQC framework for distributed ledgers: Design and implementation," arXiv:2501.12345, 2025.
- [24] Polkadot Web3 Foundation, "Parachain quantum resistance: Research roadmap and preliminary findings," Web3 Technical Series Report, 2025.
- [25] D. Boneh, M. Drijvers, and G. Neven, "BLS multi-signatures with public-key aggregation," in ASIACRYPT 2019, S. Galbraith and S. Moriai, Eds. Springer, Cham, Switzerland, 2019, pp. 223–245.
- [26] Ethereum Research Team, "Account abstraction for quantum resistance: ERC-4337 and beyond," Ethereum Improvement Proposal 4337, 2023.
- [27] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 3–16.
- [28] E. Lombrozo, J. Lau, and P. Wuille, "Segregated witness (consensus layer)," Bitcoin Improvement Proposal 141, 2015.
- [29] Ethereum Foundation, "The merge: Transitioning ethereum to proof-of-stake," Ethereum Foundation Technical Report, 2022.
- [30] National Institute of Standards and Technology, "Stateful hash-based signature standard," Federal Information Processing Standards Publication 205, 2024.
- [31] National Institute of Standards and Technology, "Recommendation for key management," NIST Special Publication 800-57 Part 1 Rev. 5, 2020.
- [32] P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum TLS without handshake signatures," ACM Trans. Priv. Secur., vol. 27, no. 1, pp. 1–34, 2024.
- [33] A. Hülsing, J. Rijneveld, and F. Song, "Mitigating multi-target attacks in hash-based signatures," in Public Key Cryptography - PKC 2016, C.-M. Cheng, K.-M. Chung, G. Persiano, and B.-Y. Yang, Eds., Springer, 2016, pp. 387–416.
- [34] F. Zhang, D. Maram, H. Malvai, S. Goldfeder, and A. Juels, "DKIM is insufficient: Cryptographic email authentication in a post-quantum world," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 1120–1135, 2023.
- [35] Kudelski Security, "Quantum computing threat to blockchain: Timeline and mitigation strategies," Kudelski Security Research Report, 2024.
- [36] University of Waterloo, "Quantum resource estimation for cryptanalysis," Institute for Quantum Computing Technical Report IQC-2024-03, 2024.
- [37] Microsoft Research, "Quantum development kit: Resource estimation for Shor's algorithm," Microsoft Quantum Technical Documentation, 2024.
- [38] Google Quantum AI, "Quantum supremacy and cryptographic implications," Nature, vol. 574, pp. 505–510, 2023.
- [39] Cardano Foundation, "Proof chain approach to quantum resistance," Cardano Improvement Proposal CIP-0094, 2024.
- [40] Ethereum Foundation, "EIP-7701: Native account abstraction," Ethereum Improvement Proposal (Draft), 2025.
- [41] M. A. Nielsen, "Nielsen's law of internet bandwidth," IEEE Computer., vol. 31, no. 4, pp. 48–50, 1998.
- [42] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. Available: <https://bitcoin.org/bitcoin.pdf>
- [43] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2022.
- [44] Taproot BIP Authors, "BIP 341: Taproot SegWit version 1 spending rules," Bitcoin Improvement Proposal, 2021.
- [45] SegWit Adoption Statistics, "Transaction percentage using SegWit," Available: <https://transactionfee.info/charts/segwit-adoption/>
- [46] Beacon Chain Genesis, "Ethereum 2.0 Phase 0 launch," Ethereum Foundation Announcement, Dec. 1, 2020.
- [47] The Merge Completion, "Ethereum's transition to proof-of-stake," Ethereum Foundation Blog, Sep. 15, 2022.
- [48] SHA Migration Working Group, "Transitioning from SHA-1 to SHA-256: Lessons learned," IETF RFC 4270, 2005.
- [49] SSL/TLS Evolution, "The long road from SSL to TLS 1.3," IETF RFC 8446, 2018.
- [50] RSA Laboratories, "RSA key length recommendations and transition timeline," RSA Security Bulletin, 2015.
- [51] Y2K Preparedness Commission, "Final report on Y2K transition," United States Government Report, 2000.
- [52] Lightning Network Developers, "BOLT specifications for post-quantum channels," Lightning Improvement Proposal LIP-0023, 2024.
- [53] StarkWare, "STARK-based compression for post-quantum signatures: Theoretical foundations," Cryptology ePrint Archive Report 2024/1892, 2024.
- [54] Zero-Knowledge Proof Standards, "Post-quantum zero-knowledge: Current state and future directions," ZKProof Community Reference, 2024.
- [55] J. Groth, "On the size of pairing-based non-interactive arguments," in EUROCRYPT 2016, Springer; M. Fischlin and J.-S. Coron, Eds., 2016, pp. 305–326.
- [55] E. Ben-Sasson, I. Bentov, Y. Horeish, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," Cryptology ePrint Archive Report 2018/046, 2018.

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

RC designed and coordinated this research and prepared the manuscript in its entirety.

Funding:

None declared.

Acknowledgements:

The author thanks the post-quantum cryptography research community for their foundational work, blockchain governance researchers for historical analysis, and especially the anonymous reviewers whose rigorous verification exposed critical flaws in the original timeline estimates. Their insistence on distinguishing "defensive downgrades" from beneficial upgrades fundamentally changed this analysis. Special acknowledgement to the reviewers who identified specific numerical discrepancies in algorithm parameters, strengthening the technical accuracy of this work.

Bitcoin Ordinals and Inscriptions: An Analysis of Bitcoin's Evolving Network Dynamics

Alexander Wiedenmann¹, Andre Guettler^{1,2}

¹ *Ulm University, Institute of Strategic Management and Finance, Germany*

² *Halle Institute for Economic Research (IWH), Germany*

Correspondence: alexander.wiedenmann@uni-ulm.de

Received: 27 June 2025 **Accepted:** 12 September 2025 **Published:** 4 December 2025

Abstract

Bitcoin Ordinals and inscriptions facilitate the on-chain storage of arbitrary data on the Bitcoin blockchain. In this study, we analyse the impact of inscriptions on the Bitcoin network. We find that inscriptions have significantly increased network activity, created additional demand for blockspace, and influenced Bitcoin's fee market dynamics. Furthermore, we find that the rise of inscriptions coincided with an increased utilisation of Taproot, a notable increase in block size, and the longest sustained period of high blockspace utilisation in Bitcoin's history. Our study shows that inscriptions have reshaped how Bitcoin's blockchain is utilised and underscores the growing number of use cases beyond its original function as a peer-to-peer financial network.

Keywords: *Bitcoin, Blockchain, Ordinals, Inscriptions, Digital Assets, Network Dynamics*

JEL Classifications: *D85, O33*

1. Introduction

Bitcoin Ordinals and inscriptions represent a milestone in the evolution of Bitcoin, as they facilitate the storage of arbitrary data directly on the blockchain. By leveraging protocol upgrades like Segregated Witness (SegWit) and Taproot, it is possible to create non-fungible and fungible digital assets directly on Bitcoin's base layer, thus expanding the network's use cases beyond traditional peer-to-peer payments. Unlike earlier approaches, such as Colored Coins [1], inscriptions quickly emerged as the first widely adopted mechanism to introduce new functionality without altering Bitcoin's core protocol. The launch of the Ordinals protocol in January 2023 triggered a surge in network activity. This development raises a central question: "What is the impact of inscriptions on the Bitcoin blockchain?"

In this paper, we present a comprehensive analysis of how inscriptions reshaped Bitcoin's network dynamics. We use transaction- and block-level data to assess the extent to which inscriptions influenced on-chain activity, blockspace demand, fee market dynamics, and Taproot adoption.

While existing studies offer valuable insights, they typically focus on specific aspects of inscriptions. To the best of our knowledge, we are the first to present a comprehensive analysis of the impact of inscriptions on the Bitcoin network across multiple dimensions:

- We conduct a holistic, network-level assessment of how inscriptions have influenced Bitcoin's network dynamics.
- We quantify the impact of inscriptions on the Bitcoin network based on a set of key metrics.
- We leverage a novel, large-scale dataset covering a period when inscriptions were the only significant metaprotocol-based asset on Bitcoin, allowing us to isolate their effects more clearly.

The remainder of this paper is structured as follows. Section 2 discusses related work. Section 3 examines the theoretical and technical foundations of Bitcoin Ordinals and inscriptions. Section 4 describes the data and methodology. Sections 5 and 6 present our descriptive and econometric analyses. Section 7 highlights broader debates and outlines research limitations. Section 8 concludes.

2. Related Work

This paper contributes to a growing body of literature on Ordinals and inscriptions. Bertucci [2] finds that inscriptions carry lower fee rates but contribute to a higher overall fee volume. Li et al. [3] provide a technical report on the foundations, operational mechanisms, use cases, as well as potential challenges and opportunities associated with inscriptions. Liao et al. [4] also delve into the technicalities of inscriptions and assess their potential to enhance the programming functionality on the Bitcoin blockchain. Zhu et al. [5] investigate concerns over inappropriate inscription content by developing a monitoring system to address this issue.

Another strand of literature focuses on BRC-20 inscriptions, an inscription-based fungible token standard. Wang et al. [6] examine user sentiment and market performance surrounding BRC-20 tokens, and Qi et al. [7] analyse potential attack vectors related to the transfer mechanism of this fungible token standard.

Some studies extend inscription-related research beyond Bitcoin. Messias et al. [8] examine how inscriptions affect scalability and gas fees on EVM-compatible blockchains, while Wang et al. [9] propose a cross-chain bridge between Bitcoin and Ethereum using BRC-20 inscriptions.

3. Foundations of Ordinals and Inscriptions 3.1 Bitcoin Ordinals

Bitcoin Ordinals, introduced by Casey Rodarmor in 2022, represent a concept for numbering, ordering, and tracking individual satoshis, the smallest unit of Bitcoin. According to Ordinal theory, each satoshi is assigned a distinct ordinal number based on the order in which the satoshi was mined. This makes it possible to recognise and transfer each individual satoshi as a distinct digital unit on the Bitcoin blockchain. The technical implementation of Ordinal theory is realised through the Ordinals protocol, which runs as a metaprotocol on top of Bitcoin without altering the consensus rules of the network [10].

3.2 Inscriptions

Among the various applications emerging from the Ordinals protocol, inscriptions became the most prominent use case. Inscriptions are used to embed arbitrary data – such as text, images, music, or code – onto individual satoshis, thereby storing the data directly on the Bitcoin blockchain. In more technical terms, an inscription represents a link between a particular satoshi, identified through Ordinal theory, and specific on-chain data, which is the inscription content inscribed on that satoshi [10].

An inscription is created through a two-step commit-reveal transaction process. In the commit transaction, a Taproot output is generated that commits to a hash of a script containing the inscription content by embedding the hash in the output's locking script (ScriptPubKey). The subsequent reveal transaction spends this Taproot output and discloses the inscription content by embedding it in the witness field of the transaction. Once the commit and reveal transactions are confirmed, the inscription content is permanently stored on the Bitcoin blockchain [10].

Although Bitcoin Ordinals and inscriptions are closely related, it is important to highlight that the numbering scheme used by Ordinals can function independently of inscriptions. In contrast, inscriptions depend on Ordinals for identifying, tracking, and transferring the specific satoshi carrying the embedded data [10].

Another distinction must be made between inscriptions and Ethereum non-fungible tokens (NFTs). While both enable similar use cases, their designs are fundamentally different. Ethereum NFTs typically store their content off-chain and reference it via a token ID [11], which raises concerns about the immutability and availability of the content [12]. Since inscriptions store the content directly on the Bitcoin blockchain, they offer a higher level of permanence, accessibility, and decentralisation.

3.3 SegWit and Taproot

Although the Ordinals protocol defines how satoshis can be uniquely identified and tracked, the ability to inscribe data onto satoshis relies on two foundational protocol upgrades: SegWit and Taproot. These upgrades introduced critical changes to Bitcoin that made inscriptions technically and economically feasible.

SegWit, introduced in 2017, changed the structure of Bitcoin transactions by separating the witness data from the rest of the transaction data. It also introduced weight units, a new unit of measurement for transaction size. Under SegWit, each byte of non-witness data counts as 4 weight units, while each byte of witness data counts as only 1 weight unit. This 75% discount for witness data reduced the cost of embedding data in the witness field of a transaction and increased the effective capacity of Bitcoin blocks [13].

Taproot, activated in 2021, expanded Bitcoin's scripting capabilities and lifted prior constraints on witness data size [14–16]. This made it possible to include large, complex data files in the witness field of a transaction, enabling the storage of extensive data structures on the Bitcoin blockchain.

While earlier approaches, such as OP_RETURN, also support on-chain data storage [17], they were limited in both capacity and cost-efficiency. In contrast, inscriptions utilise the enhancements introduced by SegWit and Taproot, making them a more scalable and economically viable method for storing arbitrary data on Bitcoin.

4. Data and Methodology

4.1 Data

For our study, we source all data from the blockchain analytics platform Dune (dune.com) using custom SQL queries.

Our dataset spans July 2022 to March 2024 and contains more than 67 million inscriptions and 237 million Bitcoin transactions.

To analyse block-level dynamics and Taproot adoption, we collect data for over 355,000 Bitcoin blocks (August 2017 to March 2024) and more than 880 million transaction outputs (November 2021 to March 2024). In addition, we gather daily Bitcoin price data to contextualise market dynamics.

4.2 Inscription Identification and Classification

We identify inscription transactions by scanning the hexadecimal structure of Bitcoin transactions for the inscription envelope (“0063036f7264”). For transactions containing this envelope, we further classify inscriptions by detecting the hexadecimal representation of their MIME type, which indicates the file format of the inscription content. In practice, this involves detecting the patterns shown in Table 1.

Table 1. Hexadecimal Identifiers Used for Inscription Classification

Inscription Category	Hexadecimal Identifier
BRC-20	2270223a226272632d323022
Text	74657874
Image	696d616765
Application	6170706c6963617469666e
Video	766964656f
Audio	617564696f

To ensure accuracy, we validated our methodology in two ways: (i) by comparing our SQL queries against alternative approaches available on Dune and (ii) by manually inspecting a random sample of inscription transactions and their associated content using Ordinals explorers. Both checks confirmed the correctness and reliability of our classification procedure.

4.3 Descriptive Analytics Framework

For our descriptive analysis of Bitcoin's network dynamics (Section 5), we employ distinct observation windows to address different analytical needs. To analyse individual inscription patterns, we consider the period from the first inscription on 14 December 2022 (block 767,430) through 31 March 2024 (block 837,164). To examine inscription transaction patterns, we focus on the period from the launch of the Ordinals protocol on 20 January 2023 (block 772,739) through 31 March 2024. To assess broader structural shifts – such as changes in block size, blockspace utilisation, and Taproot adoption – we extend the observation window further back in time to capture pre-Ordinals dynamics. All dates are based on Coordinated Universal Time (UTC). We conclude our study period at the end of March 2024, which is prior to the Bitcoin halving and the launch of the Runes metaprotocol on 20 April 2024, to avoid potential confounding effects from these events.

We classify any transaction containing at least one inscription as an “inscription transaction,” while all other transactions are classified as “regular transactions.” In some cases, transactions contain multiple inscriptions

(batch inscriptions). We split these batch inscriptions into their individual inscriptions and allocate transaction size, blockspace consumption, and transaction fees proportionally across all inscriptions included in the batch. Although this approach may introduce some imprecision, particularly for batch inscriptions containing inscriptions of different categories, it provides a practical and consistent framework for category-level analysis.

To capture inscription activity and its direct impact on the Bitcoin network, we define three primary inscription-specific metrics:

- **Transaction Share:** The proportion of all Bitcoin transactions that contain at least one inscription.
- **Blockspace Share:** The share of blockspace consumed by inscription transactions.
- **Fee Share:** The proportion of total transaction fees paid by inscription transactions.

To assess broader network dynamics potentially influenced by inscriptions, we analyse three additional metrics:

- **Blockspace Utilisation:** The share of available blockspace that is consumed by all transactions.
- **Block Size:** The size of Bitcoin blocks measured in megabytes (MB).
- **Taproot Utilisation:** The share of Taproot transaction outputs.

All metrics are aggregated at the daily level.

4.4 Regression Methodology

To formally assess the impact of inscriptions on Bitcoin's network dynamics, we complement our descriptive analysis with regression models. The regression analysis covers the period from 1 July 2022 to 31 March 2024. This window allows us to capture both the pre-Ordinals baseline and the post-launch adoption phase, while avoiding potential confounding effects from events outside this window.

We employ ordinary least squares (OLS) regressions with heteroskedasticity- and autocorrelation-robust (HAC) standard errors to account for serial correlation in daily blockchain data. To improve model fit and interpretability, variables exhibiting strong skewness were log-transformed (natural logarithm) prior to estimation.

The general regression specification is given by:

$$Y_t = \alpha + \sum_{i=1}^k \beta_i X_{i,t} + \epsilon_t$$

where Y_t denotes the dependent variable, α the constant, β_i the coefficient estimates of the independent variables, $X_{i,t}$ the independent variables, and ϵ_t the error term.

The selection of dependent variables is motivated by the analysis in Section 5, where we identify inscription-related shifts in transaction activity, Taproot adoption, blockspace dynamics, and transaction fees. From these findings, we derive hypotheses that are tested econometrically in Section 6. The dependent variables include:

- Total Transactions (log)
- Regular Transactions (log)
- Taproot Utilisation (%)
- Average Block Size (MB)
- Blockspace Utilisation (%)
- Inscription Transaction Share (%)
- Total Transaction Fees (log)
- Regular Transaction Fees (log)

The independent variables are chosen to capture the impact of inscriptions and to control for price dynamics, which may also influence the dependent variables. These include:

- Inscription Transaction Share (%)
- Inscription Blockspace Share (%)
- Daily Bitcoin Log Returns
- 7-Day Price Volatility of Bitcoin
- 7-Day Price Volatility of Bitcoin

We use inscription-related metrics in relative terms (share values) rather than absolute values to account for the unique characteristics of inscriptions and to better capture their impact on overall network dynamics. For instance, a single inscription transaction may fill almost an entire block, which is clearly reflected in the share value but less so in absolute terms. We include daily Bitcoin log returns to control for short-term price fluctuations and 7-day price volatility to control for the effect of short- to medium-term market uncertainty on on-chain activity. Price volatility is calculated as 7-day standard deviation of daily log returns.

Table 2. Summary Statistics for Variables Used in Regression Analysis (Daily data, 1 July 2022 – 31 March 2024)

Variable	Observations	Mean	Std. Dev.	Min	Median	Max
Total Transactions (log)	640	12.773	0.315	12.142	12.710	13.503
Regular Transactions (log)	640	12.499	0.145	11.885	12.500	13.185
Taproot Utilisation (%)	640	17.80	16.78	0.14	13.93	65.24
Average Block Size (MB)	640	1.563	0.312	0.825	1.654	2.518
Blockspace Utilisation (%)	640	92.31	11.83	54.58	99.20	99.85
Total Transaction Fees (log)	640	3.418	0.878	1.780	3.196	6.454
Regular Transaction Fees (log)	640	3.304	0.788	1.780	3.133	5.934
Inscription Transaction Share (%)	640	20.38	21.67	0.00	12.60	75.50
Inscription Blockspace Share (%)	640	15.22	13.61	0.00	15.85	55.26
Daily Bitcoin Log Returns	640	0.002	0.021	−0.110	0.001	0.107
7-Day Price Volatility	640	0.017	0.009	0.003	0.016	0.061

All variables used in the regression analysis are calculated at the daily level for our 640-day observation period. The summary statistics for these variables are reported in Table 2.

5. Exploration of Bitcoin's Network Dynamics

5.1 Composition and Evolution of Inscriptions

Between December 2022 and March 2024, 67.3 million inscriptions were recorded on the Bitcoin blockchain. As shown in Table 3, BRC-20 inscriptions were the dominant category, accounting for 77.7% of all inscriptions, followed by text (16.2%) and image (3.5%) inscriptions.

As illustrated in Figure 1, early inscription activity following the launch of the Ordinals protocol in January 2023 was primarily driven by text and image inscriptions. This pattern changed significantly with the introduction of the BRC-20 token standard in March 2023, which triggered the first major wave of inscription activity in the following months. Inscription volume surged until late September, with BRC-20 accounting for the vast majority of inscriptions. Overall, the evolution of inscriptions shows a dynamic and rapidly shifting ecosystem. The data in Figure 1 indicate that the timing of inscription waves appears to be more closely linked to protocol innovations – such as the introduction of BRC-20 – than to Bitcoin price fluctuations. This motivates our first hypothesis:

H1: Short-term Bitcoin price dynamics have only a limited direct influence on inscription activity.

Table 3. Inscriptions per Category

Inscription Category	Count	Share (%)
BRC-20	52,287,206	77.68
Text	10,929,318	16.24
Image	2,358,488	3.50
Other	956,205	1.42
Application	699,332	1.04
Video	78,316	0.12
Audio	1,299	0.00
Total	67,310,164	100.00

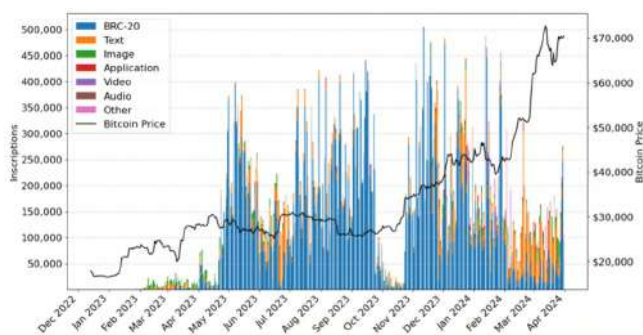


Figure 1. Inscriptions and Bitcoin Price.

5.2 Transaction Analysis

5.2.1 Transaction Dynamics

To assess the impact of inscriptions on Bitcoin's on-chain activity, we examine the transaction share of inscription transactions and analyse how this metric interacts with overall network activity. As shown in Table 4, Bitcoin recorded nearly 64 million inscription transactions between 20 January 2023 and 31 March 2024, representing 34.6% of all transactions during this period. Figure 2 shows that the number of regular transactions remained relatively stable, implying that inscription transactions added to overall network activity rather than replacing existing transaction flows.

As shown in Panel A of Table 5, BRC-20 inscriptions accounted for the vast majority of inscription transactions, followed by text and image inscriptions.

Table 4. Transactions Distribution

Transaction Type	Count	Transaction Share (%)
Regular Transactions	121,121,535	65.44
Inscription Transactions	63,959,185	34.56
Total	185,080,720	100.00

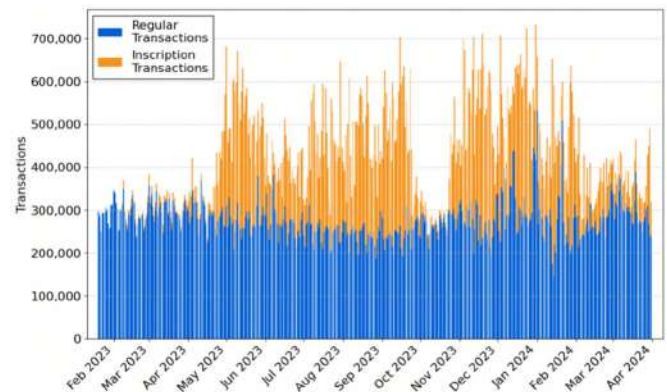


Figure 2. Transactions Distribution.

Figures 1, 2, and 3 indicate that inscription transaction volumes closely mirrored the number of individual inscriptions created. Since each inscription must be recorded in a transaction, the number of new inscriptions directly drives inscription-related transaction volume. The fact that there is no perfect correlation between these two metrics can be attributed to batch inscriptions, which allow multiple inscriptions to be created in a single transaction. As shown in Table 6, approximately 3.7 million inscriptions were created in 344,287 batch inscriptions, reducing inscription-related transaction volume by approximately 3.36 million and explaining the imperfect correlation between the number of individual inscriptions and inscription transactions.

Table 5. Main Metrics per Inscription Category
Panel A: Share Relative to All Inscription Transactions

Inscription Category	Transaction Share (%)	Blockspace Share (%)	Fee Share (%)
BRC-20	81.54	56.70	73.47
Text	13.46	15.78	13.86
Image	3.05	24.90	8.84
Other	1.95	2.62	3.83
All Insc. Transactions	100.00	100.00	100.00

Panel B: Share Relative to All Bitcoin Transactions

Inscription Category	Transaction Share (%)	Blockspace Share (%)	Fee Share (%)
BRC-20	28.18	12.86	16.24
Text	4.65	3.58	3.06
Image	1.05	5.65	1.95
Other	0.67	0.59	0.85
All Insc. Transactions	34.56	22.68	22.10

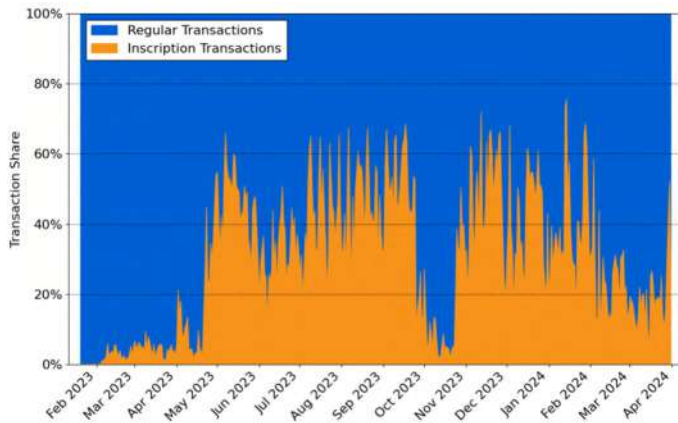


Figure 3. Transaction Share.

The transaction share metric highlights that inscriptions introduced a novel use case that significantly increased on-chain activity on Bitcoin's base layer. At the same time, regular transaction volume remained largely unaffected. Taken together, these findings motivate the following hypotheses:

H2.1: Higher levels of inscription activity are associated with an increase in the total number of Bitcoin transactions.

H2.2: Higher levels of inscription activity are not associated with a substantial reduction in the number of regular transactions.

Table 6. Batch Inscriptions

Batch Size	Batch Inscriptions	Share (%)
≥ 10,000	6	0.00
5,000–9,999	1	0.00
1,000–4,999	776	0.23
500–999	714	0.21
100–499	4,934	1.43
50–99	4,114	1.19
10–49	24,451	7.10
3–9	35,185	10.22
2	274,106	79.62
Total	344,287	100.00

5.2.2 Taproot Utilisation

As outlined in Section 3.2, the creation of an inscription requires the generation of a Taproot output. This link between Taproot outputs and inscriptions motivates us to investigate whether the rise in inscription transactions corresponded with an increase in Taproot utilisation. We define Taproot utilisation as the share of Taproot outputs relative to all transaction outputs.

Figures 4 and 5 show that prior to 2023, Taproot use was minimal. Following the launch of the Ordinals protocol, both the number of Taproot outputs and Taproot utilisation increased sharply. We can further observe that Taproot utilisation exhibited a strong co-movement with the share of inscription transactions. This pattern suggests that Taproot adoption was driven less by general demand for its technical features and more by the emergence of inscriptions as a new use case that is dependent on this protocol upgrade. We thus derive the following hypothesis:

H3: Higher levels of inscription activity are associated with increased Taproot utilisation.

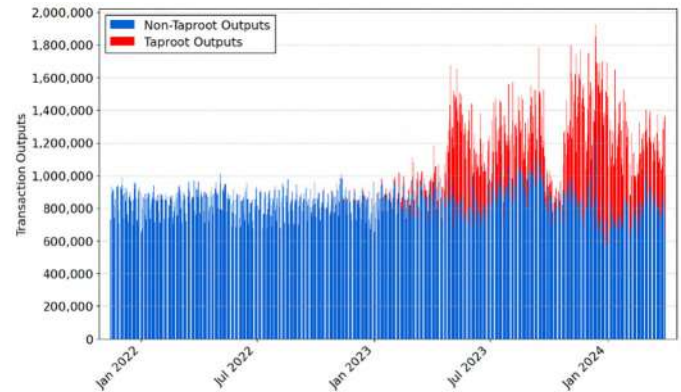


Figure 4. Transaction Outputs Distribution.

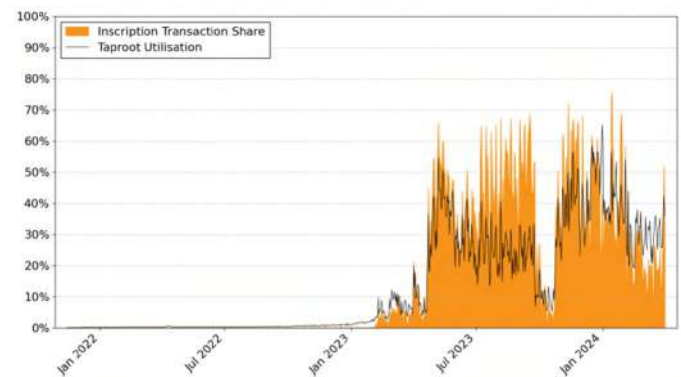


Figure 5. Inscription Transaction Share and Taproot Utilisation.

5.3 Blockspace Analysis

5.3.1 Blockspace Dynamics

Bitcoin's base layer operates under a strict block size limit, which caps the amount of data and thus the number of transactions that can be included in each block. As a result, transactions compete for limited blockspace. The emergence of inscriptions intensified this competition. We use the blockspace share metric to assess the impact of inscriptions on one of the network's most constrained resources.

Panel B of Table 5 shows that between January 2023 and March 2024, inscription transactions consumed 22.7% of the network's total blockspace, which is notably lower than their 34.6% share of total transactions. Figures 3 and 6 illustrate that this divergence between transaction share and blockspace share persisted throughout the sample period. This can be explained by the variability in size and frequency of transactions across different inscription categories. As shown in Panel A of Table 5, BRC-20 and text inscriptions, which together comprised 95% of inscription transactions, accounted for only 72.5% of inscription-related blockspace consumption. By contrast, image inscriptions represented just 3% of inscription transactions but consumed nearly 25% of inscription-related blockspace. Transaction size data in Table 7 corroborates this pattern. On average, BRC-20 and text transactions were 61% and 49% smaller than regular transactions, respectively, while image inscription transactions were 276% larger. This dynamic underscores that blockspace consumption is shaped not only by aggregate inscription volume but also by the characteristics and composition of inscription categories.

5.3.2 Blockspace Utilisation and Block Size

The analysis of blockspace dynamics associated with inscriptions reveals two additional insights. First, the rise of inscriptions had a substantial impact on blockspace utilisation. Figure 7 shows that as the blockspace

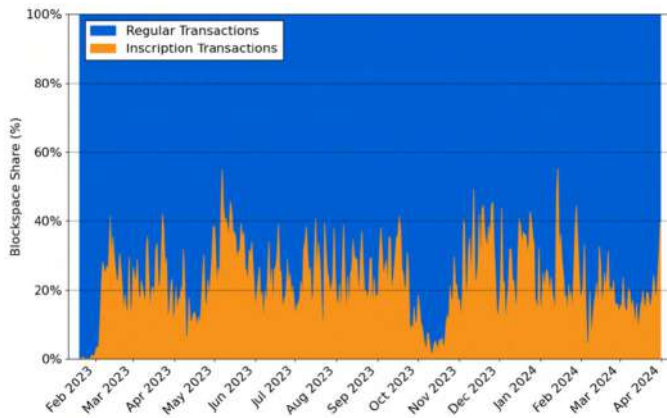


Figure 6. Blockspace Share.

Table 7. Transaction Size Comparison

Transaction Type	Size (virtual bytes)		Delta to Regular (%)	
	Median	Avg.	Median	Avg.
Regular	163	406	–	–
BRC-20	143	157	–12	–61
Text	147	208	–10	–49
Image	328	1,525	+101	+276
Other	155	218	–5	–46

share of inscriptions rose in February 2023, Bitcoin blocks began to reach full capacity more frequently, and overall blockspace utilisation increased. With the first major wave of BRC-20 inscriptions in April 2023, the network entered the longest sustained period of persistently high blockspace utilisation in Bitcoin's history. Prior to 2023, such periods typically lasted only for a few months. These dynamics suggest an association between inscription activity and the degree to which available blockspace is utilised. Accordingly, we derive the following hypothesis:

H4: Higher inscription blockspace shares are associated with higher levels of blockspace utilisation.

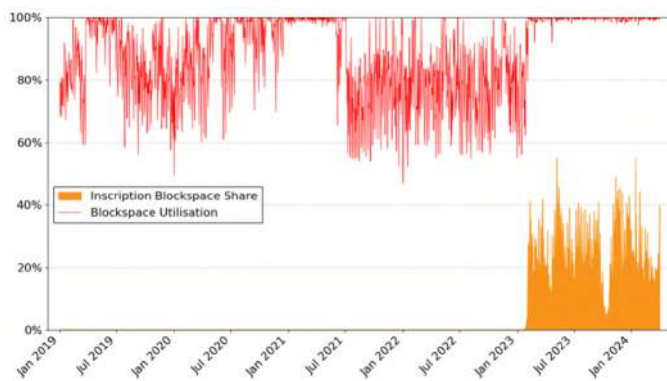


Figure 7. Inscription Blockspace Share and Blockspace Utilisation.

The second notable observation concerns block size. As shown in Figure 8, the average daily block size remained relatively stable after the SegWit upgrade, even though this upgrade enabled individual blocks to reach a capacity of up to 4 MB. Following the launch of the Ordinals protocol,

average block size rose sharply, frequently exceeding 2 MB during the early phase of inscriptions. Throughout the remainder of the sample period, the daily average block size remained at an elevated level.

To further assess the impact of inscriptions, we compare block size metrics between two equally long 437-day periods before and after the launch of the Ordinals protocol. Table 8 shows that the average block size increased from 1.18 MB to 1.74 MB, a 47% rise, while the median increased by 20%. Stripped block size – which excludes witness data and therefore inscription content – experienced only modest changes over the same period. In fact, the median value decreased slightly. This suggests that the observed growth in block size was largely attributable to witness data, which is also driven by inscriptions. Based on these findings, we formulate the following hypothesis:

H5: Higher inscription blockspace shares are associated with an increase in the average size of Bitcoin blocks.

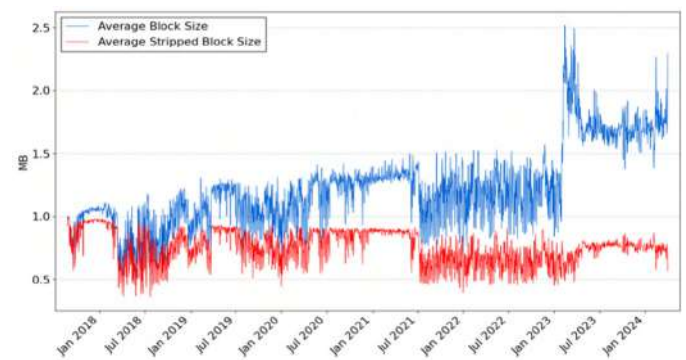


Figure 8. Block Size Comparison.

Table 8. Bitcoin Block Size Changes

	Pre-Ordinals (MB)	Post-Ordinals (MB)	Change (%)
Average Size	1.182	1.737	+47
Median Size	1.394	1.673	+20
Average Stripped Size	0.648	0.737	+14
Median Stripped Size	0.794	0.770	–3

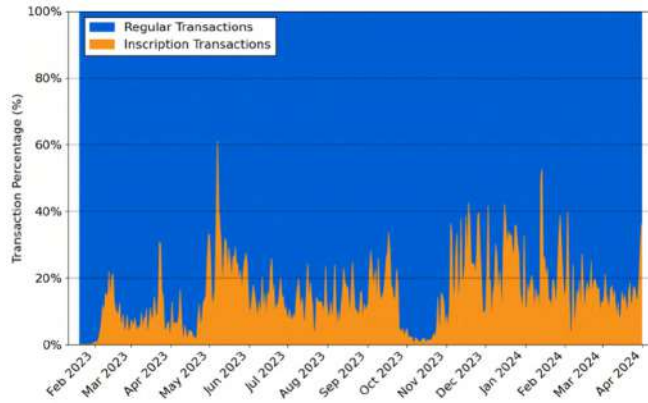
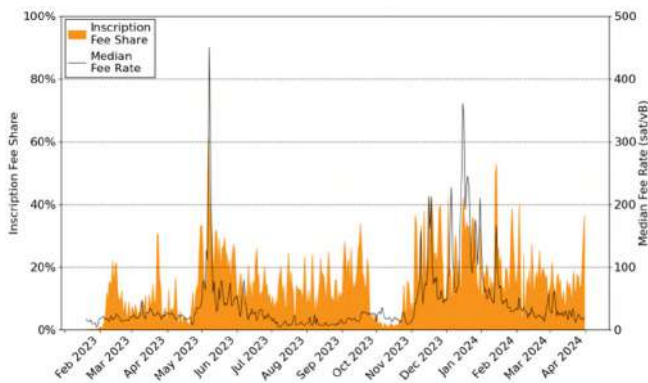
5.4 Fee Analysis

Bitcoin's fee market allocates blockspace through a competitive bidding process, with miners prioritising transactions based on their fee rates, expressed in satoshis per virtual byte (sat/vB). Given our findings about inscription activity in Sections 5.2 and 5.3, it is relevant to assess how inscriptions affected fee market dynamics.

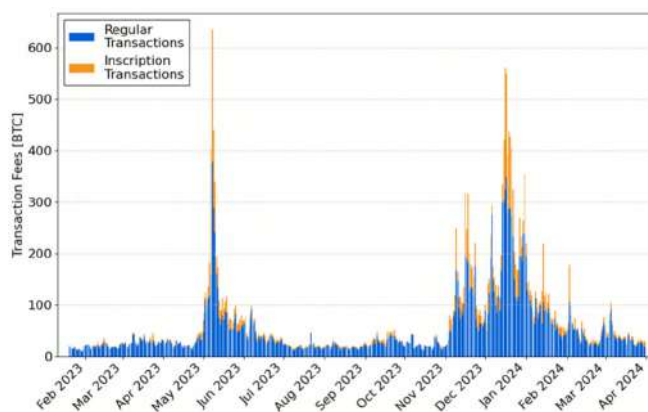
As shown in Table 9, total transaction fees on the Bitcoin network amounted to 29,060 Bitcoin between January 2023 and March 2024, of which inscription transactions contributed 6,423 Bitcoin, or 22.1%. This value is lower than their 22.7% blockspace share, indicating that inscription transactions, on average, paid slightly lower fees per unit of blockspace than regular transactions. This pattern also holds over time. As illustrated in Figures 6 and 9, the fee share of inscriptions generally mirrored their blockspace share throughout the sample period, albeit at a lower magnitude. The near parity between inscriptions' total fee share and blockspace share can be explained by inscriptions contributing disproportionately more fees during periods of heightened network fee rates (Figures 10 and 11).

Table 9. Transaction Fees Distribution

Transaction Type	Fees (BTC)	Share (%)
Regular TXs	22,637	77.90
Inscription TXs	6,423	22.10
Total	29,060	100.00

**Figure 9.** Transaction Fee Share.**Figure 10.** Transaction Fee Share and Median Fee Rate.

At the category level, Panel A of Table 5 shows that BRC-20 inscriptions were the only major category whose fee share (73.5%) exceeded their blockspace share (56.7%). In contrast, image inscriptions accounted for 24.9% of blockspace consumed by inscriptions but contributed only 8.8% of transaction fees paid by inscriptions. Consistent with this observation, Table 10 shows that image inscription transactions exhibited the lowest fee rate of all categories. It also shows that inscription transactions, on average, paid a lower fee rate than regular transactions. These findings are consistent with the results of Bertucci [2].

**Figure 11.** Transaction Fees Distribution.**Table 10.** Transaction Fee Rates

Transaction Type	Median Fee Rate(sat/vB)
All Transactions	27.51
Regular	28.98
All Inscriptions	23.92
BRC-20	22.68
Text	24.91
Image	20.57
Other	45.91

Bitcoin's fee market dynamics reflect the interplay between on-chain activity, blockspace scarcity, and user bidding behaviour. Although inscriptions paid, on average, lower fees per unit of blockspace than regular transactions, they created additional network activity and increased competition for limited blockspace. These dynamics suggest that inscriptions may have contributed to higher total fee revenue and may have also influenced regular transactions to bid more aggressively for block inclusion. We therefore derive the following hypotheses:

H6.1: Higher inscription blockspace shares are associated with an increase in total transaction fees.

H6.2: Higher inscription blockspace shares are associated with an increase in regular transaction fees.

While fee rates represent an important dimension of Bitcoin's network dynamics, we do not econometrically assess them in our study, as this topic requires a dedicated analysis beyond the scope of this paper (see [2] for a detailed assessment).

6. Impact of Inscriptions on Bitcoin's Network Dynamics

Building on the descriptive evidence in Section 5, we now turn to a formal econometric analysis of how inscriptions have affected Bitcoin's network dynamics. We use OLS regression analysis to quantify this effect and test the hypotheses derived in the previous section, using inscription-related metrics as the key explanatory variables (except for H1) while controlling for Bitcoin price dynamics. The regression results are summarised in Table 11.

H1: Short-term Bitcoin price dynamics have only a limited direct influence on inscription activity.

The regression results show that daily log returns are statistically insignificant, while 7-day price volatility has a negative and significant effect. This suggests that higher volatility may dampen inscription activity, whereas short-term price changes exert no measurable influence. However, the explanatory power of the model is very low, indicating that price dynamics explain only a small fraction of variation in inscription activity. Broader market cycles, however, may still affect inscription activity.

H2.1: Higher levels of inscription activity are associated with an increase in the total number of Bitcoin transactions.

The regression for total transactions shows a strong and highly significant positive association between the share of inscription transactions and overall transaction volume on Bitcoin, with the model explaining a substantial share of the variation. The results indicate that a 1 percentage point increase in the inscription transaction share is associated with a 1.3% increase in total transactions, confirming our assumption that inscriptions add additional on-chain activity.

Daily log returns also enter positively and significantly, suggesting that short-term price changes stimulate higher transaction activity, for instance, when users adjust their Bitcoin holdings in response to price swings. In contrast, 7-day price volatility remains statistically insignificant. Therefore, both inscription activity and short-term price changes contribute to transaction growth.

H2.2: Higher levels of inscription activity are not associated with a substantial reduction in the number of regular transactions.

The regression for regular transactions indicates a small but statistically significant negative effect of inscription activity, suggesting that a 1 percentage point increase in the inscription transaction share is associated with a 0.1% decline in regular transactions. Log returns again enter positively and significantly, consistent with the assumption that price movements spur regular transaction volume, while 7-day volatility remains insignificant.

Although the results suggest a limited substitution effect, we interpret this with caution. Our findings from H2.1 indicate that the net effect of inscription activity is positive for overall transaction volume. Given the limited explanatory power of the model used to test H2.2, we regard the substitution effect as modest in magnitude and insufficient to offset the broader increase in network activity.

H3: Higher levels of inscription activity are associated with increased Taproot utilisation.

The regression results support our hypothesis. The share of inscription transactions is positively and significantly associated with Taproot utilisation. An increase of 1 percentage point in the share of inscription transactions corresponds to a 0.69 percentage point increase in Taproot utilisation. The fact that the effect is smaller than unity most likely reflects that not all inscription transactions consist exclusively of Taproot outputs and that Taproot is not exclusively used for inscriptions. Given the high explanatory power of our model and the lack of significant effects from price dynamics, the evidence suggests that the adoption and utilisation of Taproot is largely associated with inscription activity.

H4: Higher inscription blockspace shares are associated with higher levels

of blockspace utilisation.

The regression results support our hypothesis. The coefficient estimate of the inscription blockspace share is positive and highly significant. An increase of 1 percentage point in the share of blockspace consumed by inscriptions is associated with a 0.58 percentage point increase in overall blockspace utilisation. This indicates that inscriptions substantially contributed to Bitcoin blocks becoming fuller.

A possible explanation for this effect lies in the heterogeneity of transaction sizes across inscription categories. As shown in Tables 5 and 7, BRC-20 and text inscriptions are considerably smaller than image inscriptions but occur in much higher numbers. A few large image inscriptions can easily consume the space of an entire block, whereas the smaller yet more numerous BRC-20 and text inscriptions can also drive blockspace consumption and efficiently fill residual space when blocks are nearly full. In both cases, the outcome is similar: inscriptions create additional demand for blockspace and thereby contribute to higher blockspace utilisation.

Log returns also exhibit a positive and significant effect, consistent with the notion that short-term price changes may stimulate transaction activity and thereby increase demand for blockspace. By contrast, price volatility shows no discernible impact. With an adjusted R-squared value of 0.46, the model accounts for a considerable share of variation in blockspace utilisation, though substantial unexplained dynamics remain.

H5: Higher inscription blockspace shares are associated with an increase in the average size of Bitcoin blocks.

The results provide evidence consistent with our hypothesis. The coefficient estimate of the inscription blockspace share is positive and highly significant. An increase of 1 percentage point in the share of blockspace consumed by inscription transactions corresponds to an increase in the average block size of approximately 0.017 MB. While this absolute value may appear modest, its cumulative effect is substantial given the block size limit of 4 MB. These regression results are consistent with our findings in Section 5.3, which show that the average block size rose sharply after the launch of the Ordinals protocol.

Because inscriptions store their content in the witness part of transactions,

Table 11. OLS Regression Results (1 July 2022 – 31 March 2024)

	(1) H1 Inscription Transaction Share (%)	(2) H2.1 Total Transactions (log)	(3) H2.2 Regular Transactions (log)	(4) H3 Taproot Utilisation (%)	(5) H4 Blockspace Utilisation (%)	(6) H5 Average Block Size (MB)	(7) H6.1 Total Transaction Fees (log)	(8) H6.2 Regular Transaction Fees (log)
Inscription Transaction Share (%)		0.013*** (0.000)	−0.001*** (0.000)	0.69*** (0.04)				
Inscription Blockspace Share (%)					0.58*** (0.05)	0.017*** (0.002)	4.071*** (0.476)	3.200*** (0.446)
Daily Bitcoin Log Returns	−5.20 (37.88)	0.742*** (0.243)	0.845*** (0.266)	20.01 (15.53)	40.75** (17.11)	0.887** (0.395)	1.984 (1.329)	2.034 (1.262)
7-Day Price Volatility	−568.82*** (159.85)	1.072 (0.763)	0.658 (0.914)	73.59 (60.30)	−57.45 (56.56)	2.045 (1.760)	2.646 (4.645)	2.506 (4.309)
Observations	640	640	640	640	640	640	640	640
Adjusted R-Squared	0.059	0.839	0.051	0.779	0.457	0.564	0.394	0.302

Note: Standard errors in parentheses. The significance levels are: *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

they can individually or collectively add substantial amounts of data, sometimes inflating block size to nearly 4 MB. Evidence from Table 8 also indicates that the increase in block size between the pre- and post-Ordinals periods was primarily driven by witness data. Although our model leaves a considerable share of variation unexplained, the combined evidence from our regression and descriptive analysis suggests that inscriptions were a major factor associated with the observed growth in block size.

H6.1: Higher inscription blockspace shares are associated with an increase in total transaction fees.

The results support our hypothesis. The coefficient estimate of the inscription blockspace share is positive and highly significant, indicating that a 1 percentage point increase in the inscription blockspace share is associated with roughly a 4% increase in total transaction fees. This suggests that inscriptions, by competing for scarce blockspace, contributed to higher fee revenue. By contrast, log returns and price volatility show no significant effects. However, our model only explains a moderate share of total fee revenue variation.

H6.2: Higher inscription blockspace shares are associated with an increase in regular transaction fees.

The coefficient estimate of the inscription blockspace share is positive and highly significant, implying that a 1 percentage point increase in the inscription blockspace share corresponds to approximately a 3.2% increase in regular transaction fees. This indicates that inscriptions, while paying lower average fee rates themselves, raised competitive pressure on regular transactions, pushing their fees higher. Price dynamics remain statistically insignificant. Although this model also only has moderate explanatory power, the results are consistent with our hypothesis that inscriptions increase fee pressure on regular transactions.

7. Discussion

7.1 Broader Debates on Inscriptions

The impact of inscriptions on Bitcoin has been highly controversial, with critics warning of negative externalities and proponents emphasising potential benefits.

Critics argue that inscriptions contribute to network congestion and fee spikes, thereby reducing usability for regular payment transactions. Some even dismiss inscriptions as “spam” that exploits protocol features and undermines Bitcoin’s original role as a peer-to-peer financial network [18].

By contrast, proponents argue that additional transaction volume from inscriptions increases miner revenue and thus strengthens the network’s long-term security budget. They also emphasise that inscriptions introduced new use cases and spurred further innovation within the Bitcoin ecosystem. Proponents further highlight that inscriptions operate within Bitcoin’s consensus rules and therefore did not alter the protocol’s fundamental design [19].

7.2 Research Limitations and Future Research

Our study offers relevant perspectives on the impact of inscriptions on the Bitcoin network, yet it is not without limitations. By focusing on a period when inscriptions were the only significant metaprotocol-based asset on Bitcoin, we are able to isolate their effects more clearly. However, as Bitcoin’s ecosystem continues to evolve, future research should explore how multiple metaprotocols and other emerging technologies interact and collectively influence Bitcoin’s network dynamics.

Our regression analysis relies on daily data. While this level of granularity is sufficient for our purposes, block-level data could provide additional insights and help assess the robustness of our results.

Finally, our regression analysis focuses on the impact of inscriptions at the

aggregate level. Future research could investigate the effects of individual inscription categories in greater detail.

8. Conclusion

Bitcoin inscriptions facilitate the on-chain storage of arbitrary data on the Bitcoin blockchain. This capability has unlocked new use cases within the Bitcoin ecosystem. In this study, we analysed the impact of inscriptions on Bitcoin’s network dynamics across multiple dimensions. Our results show that inscriptions increased on-chain activity, intensified competition for blockspace, and influenced Bitcoin’s fee market dynamics. We also find that the rise of inscriptions coincided with an increased utilisation of Taproot, an increase in average block size, and the longest sustained period of high blockspace utilisation in Bitcoin’s history. Overall, these findings demonstrate that inscriptions have reshaped how the Bitcoin blockchain is used and underscore the growing diversification of its applications beyond its role as a peer-to-peer financial network.

References

- [1] M. Rosenfeld, et al., “Overview of colored coins,” *White Paper*, bitcoincolors.com, vol. 41, p. 94, 2012.
- [2] L. Bertucci, “Bitcoin ordinals: Determinants and impact on total transaction fees,” *Research in International Business and Finance*, vol. 70, p. 102338, 2024, <https://doi.org/10.1016/j.ribaf.2024.102338>.
- [3] N. Li, M. Qi, Q. Wang, and S. Chen, “Bitcoin inscriptions: Foundations and beyond, 2024,” *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2024, pp. 1–5, <https://doi.org/10.1109/ICBC59979.2024.10634475>.
- [4] G. Liao, T. Wang, Q. Yang, Y. Xia, L. Shi, X. Zhao, X. Wu, S. Zhang, A. Chan, and R. Yuen, “Programming on bitcoin: A survey of layer 1 and layer 2 technologies in bitcoin ecosystem,” 2024, <https://doi.org/10.48550/arXiv.2409.19622>.
- [5] Z. Zhu, Z. Guo, X. Ma, and K. Yin, “Research on bitcoin inscriptions risk monitoring,” 2024 2nd International Conference on Big Data and Privacy Computing (BDPC), 2024, pp. 200–205, <https://doi.org/10.1109/BDPC59998.2024.10649295>.
- [6] Q. Wang, G. Yu, and S. Chen, “Understanding BRC-20: Hope or hype,” *IEEE Transactions on Computational Social Systems*, 2025, <https://doi.org/10.1109/TCSS.2025.3577174>.
- [7] M. Qi, Q. Wang, Z. Wang, L. Zhong, T. Zhu, S. Chen, and W. Knottenbelt, “BRC20 pinning attack,” 2024, <https://doi.org/10.48550/arXiv.2410.11295>.
- [8] J. Messias, K. Gogol, M. I. Silva, and B. Livshits, “The writing is on the wall: Analyzing the boom of inscriptions and its impact on EVM-compatible blockchains,” 2025, <https://doi.org/10.48550/arXiv.2405.15288>.
- [9] Q. Wang, G. Yu, and S. Chen, “Bridging BRC-20 to ethereum,” 2024 *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2024, pp. 264–272, <https://doi.org/10.1109/ICBC59979.2024.10634341>.
- [10] C. Rodarmor and J. Ruffing, *Ordinal Theory Handbook*. 2022. Accessed: Dec. 5, 2024. [Online]. Available: <https://docs.ordinals.com/>.
- [11] L. Balduf, M. Florian, and B. Scheuermann, “Dude, where’s my NFT: Distributed infrastructures for digital art,” *Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good*, 2022, pp. 1–6, <https://doi.org/10.1145/3565383.3566106>.
- [12] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, “Understanding security issues in the NFT ecosystem,” *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 667–681, <https://doi.org/10.1145/3548606.3559342>.
- [13] P. Wuille, E. Lombrozo, and J. Lau, BIP 141: Segregated Witness (Consensus Layer). 2015. Accessed: Dec. 5, 2024, [Online]. Available: <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>.
- [14] P. Wuille, J. Nick, and T. Ruffing, BIP 340: Schnorr Signatures for secp256k1. 2020. Accessed Dec. 5, 2024, [Online]. Available: <https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki>.
- [15] P. Wuille, J. Nick, and A. Towns, BIP 341: Taproot - SegWit Version 1 Spending Rules. 2020. Accessed Dec. 5, 2024, [Online]. Available: <https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki>.

github.com/bitcoin/bips/blob/master/bip-0341.mediawiki.

[16] P. Wuille, J. Nick, and A. Towns, BIP 342: Validation of Taproot Scripts. 2020. Accessed Dec. 5, 2024. [Online]. Available: <https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki>.

[17] E. Strehle and F. Steinmetz, "Dominating OP returns: The impact of omni and veriblock on bitcoin," *Journal of Grid Computing*, vol. 18, no. 4, pp. 575–592, 2020, <https://doi.org/10.1007/s10723-020-09537-9>.

[18] J. Nelson, Rising Bitcoin Fees Prompt Renewed Battle Over Ordinals, BRC-20 Tokens. Decrypt. 2023. Accessed: Aug. 15, 2025. [Online]. Available: [https://decrypt.co/208945/](https://decrypt.co/208945/rising-bitcoin-fees-prompt-renewed-battle-over-ordinals-brc-20-tokens)

[rising-bitcoin-fees-prompt-renewed-battle-over-ordinals-brc-20-tokens](https://decrypt.co/208945/rising-bitcoin-fees-prompt-renewed-battle-over-ordinals-brc-20-tokens).

[19] M. Castrovilli, "How the ordinals movement will benefit the bitcoin blockchain," *Cointelegraph*, 2023. Accessed: Aug. 15, 2025. [Online]. Available: [https://cointelegraph.com/](https://cointelegraph.com/news/how-the-ordinals-movement-will-benefit-the-bitcoin-blockchain)

[news/how-the-ordinals-movement-will-benefit-the-bitcoin-blockchain](https://cointelegraph.com/news/how-the-ordinals-movement-will-benefit-the-bitcoin-blockchain)

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

Alexander Wiedenmann: Conceptualization, Data curation, Formal analysis, Methodology, Visualization, Writing – original draft & editing

Andre Guettler: Conceptualization, Supervision, Writing – review & editing.

Funding:

None declared.

Acknowledgements:

None.

PEER-REVIEWED RESEARCH

OPEN ACCESS

ISSN Print: 2516-3949

[https://doi.org/10.31585/jbba-8-2-\(7\)2025](https://doi.org/10.31585/jbba-8-2-(7)2025)

Rate Discovery in Decentralised Lending

Charlotte Eli, Hervé Alexandre

Université Paris Dauphine-PSL, Dauphine Fintech Chair, France

Correspondence: charlotte.eli@dauphine.psl.eu and herve.alexandre@dauphine.psl.eu**Received:** 27 December 2024 **Accepted:** 29 May 2025 **Published:** 6 November 2025

Abstract

This paper introduces a novel framework for rate discovery in decentralised finance (DeFi), focusing on the unique challenges and opportunities within decentralised lending platforms. We explore the mechanisms of interest rate formation in a decentralised environment, without traditional banking institutions' control. By leveraging lending pool dynamics, we propose a method that integrates borrowers' risk profiles with market liquidity conditions to determine fair borrowing rates without third-party involvement. Our model aims to offer a transparent and reliable solution for rate discovery in DeFi. Through a series of simulations, we demonstrate the potential of our framework to improve lending practices in the DeFi ecosystem, making it a viable and competitive alternative to conventional financial systems. The findings suggest that our approach not only enhances the transparency and fairness of the lending process but also encourages a more informed participation of lenders and borrowers, ultimately contributing to the stability and growth of the DeFi market.

Keywords: *Lending, Blockchain, DeFi, Interest Rate***JEL Classifications:** *G20, G23*

List of Symbols

Symbol	Description
R_0	Minimum interest rate (base rate)
R_{slope1}	Interest rate slope below optimal utilisation
R_{slope2}	Interest rate slope above optimal utilisation
U	Utilisation rate
$U_{optimal}$	Optimal utilisation rate
R_t	Borrowing rate at time t
r^*	True value borrowing rate (market rate)
r_i	Tick-specific borrowing rate
ROI	Borrower's maximum acceptable borrowing rate
K	Target loan amount
$D_{LPB,\tau}$	Total deposit amount (TVL) in borrower's lending pool
CD_{r_i}	Cumulative deposit volume up to tick r_i
RR	Recovery rate upon default
$p_{d,k}$	Borrower's default probability assessed by lender k

1. Introduction

The determination of interest rates in financial markets is a process influenced by a variety of factors, ranging from individual creditworthiness to broader macroeconomic conditions. Traditional financial systems have long relied on intermediaries, such as banks, to assess borrower risk and set interest rates accordingly. However, this reliance on centralised institutions introduces challenges related to information asymmetry [1, 2], where lenders possess less information than borrowers, leading to potential inefficiencies and inequities in lending practices.

Decentralised finance (DeFi) represents a significant departure from traditional financial systems, offering a decentralised approach to lending that eliminates the need for trusted third-party intermediaries. By leveraging blockchain technology, DeFi platforms enable peer-to-peer transactions and lending agreements, thereby democratising access to financial services. However, the decentralised nature of DeFi also introduces unique challenges, particularly in determining fair and transparent borrowing rates in the absence of centralised control.

This paper aims to address these challenges by proposing a theoretical framework for interest rate discovery within the DeFi ecosystem. Our approach builds upon existing literature on credit rationing, information asymmetry, and auction theory, extending these concepts to the decentralised context. By examining the dynamics of lending pools and integrating borrowers' risk profiles with market liquidity conditions, we seek to develop a model that facilitates equitable rate determination without intermediary involvement.

Central to our framework is the concept of an auction mechanism, where lending rates are determined through a competitive bidding process among liquidity providers. This mechanism is designed to reflect the true market value of borrowing rates, taking into account both the borrower's risk profile and prevailing market conditions. Through a series of simulations, we explore the potential of our framework to enhance transparency and

fairness in DeFi lending practices.

The findings suggest that our model not only aligns incentives between lenders and borrowers but also fosters a more informed and stable lending environment. By encouraging the disclosure of financial information and leveraging market dynamics, our approach contributes to the theoretical discourse on financial decentralisation and offers insights into the potential of DeFi to provide reliable lending and borrowing options in a decentralised manner.

Moreover, this paper delves into the implications of our proposed framework for the broader financial ecosystem, examining its potential to address long-standing issues related to information asymmetry and credit rationing. By advancing our understanding of decentralised rate discovery mechanisms, we aim to contribute to the ongoing evolution of DeFi and its integration into the global financial landscape.

Interest Rate Model in DeFi

Lending protocols such as Aave, Compound, Maker DAO, and dYdX have established a robust foundation for the lending market in DeFi [3]. They enable cryptocurrency holders to earn interest on their assets in a permissionless manner, thereby democratising access to financial services.

A pivotal aspect of these protocols is the determination of borrowing rates, which is intricately linked to the concept of utilisation rate. The utilisation rate, denoted as U is a metric that quantifies the proportion of supplied assets that are currently borrowed within a lending pool. Mathematically, it is expressed as:

$$U = \frac{\text{Total Borrows}}{\text{Total Supplies}}$$

This rate serves as an indicator of the availability of capital within the pool, with higher utilisation rates signifying greater demand for borrowing relative to the supply of assets. The utilisation rate is fundamental in managing liquidity risk within the protocol, as it influences borrowing and lending behaviours through dynamic interest rate adjustments.

The interest rate model employed by these protocols is algorithmically designed to optimise capital utilisation and manage liquidity risk. Specifically, the borrowing interest rates are derived from the utilisation rate through a piecewise linear function. According to Aave's documentation, the interest rate model is defined as follows:

- if $U \leq U_{\text{optimal}}$, $R_t = R_0 + \frac{U_t}{U_{\text{optimal}}} R_{\text{slope1}}$
- if $U > U_{\text{optimal}}$, $R_t = R_0 + R_{\text{slope1}} + \frac{U_t - U_{\text{optimal}}}{1 - U_{\text{optimal}}} R_{\text{slope2}}$

where,

- R_0 is the minimum interest rate charged to borrowers when the utilisation rate is at its lowest. It represents the baseline cost of borrowing, irrespective of the demand for the asset. It is typically set to cover the basic operational costs and risks associated with lending.

- R_{slope1} , determines the rate of increase in the interest rate as the utilisation rate rises from 0% to the optimal utilisation rate. It reflects how sensitive the interest rate is to changes in utilisation within this range. A steeper slope indicates a more rapid increase in the interest rate as utilisation increases, incentivising borrowers to repay their loans or suppliers to provide more liquidity as demand rises.

- R_{slope2} governs the rate of increase in the interest rate when the utilisation rate exceeds the optimal utilisation rate. It is generally steeper than to

discourage high utilisation, which could lead to liquidity shortages. A higher ensures that as the pool becomes more utilised, the cost of borrowing increases significantly, encouraging repayments and additional supply to maintain liquidity.

The model parameters (R_0 , U_{optimal} , R_{slope1}) are asset dependent. The interest rate parameters of assets with lower liquidity levels are more conservative. Model's parameters can also be subject to change depending on market conditions.

By understanding and effectively managing the utilisation rate, DeFi protocols can incentivise behaviours that support liquidity and optimise capital allocation, thereby enhancing the overall functionality and reliability of the decentralised lending ecosystem.

The current landscape of decentralised finance (DeFi) lending is primarily focused on highly collateralised borrowing, where borrowers must provide collateral equal to or greater than the borrowed amount. This approach ensures repayment and minimises default risk by enabling the sale of collateral in case of extreme market fluctuations [4]. The borrowing rate is influenced by liquidity in the pool, rather than reflecting the financial health of the borrower; it is more indicative of liquidity and market risk. Hence, when considering over-collateralised lending, the extent to which DeFi lending protocols facilitate true borrowing – where an agent gets into a position of net debt – is limited, creating a gap compared to traditional finance (TradFi) offerings.

To bridge this gap, a potential solution involves reducing the on-chain collateral requirement by replacing it with off-chain collateral that can be materialised through the creation of a dedicated Special Purpose Vehicle (SPV). Rather than having the corporation serve as the legal obligor, an SPV structure leverages the advantages of traditional securitisation frameworks. It does this by collateralising the loan with a diversified asset portfolio within an SPV and subjecting these assets to eligibility criteria, robust portfolio covenants, and comprehensive legal recourse. Another solution lies in the tokenisation of off-chain assets, allowing them to serve as collateral on-chain. By making the collateral ratio variable, we preserve the signalling role of collateral quality while enabling more flexible borrowing conditions [1]. By reducing the onchain over-collateralisation requirement, we introduce default risk, posing a challenge in determining a borrowing rate that accurately reflects the borrower's financial risk without relying on a third party or arbitrarily adding a risk premium to the existing algorithmic rate model.

While Aave and Compound use algorithmic interest rate curves based on utilisation, protocols that do not rely on on-chain over-collateralisation – like Notional, Maple Finance, or Goldfinch – involve fixed-rate lending through centralised negotiations or credit committee assessments. Our approach introduces decentralised, transparent rate formation suitable for unsecured lending at scale.

The following section details our structured approach to decentralised rate discovery. It includes the implementation of an auction, proposed as a method to accurately reflect credit risk in addition to enabling fixed borrowing rates, which are more suitable for most borrowing use cases.

Lending Pools Framework to Enable a Decentralised Rate Discovery

The lending process is initiated by the creation of a lending pool on-chain. These pools are tailored to individual borrowers and possess distinct characteristics, including the desired loan type, loan amount K , maturity period, and token type. We denote $LP_{B,\tau}$ as a lending pool assigned to a borrower B , and $D_{LP_{B,\tau}}$ represents the total deposit amount within that particular pool.

Pre-Pool Opening Phase

In order to deter borrowers from creating idle lending pools, it is required that borrowers lock a deposit before the opening of the pool. The size of the deposit is determined by a fraction of the desired borrowed amount. Once the borrower successfully borrows from their pool, the deposit will be returned to them.

However, in cases where the borrower does not end up borrowing from their pool despite the pool being filled up, the deposit will be distributed among the liquidity providers of that particular pool. This constraint ensures that borrowers have an interest in utilising the lending pool, as they risk losing their deposit if they do not borrow from it.

Lending Pool as a Set of Ticks

To enable an on-chain rate discovery, we propose to implement an auction process enabled by the division of lending pools into a series of ticks. Each tick represents a sub-pool of funds within the borrower's pool, and corresponds to a specific lending rate.

Liquidity providers, when contributing to the pool, select their lending rate, and their funds are allocated to the corresponding tick. For instance, if a liquidity provider opts for a 5% rate, their funds find placement in the 5% tick of the borrower's lending pool. The visual representation below offers a clearer depiction of the lending pool design:

Consider a zero-coupon bond auction where a bond unit delivers 100 at maturity. Let's assume a lending pool with lending rates of $r_1, \dots, r_n$, with T being the bond maturity, $p_1, \dots, p_n$ the implied bid prices and $d_1, \dots, d_n$ representing the amount of deposit available in each tick. We can derive the following bids:

Order Book Representation

Side	Rate	Deposit Available	Implied Bid Price	Implied Buyable Bond Units
bid	r_1	d_1	$p_1 = 100/(1 + r_1)^T$	d_1/p_1
bid	r_i	d_i	$p_i = 100/(1 + r_i)^T$	d_i/p_i
bid	r_n	d_n	$p_n = 100/(1 + r_n)^T$	d_n/p_n

where,

$$0 < r_1 < r_i < r_n, \text{ and } d_i \geq 0 \quad \forall i \in [0, n]$$

It is important to note that pools should not be limited in size; therefore, even if the amount in the pool is higher than the target amount to be borrowed, any lender can still add liquidity to the lending pool and challenge the lending rates until the end of the book-building phase. This creates market dynamics, rate competition, and gives access to a market rate discovery for borrowers.

During the book-building phase, the borrower is not yet authorised to borrow from their pool. They must wait for the end of the book-building phase to make sure all the commits have been gathered and are final.

Loan Origination Phase

After the conclusion of the book-building phase, liquidity providers are unable to make any further deposits or withdrawals. During the origination phase, borrowers can borrow a predetermined amount of K tokens from their pool. The borrower cannot borrow more or less than this agreed-upon amount, unless there is insufficient liquidity in the pool (i.e., if $D_{LP_{B,T}} \leq K$). The origination phase has a specific time limit corresponding to the duration set in the characteristics of the pool.

Lenders are provided with their chosen lending rate, resembling a form of discriminatory auction where the winning participants pay their bid prices [12]. It is essential to emphasise that, given the on-chain nature of bids, the auction is not sealed but open, fostering transparency and accessibility. The borrowing rate is simply the lowest volume-weighted rate that corresponds to the amount borrowed. It is derived from the ticks and is the result of the amount available in each tick. The borrowing rate is fixed and does not change during the life period of the loan.

The choice of discriminatory matching over uniform matching is motivated by the tick model's ability to establish an order book for the secondary market while maintaining consistent mechanisms within smart contracts. A borrowing event is likened to a selling event, and secondary prices can be derived from discounted future cash flow.

Monostori [13] suggests that the choice of auction format can significantly impact the behaviour of bidders and the functioning of the primary market. Monostori's findings indicate that uniform-price auctions tend to attract a larger number of bidders and enhance the role of the primary market compared to discriminatory-price auctions [14]. However, a deeper analysis of discriminatory-price auctions reveals potential advantages, such as ensuring continuity of financing, reducing volatility on the primary market, and preventing collusion. This is supported by Morales-Camargo et al. [15], who argue in favour of discriminatory auctions, contrary to the conclusions drawn by proponents of uniform-price auctions. Furthermore, Goldreich [16] highlights the susceptibility of uniform-price auctions to

The integration of auctions and ticks in decentralised lending frameworks offers several advantages over traditional DeFi models like Aave. Auctions facilitate market-driven rate discovery by leveraging competitive bidding [5, 6], ensuring rates reflect true market values and enhancing transparency and fairness [7, 8]. The use of ticks allows for granular rate adjustments, dynamically aligning lending rates with market conditions [9, 10] and incentivising information disclosure. This approach can lower transaction costs [11] by streamlining the lending process.

The pool opening marks the beginning of the book-building phase.

Book-Building Phase

The book-building phase is time-limited; its duration is set in the pool's characteristics. During this phase, liquidity providers can freely deposit into the lending pool at the lending rate of their choice. They are free to update their lending rate.

Additionally, liquidity providers can freely withdraw their funds as their funds have not yet been borrowed.

The ticks can be transposed to a limit order book restricted to the bid side. The bids are limit orders, and the bond issuance is a sell market order.

overbidding, as participants attempt to signal the secondary market, indicating potential drawbacks of this format.

Additionally, Myers et al. [17] emphasise the increased risk of collusion in uniform auctions, particularly in repeated settings, due to the payoff irrelevance of infra-marginal bids. It is crucial to acknowledge that the advantages of each auction format may vary based on specific market conditions and the objectives of the issuer. This is in line with the study by Beierlein and Katô [18], which highlights the trade-offs between auction formats, indicating that uniform-price auctions achieve lower award concentration and higher average revenues but experience higher revenue variance compared to discriminatory-price auctions. Therefore, Monostori's article concludes that the choice between auction formats should be carefully considered based on the specific context and desired outcomes. Hence, the decision to prefer discriminatory matching over uniform for practical reasons does not contradict observed choices in Monostori's article [13].

The decision to have bidders select lending rates instead of primary and secondary bond prices is driven by several factors, with a particular emphasis on the implications for gas consumption. Gas, in the context of blockchain, refers to the computational effort required to execute operations. In decentralised finance, every transaction, including the continuous updating of bid prices, incurs a cost in gas, which can accumulate significantly over time. By choosing to base the system on lending rates, the protocol significantly reduces the frequency and complexity of transactions that lenders need to perform. This is because lenders no longer need to continually update bid prices throughout the loan term, a process that can consume substantial amounts of gas due to the repeated and complex calculations involved. Instead, bid prices can be easily derived from the lending rate and the remaining time until maturity, simplifying the transaction process. This approach not only conserves gas, thereby minimising operational costs for users, but also contributes to the overall effectiveness of the smart contract implementation.

Loan Life Period

Depending on the type of loan, borrowers are required to make principal and interest payments either before or at maturity. Throughout the loan duration, lenders with unused funds in the pool can withdraw their remaining amount at any time. This allows for the withdrawal of pre-maturity interest payments and instalment payments. Once the final payment is made, all liquidity providers can freely withdraw their funds from the lending pool.

In the next section, we will evaluate the equilibrium of our proposed rate model, analysing its stability and performance in various scenarios.

Modelling the Rate Discovery Rate Discovery Game Framework

Our approach to rate discovery is, in fact, an open multi-unit auction, casting the borrower as the seller and lenders as bidders, and that can be formalised as an extensive form game. In this context, the seller offers multiple units for sale, and each bidder assigns a valuation to the units on offer. The game unfolds with the borrower declaring the desired borrowing amount. Subsequently, lenders deposit an amount into the tick that aligns with their preference and information and submit bids for the number of units they wish to purchase. The game concludes on the specified borrowing date, with units allocated to winning bidders, and successful bidders remit the amount of their bid to the seller.

Our game model comprises the following components:

- **Players:** One borrower, N lenders.
- **Action Sets:**

- $A_{lender} = \{\text{does not deposit, deposits any amount between 1 and } K \text{ at a rate in the range } r_1 \text{ to } r_n, \text{ updates the rate of an existing position}\}$
- $A_{borrower} = \{\text{borrows } K, \text{ does not borrow}\}$

Choice Nodes: Lenders are free to deposit and/or update their rate until the end of the book-building phase. The borrower cannot perform any action before the end of that phase.

Terminal Nodes: At the end of the book-building phase, the borrower can either borrow or not borrow.

We make the following assumptions:

- A borrower who has placed a significant amount as collateral and is a repeat borrower, thus being cautious about reputation risk. This implies that the borrower will not default maliciously and that there is no incentive for them to borrow regardless of the borrowing rate.
- The borrower expects to make a certain return on investment (ROI) on the borrowed amount, and any additional cost from borrowing is priced into the rate, which is the maximum rate that they are willing to accept for each unit. If the reserve rate is too low, there may not be enough lenders willing to bid at or below that rate, and the auction will not generate any revenue. If the reserve rate is too high, the borrower may not get the maximum revenue possible.
- The ROI is known by the lenders, or the borrower discloses a maximum rate at which they'd be willing to borrow, which is representative of the ROI. The assumption that borrowers' reserve rates (ROI) are known to lenders may be supported through verifiable disclosures. In practice, this could be enabled by cryptographic tools such as zero-knowledge proofs, DAO-approved financial statements, or decentralised credit scoring protocols. These mechanisms would allow borrowers to demonstrate expected returns without compromising decentralisation or privacy.
- We assume heterogeneous beliefs among lenders. Each lender k associates a default probability $p_{d,k}$ to the borrower which remains constant throughout the game. The assumption of heterogeneous beliefs among bidders is well-supported by the literature. Ockenfels and Roth [19] discuss the incidence of multiple bidding and its relation to late bidding, indicating that bidders may have varying beliefs about the auctioned item, leading to diverse bidding behaviours. Li and Zheng [20] develop an empirical model of entry and bidding controlling for unobserved auction heterogeneity, highlighting the presence of diverse beliefs among bidders in auction settings. Krasnokutskaya [21] and Decarolis [22] emphasise the importance of considering unobserved auction heterogeneity and the impact of asymmetric information, which can be indicative of heterogeneous beliefs among bidders. Moreover, Crosetto et al. [23] provide evidence that individual belief reports can be rationalised by subjective beliefs that differ from the objective truth, further supporting the presence of diverse beliefs among bidders in auction scenarios.
- We define RR as the recovery rate, the estimated per cent of the loan that will still be repaid to creditors in the event of default or bankruptcy.
- We set the risk-free rate to zero without loss of generality.
- As borrowing time is known and lenders have the ability to update their rate, we assume that lenders choose their lending rate with the knowledge of all the choices made by others. This implies that we are considering a finite perfect information game, and at least one pure strategy Nash equilibrium exists.

Objective Definition

To evaluate the suitability of our rate discovery, we must first define our objectives. While some auction models are assessed based on the expected revenue of the auctioneer, our objectives are as follows:

- Convergence: We aim to understand the mechanism that links the borrowing rate to the borrower's default probability that is assessed by the market.
- Speed of Convergence: Literature has shown that in centralised lending processes, banks can fail to discriminate between risky and non-risky borrowers [1, 2]. In decentralised lending, borrowers are compelled to provide their own information since there is no third party to furnish it. In the early 1980s, particularly in works by Milgrom [24] and in collaboration with Weber [25], significant advancements were made in auction theory. This research explored scenarios involving both private and common values, within reasonably straightforward mathematical conditions governing bidder information and value distribution. Milgrom's comprehensive analysis shed light on instances where sellers could potentially increase their revenues by sharing expert appraisals, like authenticity certificates or inspection protocols, with prospective bidders [26]. We will try to assess whether our rate discovery model can serve as an incentive for borrowers to provide more information, thus enabling their borrowing rate to converge more rapidly.

We proceed to assess our model equilibrium and evaluate whether it corresponds to lenders depositing in a tick that represents their true valuation of the borrower's default probability.

Multi-Unit Game with n Players and Perfect Information

In this section, we present a multi-unit model that captures the rate discovery process that we described in the first section.

Game Description

The game involves one borrower and N lenders. The borrower can choose to either borrow K or not borrow, while lenders can deposit any amount from 1 to K in the tick of their choice. There are n ticks.

Utility Functions

We define as d_i the deposit amount in tick r_i and CD_r , the cumulative volume up to tick r_i starting from the lowest tick. We assume that the lenders and the borrower have perfect information about the state of the pool at all times.

Lenders

For lender k and tick r_i ,

$$u_{lender_k}(\text{deposit } m \text{ at } r_i, \text{borrower borrows}) \\ = m \times [(1 - p_{d,k}) \times r_i - p_{d,k} \times (1 - RR)] \times 1_{CD_{r_i} \leq K}$$

where $p_{d,k}$ is the default probability evaluated by lender k , and RR is the recovery rate.

Borrower

$$u_{borrower}(\text{borrows}) = K \times (ROI - \sum \delta_i \times r_i)$$

where

$$(\delta_1, \delta_2, \dots, \delta_n) = \underset{\delta_i \leq a_i}{\operatorname{argmin}} \sum \delta_i \times r_i \\ \text{such that } \sum \delta_i = K$$

Equilibrium

Let $r_{borrowing}$ be the rate that corresponds to the one that would have been achieved if the borrower were to borrow K in the current state. We observe that in the case where the total value in the pool is lower than K, it is a strictly dominant strategy for all lenders to deposit at the rate that corresponds to the borrower's ROI as it maximises their utility function. However, if the total value in the pool exceeds K, the lenders are incentivised to deposit at a lower rate. If a certain percentage of the lenders are willing to lower their rate, in that case, they will lower their rate as low as they need in order to guarantee matching. We can derive an analogy between our model and the model described by Ausubel [27], who proposes an ascending- bid auction for multiple objects. Nonetheless, in our model, the bids (both the lending rate and the deposit amount) are updated not because the auctioneer raises the price but because bidders might want to lower their bidding rate to ensure matching. In the Ausubel auction, sincere bidding is an ex-post equilibrium [28] meaning that it is in the best interest of each bidder to submit sincere bids and accurately reveal their valuations for the items they want. In hindsight, after the auction concludes, no bidder could have achieved a better outcome by submitting dishonest or manipulative bids. The auction's design encourages truthful bidding, making it a strategy-proof mechanism. In our model, lenders will only be inclined to lend at their 'true value rate' r^* if their true value rate is below ROI and $CD_{r^*+rate \text{ spacing}} > K$. Overall, this requirement for lenders to deposit at their true value implies that the pool's total value must significantly exceed the amount to be borrowed, which leads to challenges in terms of capital efficiency.

Numerical Illustration

To illustrate the equilibrium of our game, we perform a numerical illustration and consider two types of borrowers. Borrower A that provides an extensive amount of information to prospective lenders and borrower B that provides a regular amount of information. We assume that they both have the exact same level of risk and have the same true default probability.

We use the following parameters:

- Order book range from 2% to 18%, rate spacing of 0.5%.
- Target loan amount: 100,000.
- Declared reserve rate 15%: the borrower declares that they will only be willing to borrow if their borrowing rate is lower than or equal to 15%.
- Recovery rate 30%.
- Lenders deposit sequentially in the pool. They choose their rate in order to maximise their utility function based on the status of the pool at deposit time.
- They can only deposit once in the pool, but can update their rate later. One deposit corresponds to one time stamp.
- Lenders can freely update their rate based on the other lenders' bids until the end of the auction, based on their utility function.
- For simplicity, the amount deposited by each lender is the same and does not change throughout the duration of the book-building phase. It differs for Borrower A and Borrower B as explained below.

We use the same default probability distribution across lenders and use a normal distribution centred on the actual default probability and a standard deviation of 1%. Hence, each lender k evaluates a default probability $p_{d,k}$ that follows a normal distribution and has an associated r_k^* such that

$$r_k^* = \left(\frac{p_{d,k} \times (1 - RR)}{1 - p_{d,k}} \right)^+ \times 0.005$$

As both borrowers have the same risk profile, we use the same parameters as for borrower A, i.e., mean 12%, standard deviation 1% which corresponds to an average r^* of 10%. The average r^* is considered the true market value borrowing rate.

To account for increased risk aversion for Borrower B and lower uncertainty for Borrower A, we model differently the lenders' bidding behaviour. Eső and Szentes [29] argue that in auctions, information plays a crucial role in attracting bidders.

They discuss how the level of information affects bidder participation and the optimal strategy for the seller in disclosing information. From their research, we can derive that an auction with more information on the valued item will attract more bidders compared to an auction with less information. Cohen and Einav [30] conducted research on risk preferences by analysing deductible choices in insurance. Although their study focuses on insurance deductibles, it provides insights into risk aversion and decision-making under uncertainty. In their benchmark model, they assume that individuals have full information about their risk exposure and level of risk aversion.

This assumption implies that individuals with more information are better equipped to assess their risk profile accurately. Therefore, a risk-averse agent with more information on the borrower would be more likely to choose a lower lending rate. Hinz and Spann [31] found that the amount and dispersion of information significantly impact bidding behaviour. They demonstrate that more information and greater dispersion of information lead to more competitive bidding behaviour. Additionally, they highlight the importance of betweenness centrality in the social network context, indicating that individuals who are well-connected and have access to diverse information sources are more likely to exhibit competitive bidding behaviour.

To reflect these findings, we assume that Borrower B's pool attracts 30% less liquidity in the same time period and that lenders in Borrower B's pool are less prone to updating their lending rate after depositing into the pool. At every new deposit, we assume that 30% of existing lenders update their rate based on the order book evolution for Borrower A and 15% for Borrower B.

Our goal is to illustrate whether the borrowing rate converges to the market value and the speed of convergence.

Analysis

Borrowing Rate

Time	TVL	Average Rate (%)	Std (%)
20	100,000	15	0
40	200,000	11.22	0.05
100	500,000	9.75	0.06

Borrower A

Time	TVL	Average Rate (%)	Std (%)
20	60,000	15	0
40	120,000	14.07	0.05
100	300,000	9.82	0.06

Borrower B

Convergence

After running the simulations, we observe that, with a significant amount of TVL and time, our model allows convergence as both borrowers are able to reach the market value borrowing rate of 10%. Lenders' lending rates converge to their respective r^* for both borrowers.

Speed of Convergence

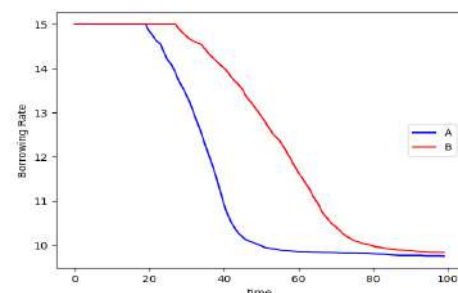
For Borrower A, the average borrowing rates are 15%, 11.22%, and 9.75% for TVL levels of 100,000, 250,000, and 500,000, respectively. For Borrower B, the average borrowing rates are 15%, 14.07%, and 9.82% for TVL levels of 60,000, 120,000, and 300,000, respectively. Borrower A reaches the market value borrowing rate faster and with a lower amount of TVL, illustrating that, given the same level of risk, Borrower A is able to achieve their true borrowing rate faster by providing more information to potential lenders. Lenders' lending rates converge to their respective r^* at a greater speed for Borrower A than for Borrower B. It is also fair to assume that by providing less information, Borrower B will attract fewer bidders than Borrower A for the same duration, so Borrower B's lending rate will be even more impacted.

Gas Consideration

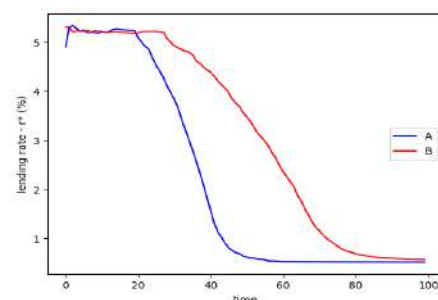
Our proposed mechanism offers accurate rate discovery at the expense of high gas requirements and frequent interactions. Given the gas costs on Ethereum L1, implementation would likely benefit from Layer 2 solutions (e.g., Optimism, Arbitrum) or dedicated app chains. Additionally, batching transactions and limiting update frequency could help reduce operational costs without significantly compromising convergence.

Gas and Capital Efficiency

The simulations illustrate that the rate model is not optimal in terms of capital efficiency, as a substantial amount of Total Value Locked (TVL) is required to reach the true value. However, it is worth noting that the required amount of TVL would sharply reduce if we were to increase the amount of update rate actions. We arbitrarily chose a 30% update rate among existing lenders at each deposit for Borrower A and 15% for Borrower B. Since capital is a scarce resource, we will explore in the next section how we can alleviate this constraint.



Evolution of Theoretical Borrowing Rate



Evolution of Lending Rate vs R Star

Multi-Unit Game with n Players and Imperfect Information

Game Description

In order to address the high capital efficiency, we introduce uncertainty in the amount to be borrowed and thus move to an incomplete information model. We introduce a Bayesian model where the borrower is faced with three business opportunities:

- Type 1: probability q_1 , high liquidity needs: they will borrow K_1 ,
- Type 2: probability q_2 , medium: they will borrow K_2 .
- Type 3: probability q_3 , low: they will borrow K_3

with $K_1 > K_2 > K_3$.

We also make the following assumptions:

- The lenders are unaware of the borrower's type.
- All lenders associate the same probability q to each opportunity, leading to r^* , the lowest rate at which the lender would be willing to lend to maintain a positive utility function.
- The reserve price / ROI on each business opportunity remains constant.

Utility Functions

The utility function of the lenders and the borrower are now as follows:

Lenders

For lender k and tick r_1 ,

$u_{lender_k}(\text{deposit } m \text{ at } r_i, \text{ borrower borrows})$

$$= q_1 \times m \times [(1 - p_{\text{default}}) \times r_i + p_{d,k} \times (1 - RR)] \times 1_{CD_{r_i} \leq K_1}$$

$$+ q_2 \times m \times [(1 - p_{\text{default}}) \times r_i$$

$$+ p_{d,k} \times (1 - RR)] \times 1_{CD_{r_i} \leq K_2}$$

$$+ q_3 \times m \times [(1 - p_{\text{default}}) \times r_i$$

$$+ p_{d,k} \times (1 - RR)] \times 1_{CD_{r_i} \leq K_3}$$

Borrower

$$u_{borrower}(\text{borrows } M) = 1/(M) \times \sum \delta_i \times r_i$$

where

$$(\delta_1, \delta_2, \dots, \delta_k) = \underset{\delta_i < d_i}{\operatorname{argmin}} \sum \delta_i \times r_i$$

$$\text{such that } \sum \delta_i = M$$

Numerical Illustration

We consider the same two different borrowers. Borrower A provides an extensive amount of information to prospective lenders and borrower B provides a low amount of information.

We use the following parameters:

- Order book range from 2% to 20%, rate spacing of 0.5%.
- Target loan amount
 - 100,000 with probability 33%

- 50,000 with probability 33%
- 20,000 with probability 33%
- Declared reserve rate 15%.
- Recovery rate 30%.
- Lenders deposit sequentially in the pool. They choose their rate in order to maximise their utility function based on the status of the pool at deposit time.
- They can only deposit once in the pool, but can update their rate later. One deposit corresponds to one time stamp.
- Lenders can freely update their rate based on the other lenders' bids until the end of the auction. Their decision is also driven by their utility function.
- For simplicity, the amount deposited by each lender is the same. It differs for borrower A and borrower B as explained below.

As for the previous simulation, depending on the borrower, we modelise differently the default probability distribution evaluated by the lenders and use the same parameters: mean 12%, standard deviation 1% which corresponds to a theoretical borrowing rate of 8%.

Analysis

Convergence and Speed of Convergence

Borrowing Rate

Time	TVL	Average Rate (%)	Std (%)
10	50,000	14.34	0
20	100,000	11.34	0
40	200,000	9.55	0.05
100	500,000	9.05	0.06

Borrower A

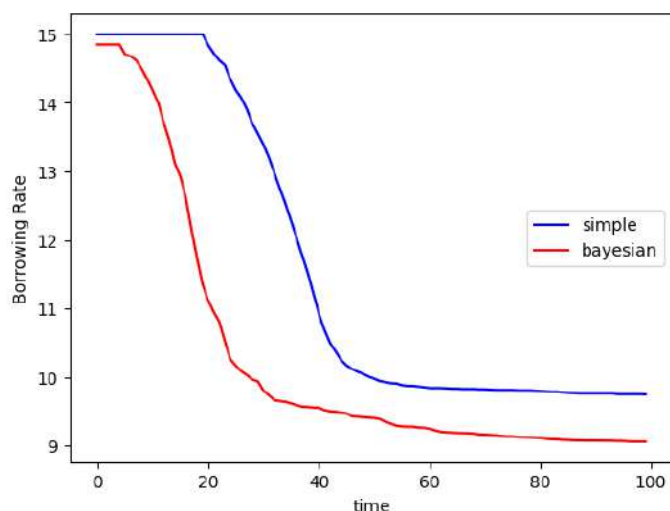
Time	TVL	Average Rate (%)	Std (%)
10	30,000	14.44	0
20	60,000	12.95	0
40	120,000	9.76	0.05
100	300,000	9.15	0.06

Borrower B

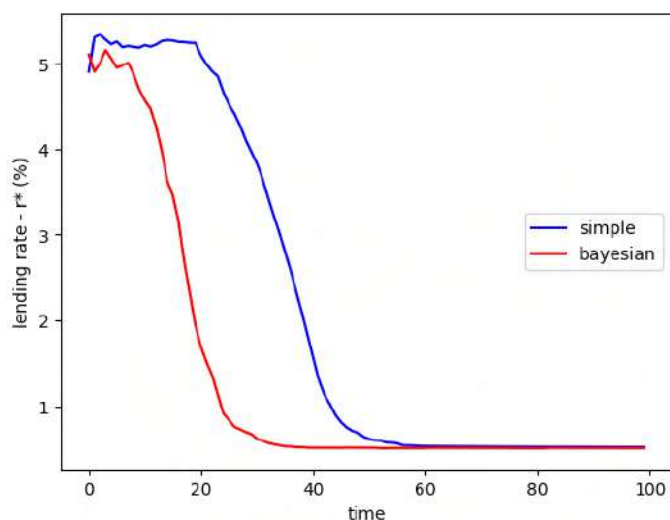
For borrower A, the average borrowing rates at time intervals of 10, 20, 40, and 100 are 14.34%, 11.34%, 9.55%, and 9.05%, respectively. For borrower B, the average borrowing rates at time intervals of 10, 20, 40, and 100 are 14.44%, 12.95%, 9.76%, and 9.15%, respectively. Similarly to the previous model, borrower A enjoys lower average borrowing rates across all time intervals thanks to their higher TVL and more frequent bid updates. By providing more information to their potential lenders, the borrowers are able to lower their borrowing rate and reach their true borrowing rate at a faster pace i.e., with a lower amount of TVL.

Comparison with Previous Model

Compared with the previous model, we can visualise that adding uncertainty on the amount borrowed allows one to reach the true borrowing rate with a lower amount of TVL. This model operates with lower capital. Adding uncertainty of the amount borrowed allows a faster convergence to the market average lending rate.



Evolution of Theoretical Borrowing Rate (Borrower A)



Evolution of Lending Rate vs R Star (Borrower A)

Model Representation Limitations

Borrower's Creditworthiness

The numerical simulations assume perfect information about the borrower's creditworthiness and difference in lender's assessment of default probability only coming from lender's expertise and information. This is a strong assumption that relies on the fact that decentralised systems allow full transparency so if we consider DAO as borrowers, it is fair to assume that we have full transparency on their creditworthiness. DAOs operate on blockchain technology, which allows for complete visibility of their financial transactions and governance decisions, making it reasonable to assume full transparency regarding their creditworthiness. For instance, a DAO's smart contracts and on-chain activity can be publicly audited, providing lenders with comprehensive insights into the organisation's financial health and operational history.

However, this assumption becomes more tenuous when applied to 'traditional' borrowers, such as individuals or conventional businesses. These entities may not operate on blockchain platforms and thus do not benefit from the same level of automated transparency. For example, a small business seeking a loan in a DeFi platform might not have its financial records or operational data readily accessible on a blockchain, making it challenging for lenders to assess creditworthiness with the same degree of

confidence as they would with a DAO.

Stiglitz and Weiss [2] argue that when there is imperfect information, lenders may not be willing to lend to all borrowers who are willing to pay the market interest rate. Stiglitz and Weiss suggest that governments can address credit rationing by providing more information about borrowers' creditworthiness, either directly or through institutions such as credit bureaus. This can help lenders make more informed lending decisions and reduce the need for credit rationing. In decentralised finance, this can be replicated by creating a data room accessible to all potential lenders where the borrowers could freely disclose all their financial documents. A limitation would be to verify the validity of the documents and ensure that everything has been shared.

Unknown Borrowed Amount

Our simulations on the Bayesian model assume that lenders have the same evaluation of the amount borrowed. When looking at a sequential open multi-unit auction, if the number of units to be sold is unknown to the bidders, it can potentially influence their bidding behaviour and make it more difficult for them to bid their true values. Each bidder has their own assumption on the number of units to be sold. The uncertainty about the number of units to be sold affects the bidders' beliefs about the strategies of the other bidders, which in turn can affect their optimal bidding strategy.

However, if the bidders have a common understanding or prior knowledge about the distribution of the number of units to be sold, they may still be able to bid their true values. For example, if the bidders know that the number of units to be sold follows a certain distribution, such as a uniform distribution, they may be able to use this information to determine their optimal bidding strategy and bid their true values. This is the case in our illustrative example. In the case of a recurrent borrower, the estimate of the amount of bidding to be sold can be based on prior knowledge and behaviour, thus improving the bidding process.

Market Frictions

While our model assumes rational actors, real-world DeFi markets often exhibit behaviours such as strategic underbidding, front-running, and lazy participation. These frictions can distort rate discovery and impact the efficiency of auctions. Future work may incorporate mechanisms such as anti-sniping rules or incentive alignment tools to mitigate such effects.

Lenders' Interactions

The model illustration assumes that lenders make their lending decisions independently and do not take into account the actions of other lenders. However, in reality, lenders may reevaluate their assessment of a borrower's default probability based on the actions of other lenders. This is because lenders may have access to different information or expertise, and their decisions may influence the borrower's financial position.

For example, if one lender decides to increase their exposure to a borrower, other lenders may perceive this as a positive signal and decide to increase their exposure as well. Alternatively, if one lender decides to reduce their exposure to a borrower, other lenders may perceive this as a negative signal and decide to reduce their exposure as well. This can lead to a cascade effect where lenders' actions reinforce each other and lead to a concentration of exposure to certain borrowers.

The impact of lenders' interactions on credit markets has been widely studied in the finance literature. Martin and Ventura [32] show how banks' decisions to lend to each other can lead to systemic risk and banking crises. In the context of decentralised lending, lenders' interactions may also play a significant role in determining the efficiency and stability of the lending market.

One way to address the issue of lenders' interactions is to introduce mechanisms that encourage lenders to share information and collaborate. For example, lenders could be incentivised to share their expertise or data about borrowers, or to form coalitions that jointly assess borrowers' creditworthiness. Such mechanisms could lead to a more efficient allocation of credit and reduce the risk of cascading defaults. However, implementing such mechanisms would require overcoming coordination and free-riding problems, as well as ensuring that lenders do not collude to manipulate the lending market.

Conclusion

This paper provides a significant advance in decentralised finance by proposing a framework for rate discovery that accurately reflects a borrower's probability of default. The model enhances our understanding of lending efficiency in DeFi while promoting a transparent and flexible borrowing environment. Encouraging the disclosure of financial information aligns incentives between borrowers and lenders, fostering trust across decentralised lending markets. This approach has the potential to broaden the scope of DeFi lending, making it a more viable and competitive alternative to traditional financial institutions.

While our model assumes rational actors, real-world DeFi markets often exhibit behaviours such as strategic underbidding, front-running, and passive participation. These frictions can distort rate discovery and reduce the efficiency of auction mechanisms. Future work could explore the implementation of this model on existing platforms, evaluating its performance under practical constraints. Additionally, incorporating mechanisms such as anti-sniping rules, dynamic bidding penalties, or incentive alignment tools could help mitigate these market inefficiencies. Such enhancements will be essential to assess the model's full impact and scalability in realworld financial environments.

References

- [1] H. Bester, "Screening vs. Rationing in credit markets with imperfect information," *The American Economic Review*, vol. 75, no. 4, pp. 850–855, 1985.
- [2] J. E. Stiglitz and A. Weiss, "Credit rationing in markets with imperfect information," 1981, doi: 10.7916/D8V12FT1.
- [3] J. Xu, "From banks to defi: The evolution of the lending market," 2021, doi: 10.48550/arxiv.2104.00970.
- [4] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, and A. Gervais, "An empirical study of defi liquidations," *Proceedings of the 21st ACM Internet Measurement Conference*, 2021, doi: 10.1145/3487552.3487811.
- [5] P. Klemperer, "Auction theory: A guide to the literature," *Journal of Economic Surveys*, vol. 13, no. 3, pp. 227–286, 1999.
- [6] P. Milgrom, "Rational expectations, information acquisition, and competitive bidding," *Econometrica*, vol. 49, no. 4, pp. 921–943, 1981.
- [7] V. Krishna, *Auction Theory*. Academic Press, 2002.
- [8] R. B. Myerson, "Optimal auction design," *Mathematics of Operations Research*, vol. 6, no. 1, pp. 58–73, 1981.
- [9] L. M. Ausubel, "An efficient ascending-bid auction for multiple objects," *American Economic Review*, vol. 94, no. 5, pp. 1452–1475, 2004.
- [10] R. P. McAfee and J. McMillan, "Auctions and bidding," *Journal of Economic Literature*, vol. 25, no. 2, pp. 699–738, 1987.
- [11] M. H. Rothkopf, T. J. Teisberg, and E. P. Kahn, "Why are vickrey auctions rarely used?" *Journal of Political Economy*, vol. 98, no. 1, pp. 94–109, 1990.
- [12] P. Klemperer, "Auctions: Theory and practice," *SSRN Electronic Journal*, 2004, doi: 10.2139/ssrn.491563.
- [13] Z. Monostori, "Discriminatory versus uniform-price auctions," *MNB Occasional Papers No. 111*, 2014.
- [14] R. Engelbrecht-Wiggans, J. A. List, and D. Reiley, "Demand reduction in multi-unit auctions with varying numbers of bidders: Theory and evidence from a field experiment*," *International Economic Review*, vol. 47, pp. 203–231, 2006, doi: 10.1111/j.1468-2354.2006.00377.x.
- [15] E. Morales-Camargo, O. Sade, C. Schnitzlein, and J. F. Zender, "Divisible good auctions with asymmetric information: An experimental examination," *Journal of Financial and Quantitative Analysis*, vol. 48, no. 4, pp. 1271–1300, 2013, doi: 10.1017/S0022109013000409.
- [16] D. Goldreich, "Underpricing in discriminatory and uniform-price treasury auctions," *Journal of Financial and Quantitative Analysis*, vol. 42, no. 2, pp. 443–466, 2007, doi: 10.1017/S0022109000003343.
- [17] E. Myers, A. Bostian, and H. Fell, "Asymmetric cost pass-through in multi-unit procurement auctions: An experimental approach*," *Journal of Industrial Economics*, vol. 69, pp. 109–130, 2021, doi: 10.1111/joie.12254.
- [18] J. J. Beierlein and H. Katô, "Ipo mechanisms: A comparison of book-building, discriminatory price auctions and uniform price auctions," *The Japanese Finance: Corporate Finance and Capital Markets in ...*, pp. 135–152, doi: 10.1016/s1569-3767(03)04007-x.
- [19] A. Ockenfels and A. E. Roth, "Late and multiple bidding in second price internet auctions: Theory and evidence concerning different rules for ending an auction," *Games and Economic Behavior*, vol. 55, pp. 297–320, 2006, doi: 10.1016/j.geb.2005.02.010.
- [20] T. Li and X. Zheng, "Entry and competition effects in first-price auctions: Theory and evidence from procurement auctions," *Review of Economic Studies*, vol. 76, pp. 1397–1429, 2009, doi: 10.1111/j.1467-937x.2009.00558.x.
- [21] E. A. Krasnokutskaya, "Identification and estimation of auction models with unobserved heterogeneity," *The Review of Economic Studies*, vol. 78, pp. 293–327, 2011, doi: 10.1093/restud/rdq004.
- [22] F. Decarolis, "Comparing public procurement auctions," *International Economic Review*, vol. 59, pp. 391–419, 2018, doi: 10.1111/iere.12274.
- [23] P. Crosetto, A. Filippin, P. Katuscak, and J. Smith, "Central tendency bias in belief elicitation," *Journal of Economic Psychology*, vol. 78, p. 102273, 2020, doi: 10.1016/j.joep.2020.102273.
- [24] P. Milgrom, "Rational expectations, information acquisition, and competitive bidding," *Econometrica*, vol. 49, p. 921, 1981, doi: 10.2307/1912511.
- [25] P. Milgrom and R. J. Weber, "A theory of auctions and competitive bidding," *Econometrica*, vol. 50, p. 1089, 1982, doi: 10.2307/1911865.
- [26] P. Klemperer, "Auction theory: A guide to the literature," *Journal of Economic Surveys*, vol. 13, pp. 227–286, 1999, doi: 10.1111/1467-6419.00083.
- [27] L. M. Ausubel, "An efficient ascending-bid auction for multiple objects," *American Economic Review*, vol. 94, pp. 1452–1475, 2004, doi: 10.1257/0002828043052330.
- [28] T. Masuda, R. Mikami, T. Sakai, S. Serizawa, and T. Wakayama, "The net effect of advice on strategy-proof mechanisms: An experiment for the vickrey auction," *Experimental Economics*, vol. 25, pp. 902–941, 2022, doi: 10.1007/s10683-021-09736-5.
- [29] P. Eső and B. Szentes, "Optimal information disclosure in auctions and the handicap auction," *Review of Economic Studies*, vol. 74, pp. 705–731, 2007, doi: 10.1111/j.1467-937x.2007.00442.x.
- [30] A. Cohen and L. Einav, "Estimating risk preferences from deductible choice," *American Economic Review*, vol. 97, pp. 745–788, 2007, doi: 10.1257/aer.97.3.745.
- [31] O. Hinz and M. Spann, "The impact of information diffusion on bidding behavior in secret reserve price auctions," *Information Systems Research*, vol. 19, no. 3, pp. 351–368, 2008, doi: 10.1287/isre.1080.0190.
- [32] A. Martín and J. Ventura, "Economic growth with bubbles," *American Economic Review*, vol. 102, pp. 3033–3058, 2012, doi: 10.1257/aer.102.6.3033.

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

CE is the main author of the paper. HA did proof-reading and project supervision.

Funding:

None declared.

Acknowledgements:

We are grateful for research grants from the Paris-Dauphine Partnership Foundation. We thank the participants to the 7th Blockchain International Scientific Conference 2025 for their very helpful comments.

F-Procure: A Decentralised, Modular Framework for Transparent, Compliant and Efficient Procurement on the Flare Network

Pax Ola

Caypax Inc., Cayman Islands

Correspondence: info@caypax.com

Received: 18 November 2025 **Accepted:** 23 January 2026 **Published:** 23 March 2026

Abstract

Procurement remains constrained by centralised digital architectures that increase administrative effort, limit transparency and complicate compliance management. This paper presents F-Procure: a decentralised, modular procurement framework organised into five layers: blockchain execution, smart contracts, ERP interoperability, AI-assisted analytics and compliance-aware governance. The framework is implemented as a minimum viable prototype on the Flare Network's Coston2 and Songbird test environments, which are used here as technical testbeds rather than as platforms under evaluation in their own right.

Using small-scale, manually executed synthetic procurement scenarios, the study examines whether core stages – tender creation, sealed-bid commit–reveal, award and escrow – can be encoded in smart contracts and traced through verifiable on-chain audit trails. An illustrative comparison with a conventional database-driven workflow suggests that the modular, event-driven design can reduce manual reconciliation effort in bid evaluation and audit preparation within the controlled scenarios tested, although no statistically generalisable performance benchmarks are reported. The prototype also demonstrates how basic procedural requirements (such as submission deadlines and documentation flags) can be expressed as programmable conditions, and how a minimal anomaly-detection layer can flag constructed irregular bidding patterns for human review.

The paper positions F-Procure within existing international experiments in blockchain-enabled procurement and related digital-government initiatives and sets out a governance model and policy-oriented adoption roadmap for future public-sector pilots. It concludes that F-Procure should be viewed as an early-stage reference architecture that suggests the potential feasibility of decentralised, compliance-aware procurement, while highlighting the need for larger-scale empirical evaluation, richer technical artefacts and comparative, platform-agnostic analysis in subsequent research.

Keywords: *Decentralized Procurement; Blockchain; Modular Architecture; Flare Network; Smart Contracts; Supply Chain Transparency.*

JEL Classifications: *D73; L14; O33; C88; G20; H57; K12; F63; L86; K24.*

1. Introduction

Public procurement remains one of the most administratively intensive functions within government and large organisations, with longstanding challenges related to transparency, auditability, vendor competition and compliance management. Traditional digital procurement systems have improved record-keeping but remain largely centralised, which can introduce opacity, reduce interoperability across departments or jurisdictions and increase vulnerability to process irregularities. These limitations have motivated exploration into distributed ledger technologies (DLTs) as a means of improving traceability, integrity and automation within procurement workflows [1–5].

Several jurisdictions have piloted blockchain-based procurement or related transparency systems, including initiatives within the European Union, South Korea and multilateral development and GovTech programmes [1,5]. These early efforts rely predominantly on permissioned or consortium-led blockchains and typically focus on improving audit trails or digitising bids. While valuable, such systems often retain infrastructural constraints—limited cross-chain interoperability, reliance on off-chain intermediaries for data feeds and difficulty integrating with legacy enterprise resource planning (ERP) systems [1–6,7].

This paper introduces F-Procure: a modular procurement framework designed for deployment on public or hybrid blockchain networks and implemented in minimum viable product (MVP) form on the Flare Network's Coston2 and Songbird environments [7]. As illustrated in Figure 1, the F-Procure model reframes procurement from a single, centralised database workflow to a modular, decentralised architecture in which auditability and control are distributed across several coordinated layers. F-Procure proposes an architectural model comprising five layers: (i) a blockchain execution layer, (ii) a smart-contract layer, (iii) an ERP interoperability layer, (iv) an AI analytics layer and (v) a compliance and governance layer. A key motivation is to illustrate how a modular design can support more transparent procurement processes without necessitating full system replacement for public-sector adopters.

Flare's technical features—specifically the Flare Time Series Oracle (FTSO), Flare Data Connector (FDC) and FAssets protocol—provide a useful testbed for examining how enshrined data feeds and trust-minimised cross-chain assets might support procurement workflows [7]. Importantly, these technologies are evaluated here not as commercial products but as architectural components enabling decentralised data access, auditability and multi-asset settlement. Comparable patterns could, in principle, be realised on other DLT platforms that offer oracle and interoperability

services; Flare is used in this study as one concrete instantiation of a broader architectural approach.

To explore technical feasibility at MVP scale, a working prototype was developed, and a series of manually executed synthetic procurement transactions were tested and recorded on-chain. These controlled evaluations focused on functional behaviour—vendor onboarding, sealed-bid commit–reveal, contract-lifecycle transitions and escrow execution. The synthetic transactions were intentionally small in number and designed to test correctness rather than throughput, with all events verified via Flare’s blockchain explorers [4]. Any observations about process efficiency in this paper are therefore indicative and scenario-specific, not statistically generalisable benchmarks.

This paper contributes to ongoing research by:

1. presenting a modular architecture for procurement on public or hybrid blockchains;
2. providing an initial technical demonstration, via small-scale synthetic workloads, of commit–reveal auctions, multi-phase contract execution and on-chain audit trails;
3. articulating a policy-oriented governance framework for future public-sector pilots; and
4. positioning F-Procure among existing international procurement pilots by clarifying where its architecture diverges from prior approaches, particularly in its use of enshrined data protocols and potential cross-chain settlement [1–5,8].

Throughout, the analysis is framed explicitly as early-stage, design-science-oriented MVP work rather than as a large-scale operational evaluation. The paper therefore foregrounds architectural contribution, feasibility insights and policy implications, while acknowledging clear limitations in scale, empirical scope and legal codification.

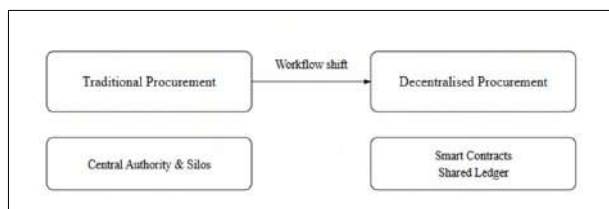


Figure 1: Conceptual comparison of legacy and decentralised procurement systems (MVP architectural framing).

2. Related Work

The intersection of DLTs and public procurement has become an important area of scholarly and institutional inquiry [1–5,9]. Early work positioned blockchain as a means to enhance transparency, reduce opportunities for corruption and introduce tamper-evident audit trails into tendering processes. Pilot programmes by international organisations and national governments have explored how distributed ledgers might support supplier registration, bid submission, contract award and payment tracking [1–3,5]. Despite this interest, large-scale operational adoption remains limited, in part because of practical challenges of scalability, compliance alignment and integration with existing enterprise resource planning (ERP) systems.

2.1 Early Experiments and Policy Context

Significant experimentation has taken place across public-sector contexts. The European Union’s explorations into blockchain for public procurement, South Korea’s Public Procurement Service pilots and World Bank–associated Procurement initiatives collectively demonstrated the feasibility of immutable audit trails, supplier identity verification and

secure document timestamping in procurement or adjacent domains [1–3,5]. These initiatives, however, generally employed permissioned or consortium blockchains, which facilitated institutional oversight but constrained interoperability and openness. The emphasis was often on document registration and verification rather than on automating the full contract lifecycle.

Scholarly works likewise highlight blockchain’s potential to automate aspects of compliance validation through smart contracts, particularly for enforcing deadlines, eligibility criteria and procedural steps [2,4,6]. At the same time, the stringent legal and procedural requirements governing procurement – especially around data sovereignty, confidentiality and fair competition—continue to limit the extent to which blockchain systems can be integrated into end-to-end procurement workflows. Much of the literature concludes that technical promise alone is insufficient without careful consideration of legal frameworks, institutional capacity and governance structures [2,4–6].

2.2 Technical Limitations in Existing Frameworks

Most prior systems emphasise auditability and record-keeping but stop short of providing an integrated, multi-layer approach that connects smart-contract logic with ERP systems, financial settlement mechanisms and ongoing analytics. The reliance on permissioned or consortium architectures can reintroduce forms of centralisation, concentrating control over validation and data access in a small set of institutions [1–3]. In many pilots, external data feeds are handled through bespoke middleware or manually curated interfaces, rather than through standardised oracle frameworks or cross-chain protocols. A high-level comparison of representative EU, World Bank and South Korean pilots with the F-Procure MVP across dimensions such as network type, smart-contract support, interoperability, ERP integration, analytics and deployment stage is presented in Figure 2, drawing on published descriptions of these initiatives [1,4,5].

The absence of robust interoperability primitives restricts the ability to bridge external data sources or legacy financial systems. Where integration with ERPs is attempted, it is often implemented as a loosely coupled add-on rather than as a coherent part of the system design. Additionally, multi-jurisdictional compliance remains a persistent challenge: procurement obligations, documentation formats and audit expectations vary considerably across legal contexts, complicating attempts to apply uniform technical standards [2,4,10–12]. As a result, many initiatives have focused on narrow functions—such as supplier registries or timestamping—rather than on full end-to-end contract-lifecycle management.

2.3 Emergent Research Directions

Recent research has explored the use of oracle networks and cross-chain infrastructure to bridge off-chain information and on-chain execution. Oracle systems such as Chainlink, Band Protocol and others have been proposed as mechanisms to feed market prices, reference data and external events into smart-contract-based procurement or financial systems [8,13]. These approaches introduce greater verifiability but often depend on external node operators and may not integrate natively with compliance rules, governance workflows or ERP processes.

Parallel work in digital-government and GovTech studies has highlighted the importance of modular architectures that can accommodate diverse legal and organisational requirements, while maintaining interoperability with existing information systems [4,5]. A smaller subset of the literature has begun to consider combinations of blockchain, artificial intelligence (AI) and data analytics to support risk-based auditing and anomaly detection in public administration. However, detailed examinations of systems that combine smart-contract automation, modular ERP integration, AI-assisted oversight and governance tooling within a unified architectural design remain relatively limited.

2.4 F-Procure's Contribution to the Literature

Within this landscape, F-Procure contributes an architectural and governance framework rather than a fully deployed production system. Its five-layer model integrates blockchain execution, smart-contract automation, ERP interoperability, AI-assisted analysis and compliance parameterisation as interdependent components. In the current MVP implementation, the Flare Network is used strictly as a technical testbed, providing enshrined data protocols (the Flare Time Series Oracle and Flare Data Connector) and a cross-chain mechanism (FAssets) that allow examination of how decentralised data feeds and trust-minimised asset representation might support procurement workflows [7].

The contribution lies not in claiming to be the first blockchain-based procurement initiative but in articulating how these capabilities may be arranged in a modular, policy-aligned framework; in explicitly addressing governance and compliance alongside technical design; and in validating core functional behaviours—vendor onboarding, commit–reveal bidding, contract-lifecycle transitions and audit-log generation—through small-scale, manually executed synthetic procurement transactions recorded on-chain. While this does not replace the need for larger-scale pilots or independent benchmarking, it provides an empirically grounded reference architecture for future work on interoperable, governance-aware procurement systems that could, in principle, be implemented on Flare or other suitable DLT platforms.

Framework	Network Type	Smart Contract Support	Interoperability	ERP Integration	Analytics	Deployment Stage
EU Pilot	Permissioned consortium	Limited	Minimal	Not integrated	None	Pilot
World Bank	Permissioned	Limited	Minimal	Not integrated	None	Pilot
South Korea	Permissioned	Moderate	Minimal	Not integrated	None	Pilot
F-Procure (MVP)	Public testnet (Flare)	MVP contract set	Architectural capability	Architectural, not implemented	MVP anomaly detection	MVP

Figure 2: Comparative landscape of blockchain procurement frameworks.

3. System Architecture

The F-Procure framework is constructed as a five-layer modular stack, designed to support interoperability, auditability and compliance-aware design whilst maintaining operational flexibility. Each layer is logically separable yet communicates through well-defined interfaces and secure data flows. This modular structure is intended to allow public-sector organisations to adopt individual components incrementally, reducing the need for disruptive, wholesale platform migration. The overall five-layer system architecture—comprising blockchain execution, smart-contract logic, ERP interoperability, AI analytics and compliance—is summarised in Figure 3. In the present work, the architecture is realised as a minimum viable product (MVP) deployment on Flare's Coston2 and Songbird test networks, with a subset of functionalities exercised through manually executed synthetic procurement transactions [7].

3.1 Blockchain Layer

At the foundation lies the blockchain layer, which provides immutable record-keeping and decentralised consensus. Procurement-relevant events—such as tender creation, bid commitment, bid reveal, contract state transitions and escrow actions—are represented as transactions recorded on the Flare test networks [7]. Flare's hybrid architecture, combining Avalanche-based consensus with Ethereum Virtual Machine (EVM) compatibility, offers a familiar smart-contract environment and relatively fast finality for the purposes of MVP experimentation.

In the present MVP, only a limited number of synthetic transactions were executed; accordingly, claims are restricted to functional correctness rather than high-volume throughput. Each transaction is hashed and

timestamped, forming cryptographic audit trails that can be independently verified on-chain without exposing sensitive bid content. This design supports selective transparency—a critical property for procurement, where commercial confidentiality must coexist with public accountability.

3.2 Smart-Contract Layer

Above the base ledger sits the smart-contract layer, which encodes the core procurement logic. Each tender is modelled as a contract instance that governs:

- vendor registration for that tender;
- sealed-bid commit–reveal submission;
- evaluation and award state transitions; and
- escrow release conditions.

The MVP implements a simplified commit–reveal protocol to preserve bid confidentiality until the evaluation phase. Bidders first submit a hash of their bid (commit), and later reveal the underlying values, allowing verification that no post hoc alterations occurred. The smart contracts emit events at each stage, and these events were used in the experiments to confirm that synthetic workloads were correctly processed and reflected in on-chain logs.

Basic audit hooks are incorporated into the contract logic, such as proof-of-submission time and proof-of-non-alteration. In the current prototype, these are demonstrated on a small number of controlled transactions; extending them into fully parameterised, jurisdiction-specific compliance modules is identified as future work.

3.3 ERP Interoperability Layer

The ERP interoperability layer is designed to bridge blockchain workflows with existing enterprise systems used by procurement agencies. Conceptually, it exposes secure APIs and data-exchange standards (for example, JSON-based payloads and OData-style interfaces) to synchronise key procurement events—such as supplier registry updates, tender status and payment milestones—between F-Procure and legacy ERP platforms.

In this phase of research, a sandbox ERP connector was specified and partially prototyped at interface level, but not fully integrated into a live ERP instance. The design work demonstrated that standard API endpoints could be used to map procurement events to conventional ERP objects (such as purchase orders and vendor records), and initial endpoint definitions were validated against test schemas. Full end-to-end ERP integration is reserved for subsequent pilot deployments and is therefore discussed in this paper as an architectural capability rather than a completed implementation.

3.4 AI Analytics Layer

The AI analytics layer introduces analytical capabilities for monitoring procurement activity and highlighting potential irregularities. At the architectural level, it is intended to accommodate machine-learning models that analyse bidding patterns, pricing behaviour and historical performance indicators so as to flag outliers or suspicious clusters of activity for human review.

In the current MVP, this layer is realised in a minimal form, using simple rule-based logic and basic statistical checks applied to the small set of synthetic transactions generated during testing. These checks were sufficient to demonstrate how bids could be programmatically flagged for further review – for example, closely clustered bid amounts or unusual timing patterns. No machine-learning models were trained or evaluated, and no general claims are made about detection performance. The contribution at this stage is therefore primarily architectural: it shows that an analytics service can subscribe to on-chain events and apply integrity checks without

altering the underlying procurement logic. More sophisticated anomaly-detection methods, including privacy-preserving or federated approaches, are left to future research.

3.5 Compliance Layer

The uppermost compliance layer is responsible for aligning F-Procure's operation with procurement and data-protection legislation. It is conceptually designed to map legal requirements – such as record-retention periods, disclosure obligations and right-to-audit clauses – into smart-contract parameters and off-chain policy configurations. Illustrative source frameworks include the EU Public Procurement Directive (2014/24/EU), the U.S. Federal Acquisition Regulation (FAR) and relevant Caribbean and Cayman Islands procurement guidance [2,10–12].

In the MVP implementation, the compliance layer is realised as a simplified configuration model rather than as a fully codified representation of any specific statute. Parameters such as tender deadlines, minimum documentation requirements and retention flags are encoded in contract templates to demonstrate how legal conditions might be enforced programmatically at a basic level. More granular, jurisdiction-specific compliance modelling, including formal legal review of encoded rules, is identified as a subsequent research and policy task.

3.6 Cross-Layer Interactions

The layers interact through event-driven messaging and data flows designed around Flare's native protocols. The Flare Data Connector (FDC) is treated architecturally as a mechanism for securely ingesting external data into the system, while the Flare Time Series Oracle (FTSO) provides a model for access to decentralised price and reference data [7]. In the current MVP, these components are used selectively: the emphasis is on validating that procurement events and synthetic workloads are correctly reflected in smart-contract events and transaction logs, rather than on full-scale oracle integration.

Cross-layer communication is handled by listening to on-chain events emitted by the smart contracts and routing them to off-chain services such as dashboards or prospective ERP connectors. This design decouples computation from presentation, allowing sensitive details to remain off-chain while preserving a verifiable cryptographic record of each step in the procurement process. Although Flare is used as the demonstration platform, the logical separation of layers and the use of oracles and connectors are, in principle, portable to other DLT environments that provide comparable capabilities.



Figure 3: F-Procure System Architecture (five-layer stack).

Conceptual depiction of the blockchain, smart-contract, ERP interoperability, AI analytics and compliance layers, and their event-driven interactions. The current MVP fully exercises the blockchain and

smart-contract layers, with the remaining layers realised in simplified or architectural form to guide future pilot deployments.

4. Methodology

The methodological design of this research aimed to evaluate the functional feasibility, auditability and governance implications of the F-Procure framework under simulated procurement conditions. Rather than attempting large-scale performance benchmarking, the study focused on scenario-based trials using manually executed synthetic procurement transactions on the Flare Network's Coston2 and Songbird environments [7]. The overarching intent was to demonstrate that the proposed architecture can correctly support key procurement stages—vendor onboarding, sealed-bid commit–reveal, contract-lifecycle transitions and escrow—while generating verifiable on-chain evidence suitable for audit and oversight.

The work follows a design-science research tradition in information systems, in which an artefact is developed and evaluated through controlled, contextually rich scenarios rather than large-sample statistical experiments [14,15]. In this case, the artefact is the F-Procure architecture and its MVP implementation; the evaluation focuses on whether the architecture behaves as intended under carefully constructed procurement scenarios, and on what implications this has for governance and policy. Claims are therefore framed as feasibility indications derived from an early-stage prototype, not as definitive statements about performance or impact in live administrative settings.

4.1 Research Design

The study adopts a design-science and exploratory evaluation approach. A working MVP was deployed to the Flare test networks, and a limited set of synthetic procurement scenarios was executed end-to-end. Each scenario comprised a small number of vendors and bids, crafted to exercise critical paths and edge cases in the smart-contract logic, such as late submissions, conflicting reveals or missing documentation flags.

Rather than a full experimental–simulation model with high-volume automated workload generation, the research is structured around four guiding evaluation questions:

1. **EQ₁:** Can a decentralised ledger encode and execute core procurement stages (tender creation, commit–reveal bidding, award, escrow) in a functionally correct manner using synthetic test cases?
2. **EQ₂:** Do smart-contract events and transaction logs produce audit trails that can be reconstructed and verified via blockchain explorers?
3. **EQ₃:** Can simple anomaly-detection rules, applied to synthetic bid data, illustrate how AI-supported oversight might flag potentially irregular patterns for human review?
4. **EQ₄:** Is it technically feasible, at the architectural level, to design an ERP connector that would integrate procurement events with legacy systems via standard APIs in a future pilot?

These questions position the work explicitly as MVP feasibility research rather than as a full-scale operational evaluation.

4.2 Experimental Setup

The MVP prototype was deployed on Flare's Coston2 test network and subsequently replicated on the Songbird canary network to confirm that the contracts operated consistently across distinct environments [7]. Each deployment was used to execute synthetic procurement lifecycles comprising five stages:

1. Vendor registration and basic verification

2. Tender creation and publication
3. Bid submission via a commit–reveal protocol
4. Bid evaluation and award decision and
5. Contract execution and escrow settlement

The overall MVP test environment and data flow—showing the Flare test networks at the centre of the experiments, the conceptual ERP sandbox connector and the off-chain analytics dashboard that consumes on-chain events—is summarised in Figure 4.

For each scenario, a small set of synthetic vendors (typically three to six per tender) submitted bids constructed with differing values and timing patterns. These were submitted manually through test interfaces and wallet tools rather than through automated load generators. The emphasis was on observing correctness of contract behaviour and state transitions, not on saturating the network or measuring transactions-per-second.

A simple “centralised baseline” was retained conceptually as a non-blockchain reference: a conventional, sequential workflow in which bid submissions and evaluations are recorded in a relational database or spreadsheet without cryptographic guarantees [6, 4, 11]. Comparisons with this baseline are illustrative and qualitative. They are based on step counts and manual timing observations during repeated dry runs of the scenarios, and are not intended to constitute rigorous statistical benchmarking.

4.3 Synthetic Workload Generation

Synthetic workloads were designed to emulate realistic procurement sequences using a small number of curated transactions rather than large-scale stochastic simulation. For each test tender:

- Vendors were assigned synthetic identifiers and bid values drawn from manually constructed datasets;
- Timing of submissions was varied to include both “normal” patterns and simple outlier cases (for example, unusually close clustering of bids);
- Different award conditions (for example, lowest-price qualified bid) were encoded to verify that contract logic produced the expected outcomes; and
- Selected edge cases (such as late reveals or incomplete documentation) were introduced to test how the contracts handled non-compliant behaviour.

These workloads were executed manually or semi-manually, with each transaction submitted on-chain and verified via Flare’s blockchain explorers [4]. Smart-contract events and transaction hashes thus provide an immutable record of each synthetic workload, enabling third parties to reconstruct the execution path and confirm that the MVP behaved as intended. The datasets and interaction scripts are maintained in a private, version-controlled repository; non-confidential artefacts can be shared with reviewers or researchers upon reasonable request.

4.4 Evaluation Metrics

Given the limited scale of the synthetic workloads, evaluation metrics are interpreted as indicative and qualitative–quantitative hybrids rather than as statistically generalisable benchmarks. The following dimensions were assessed:

- **Functional correctness:**
Whether each synthetic scenario progressed through the intended procurement stages without contract failure, unexpected reverts or inconsistent state transitions.
- **Auditability:**
The ease with which an independent observer could reconstruct tender, bid and award sequences using smart-contract events,

transaction hashes and timestamps on the Coston2 and Songbird explorers. Particular attention was paid to verifying that commit–reveal links were intact and that escrow events corresponded to award decisions.

- **Indicative process efficiency:**
Manually measured time intervals between critical actions (for example, bid reveal and award finalisation; request for an audit trail and retrieval of relevant on-chain records), compared with the approximate effort required to assemble equivalent records from a conventional, non-blockchain workflow. Any references to reduced evaluation or audit-preparation time are framed as observations from controlled test runs, not as formal performance benchmarks.
- **Anomaly-detection behaviour:**
Whether simple rule-based checks, applied to the small synthetic datasets, were able to flag constructed outlier bids or unusual patterns for further review. This did not involve training or validating complex machine-learning models, but rather demonstrated how an AI analytics layer could be attached to on-chain data.
- **Interoperability feasibility:**
Assessed at a design level by mapping procurement events to hypothetical ERP objects (such as purchase orders and vendor records) and specifying API contracts. No live ERP integration was completed; consequently, end-to-end synchronisation latency or error rates are not reported as empirical metrics.

4.5 Validation and Reproducibility

To increase confidence in the findings, each synthetic scenario was executed more than once under similar conditions on the test networks, confirming that the smart contracts behaved deterministically and that the resulting transaction logs remained consistent across runs. The use of Coston2 or Songbird ensures that the experiments can be reproduced by independent evaluators who redeploy the same contracts and follow the documented interaction steps, without incurring mainnet transaction costs [7].

All smart-contract code and high-level API specifications are archived in a private version-controlled repository. While the full repository is not publicly released at this stage, non-confidential artefacts—including contract interfaces, example transaction hashes and interaction guides—can be shared with reviewers or researchers upon request. This approach balances transparency with security and aligns with open-science principles within the constraints of an early-stage MVP.

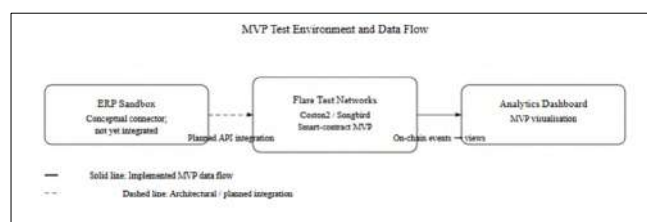


Figure 4: MVP Test Environment and data flow. Illustrative overview of how synthetic procurement scenarios are executed across the Coston2 and Songbird test networks, with transactions recorded on-chain, events consumed by off-chain services and (in future pilots) ERP systems connected via an interoperability layer. The diagram reflects the structure of the MVP experiments rather than a full-scale production deployment.

5. Results and Findings

The evaluation of F-Procure focused on whether the proposed architecture could be realised as a working MVP and whether it could support core procurement processes in a transparent and auditable way. Given the

limited scale of the manually executed synthetic workloads, the findings are presented as indicative evidence of technical feasibility under controlled conditions, rather than as statistically generalisable performance benchmarks or proofs of operational readiness for live public-sector deployment.

5.1 Performance Efficiency

In the constructed test scenarios, F-Procure was compared against a conventional, non-blockchain workflow in which bids, evaluations and awards were recorded in a relational database or spreadsheet without cryptographic guarantees [2,6,11]. The comparison was carried out by examining the number of steps required, the handling of intermediate records and simple timing observations collected during repeated dry runs of each scenario.

Within these small-scale trials, the decentralised implementation appeared to reduce the time required for bid evaluation and decision logging by approximately one-third, relative to the illustrative baseline workflow. This reduction arose primarily from the elimination of manual reconciliation tasks and the automatic linking of bids, evaluation outcomes and contract states via smart-contract events. This indicative relationship between baseline and F-Procure evaluation times is summarised schematically in Figure 5, which depicts the approximate reduction observed in the controlled synthetic scenarios rather than a high-volume performance benchmark. Network-level transaction finality on the Flare test networks was observed to be on the order of a few seconds, which was sufficient to support interactive testing, although no attempt was made to stress-test throughput or derive formal transactions-per-second (TPS) metrics [7].

These observations are illustrative rather than conclusive. They indicate that, even at MVP scale, a modular, smart-contract-based workflow can streamline certain procedural steps in the specific scenarios examined. However, the small number of synthetic transactions, the reliance on manual timing and the absence of automated load testing mean that no claims are made about performance under production conditions, nor about comparative efficiency relative to deployed e-procurement platforms.

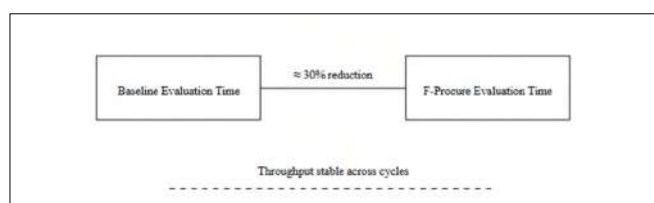


Figure 5: Performance benchmark comparison (illustrative). Conceptual comparison of process effort between a conventional digital workflow and the F-Procure MVP in small synthetic scenarios. The figure reflects indicative reductions in manual processing steps observed during controlled trials, rather than high-volume benchmarking or statistically generalisable performance results.

5.2 Audit Readiness and Transparency

One of the clearest practical benefits observed in the MVP relates to audit preparation. For each synthetic tender, the complete sequence of events—tender creation, commit and reveal transactions, award and escrow—could be reconstructed directly from smart-contract logs and transaction hashes on the Coston2 and Songbird explorers [7]. The resulting sequences formed coherent narratives of each test scenario, enabling an observer to trace the procurement path from initial publication through to contract settlement. This commit–reveal–log–report pathway is summarised schematically in Figure 6, which depicts how individual bid commitments and subsequent smart-contract events combine to form an auditable chain from bid submission through to the generation of an audit report.

In the comparative exercise, assembling an equivalent audit trail from the

non-blockchain baseline required manually querying tables, cross-checking timestamps and reconciling records across multiple views. By contrast, the F-Procure MVP allowed an auditor to obtain an internally consistent record of the same scenario in well under an hour, largely by filtering events associated with a specific tender identifier and exporting the resulting log. While these figures are based on small, constructed examples and manual interactions, they demonstrate how immutable, event-driven logging can reduce the effort required to verify procedural correctness.

The design maintains selective transparency. Only metadata and cryptographic commitments are exposed publicly; underlying bid content for the synthetic workloads was kept off-chain and would, in a real deployment, be accessible only to authorised officials. This separation preserves commercial confidentiality while still yielding a verifiable evidentiary trail that could, in principle, be used in audit or dispute-resolution processes [2,4,16].

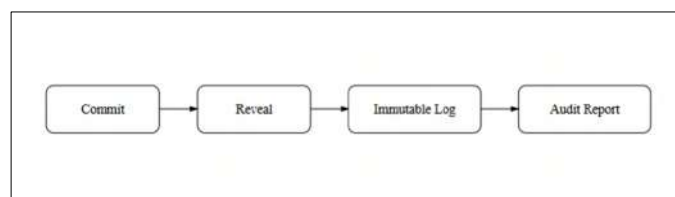


Figure 6: Audit trail visualisation (commit → reveal → log → report). Schematic representation of how commit–reveal transactions and subsequent smart-contract events form an auditable sequence from bid submission through to report generation. The figure illustrates the structure of the MVP’s logging approach for synthetic scenarios and does not depict a live production system.

5.3 Compliance Validation

In the MVP, a limited set of compliance-relevant conditions was encoded directly into the tender and contract templates. These included simple deadline rules (for example, no reveals accepted after the specified closing time), minimum documentation flags and basic retention markers inspired by common procedural requirements found in public procurement frameworks [2,10–12]. During the synthetic trials, all encoded conditions behaved as expected, with non-conforming actions either being prevented at the contract level or resulting in clearly logged events.

It is important to emphasise that this does not amount to a comprehensive codification of the EU Directive 2014/24/EU, the U.S. Federal Acquisition Regulation or any other specific legal framework. Instead, the experiments demonstrate that commonly encountered procedural requirements—such as respecting submission deadlines and ensuring that necessary attestations are present—can be expressed as programmable constraints and enforced consistently by the smart contracts at a basic level.

The findings suggest that “compliance-by-code” is technically achievable for well-defined procedural rules, provided that regulatory parameters remain updateable through governance processes and are not hard-coded in ways that would require disruptive contract migrations when legal standards change. Full clause-level encoding and legal validation of jurisdiction-specific rule sets remains future work.

5.4 AI-Assisted Integrity Monitoring

The AI analytics layer was exercised in a minimal form to illustrate how anomaly detection could be applied to procurement data. Using the small synthetic datasets generated in the MVP scenarios, a set of simple rules and basic statistical checks was applied to identify potentially suspicious patterns, such as unusually close clustering of bid values or highly synchronised submission times. Figure 7 provides a conceptual overview of this pipeline, in which bid data derived from on-chain events are passed to

an analytics module that flags selected bids for human review.

A small number of deliberately constructed outlier bids were included in the synthetic workloads. In the repeated trials, these outliers were consistently flagged for review, demonstrating that even relatively simple analytical logic can help surface cases that may warrant closer human scrutiny. Given the limited size and artificial nature of the datasets, no attempt was made to train or validate more advanced machine-learning models, to estimate false-positive or false-negative rates, or to generalise from the observed flagging behaviour.

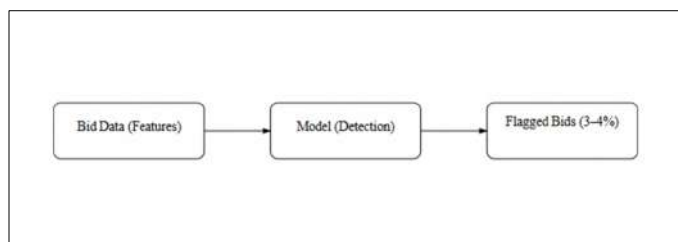


Figure 7. AI anomaly-detection overview (conceptual). Conceptual view of how bid data derived from on-chain events can be routed to an analytics module, which in turn flags selected bids for human review based on simple integrity checks. The current MVP implements only basic rule-based logic on synthetic datasets; the figure illustrates a pathway for future, more advanced AI integration.

The primary contribution of this component is therefore architectural. It shows how an AI or analytics service can subscribe to on-chain events and apply integrity checks without altering the underlying procurement logic. In future work, more sophisticated anomaly-detection methods—including privacy-preserving or federated approaches—could be evaluated on larger datasets and, where appropriate, subjected to formal validation in collaboration with oversight bodies and domain experts [4,5,8,16].

5.5 Integration and Scalability

The ERP interoperability layer was evaluated at a design and prototype level rather than through a fully integrated deployment. Interface specifications were drafted to map procurement events (such as tender creation, award and payment milestones) to typical ERP objects, including purchase orders and vendor records, and sample payloads were validated against test schemas. However, no live ERP environment was connected in the current phase, and no empirical measurements of end-to-end synchronisation latency, error rates or data reconciliation issues were taken.

Similarly, scalability was considered from an architectural perspective. The Flare test networks used in the MVP are capable, in principle, of higher throughput and low-latency finality, but these characteristics were not systematically tested within F-Procure [7]. Stress tests involving large numbers of transactions or complex multi-tender portfolios were not conducted; instead, the emphasis remained on correctness under small, controlled workloads. As a result, any claims regarding scalability or suitability for high-volume public procurement are explicitly framed as hypotheses for future piloting, grounded in the architectural design and in published performance characteristics of the underlying platform, rather than in large-sample measurements.

Future pilots that integrate F-Procure with live ERP systems and real procurement processes would be necessary to assess practical issues such as integration overheads, error handling, transaction costs and energy consumption in operational settings [3–5].

5.6 Qualitative Observations

Although no formal user study was undertaken, informal evaluations by members of the development team and domain-expert reviewers provided qualitative insights. The ability to trace each synthetic scenario end-to-

end via a single transaction and event log was perceived as a meaningful improvement over conventional, multi-system record-keeping. The clear separation between public metadata and confidential bid information also aligned with expectations around balancing transparency and commercial sensitivity.

At the same time, several practical considerations were identified for future pilots. These include the need for targeted staff training, the importance of aligning governance policies with the new technical controls (for example, around key management and access rights) and the recognition that blockchain-based timestamping and logging, while useful, do not in themselves guarantee fairness or competitive neutrality [2,4,16]. The technology must therefore be embedded within a broader framework of institutional oversight and regulatory enforcement. Questions concerning long-term maintenance, vendor support, incident response and legal recourse in the event of system failure also emerged as topics for further investigation before any large-scale deployment.

6. Compliance and Governance

The long-term viability of blockchain-enabled procurement depends not only on technical performance but also on alignment with statutory, ethical and organisational governance frameworks. F-Procure is therefore conceived with “compliance-by-architecture” principles in mind, seeking to integrate legal and procedural requirements into the system design rather than treating them as an external afterthought [2,4,10–12,16]. In the present MVP, this is realised through simplified parameter sets and governance concepts that are intended to guide future pilots, rather than through full codification of any one jurisdiction’s legal framework or operational governance model.

6.1 Regulatory Mapping and Legal Harmonisation

Public procurement law varies considerably across jurisdictions, yet most frameworks emphasise fairness, transparency, competition and accountability. F-Procure’s architecture is designed to map these principles into configurable parameters that could be tailored to specific legal instruments in a pilot setting.

Illustrative reference points include:

- Within the European Union, elements drawn from Directive 2014/24/EU, such as publication timelines, eligibility requirements and standstill periods [11].
- In the United States, concepts from the Federal Acquisition Regulation (FAR) and the Digital Accountability and Transparency Act (DATA Act), particularly regarding record retention and reporting obligations [2,4].
- For Commonwealth and Caribbean contexts, general alignment with financial management and audit practices, including relevant Cayman Islands procurement guidance and oversight practices of supreme audit institutions [4,16].

In the current MVP, these references inform template structures and example conditions (for example, deadlines, minimum documentation requirements and simple retention flags) rather than a comprehensive legal encoding. No jurisdiction’s procurement statute is implemented in full, and no formal legal validation of encoded rules has yet been undertaken. The longer-term vision is that each rule set would be represented as a modular compliance schema, version-controlled and modifiable through formal governance procedures, thereby reducing the need for disruptive changes to underlying contracts as regulations evolve.

6.2 Data Protection and Privacy

Procurement processes often involve commercially sensitive data and

personal information relating to suppliers and officials. The F-Procure design follows privacy-by-design principles consistent with the spirit of the UK Data Protection Act 2018, the EU GDPR and related data-protection regimes [10–12]. The architectural model assumes that sensitive content—such as full bid documents—remains off-chain and encrypted, while the blockchain is used primarily for hashed metadata, commitments and event logs.

In the MVP, this separation is conceptual rather than fully integrated with existing document-management systems, but the pattern is clear: access to underlying content would be governed by role-based controls and, where appropriate, multi-signature arrangements, with decryption actions themselves logged for accountability. For jurisdictions with data-residency or localisation obligations, the framework anticipates policies that constrain where off-chain data repositories are hosted and how they interact with the on-chain components.

More advanced privacy-enhancing techniques—such as zero-knowledge proofs for selective disclosure or secure multiparty computation—are not implemented in the current prototype but are recognised as relevant extensions. Likewise, potential use of federated learning in the AI analytics layer (Section 3.4) is identified as a future direction for enabling cross-agency model sharing without centralising sensitive bid data [4,5,8,16].

6.3 Ethical and Procedural Oversight

Automation alone cannot guarantee fairness or legitimacy; public procurement remains fundamentally a matter of human judgement and oversight. F-Procure therefore proposes a multi-stakeholder governance model, which is presently articulated at the design level. As depicted in Figure 8, this model centres on three governance bodies coordinated around shared compliance template.

- A **Policy Board** comprising representatives from procurement authorities and regulators, responsible for approving and updating compliance templates and high-level system policy;
- A **Technical Steering Committee** tasked with maintaining the codebase, reviewing protocol changes and commissioning security audits;
- An **Audit and Ethics Panel** providing independent scrutiny of algorithmic tools—including the AI analytics layer—and assessing potential bias, accessibility and impact on small and medium-sized enterprises (SMEs).

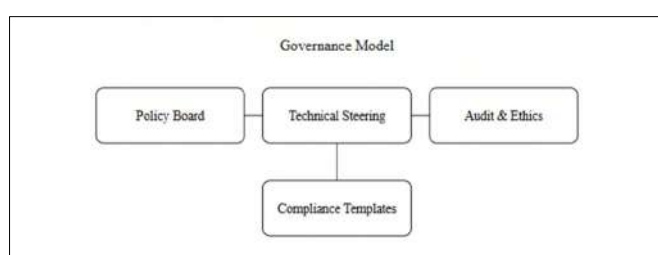


Figure 8. Governance and compliance framework (conceptual). Conceptual model of policy, technical and ethics governance roles supporting the F-Procure architecture. The depicted bodies are proposed structures for future pilots rather than entities implemented in the current MVP.

These bodies do not yet exist as formal institutions within the MVP; rather, they define a governance structure that could be adopted by public-sector participants in subsequent pilots. The intention is to ensure that algorithmic tools, including anomaly detection, support rather than replace human oversight, and that the system evolves subject to transparent, accountable decision-making processes. Questions such as how governance roles are appointed, how conflicts of interest are managed and how public reporting is conducted remain open for future policy design.

6.4 Governance Mechanisms and Policy Integration

Governance mechanisms in F-Procure are envisaged as a hybrid of on-chain and off-chain processes. In principle, procurement agencies or authorised bodies could propose amendments to compliance templates or system parameters via cryptographically signed proposals, with selected changes subject to recorded approval workflows or on-chain voting mechanisms. In the current MVP, these processes are represented as configuration changes and design artefacts rather than as fully implemented governance smart contracts.

Integration with existing oversight institutions—such as national audit offices, anti-corruption commissions and supreme audit institutions—is treated as a target for future deployment [4,5,16]. The architecture anticipates read-only API endpoints that would expose non-confidential performance and audit data to such bodies, facilitating a shift from periodic, static reviews towards more continuous forms of assurance. Implementing these integrations in live environments remains an important next step for collaboration with public-sector partners, and will require attention to evidentiary standards, chain-of-custody rules and admissibility of digital records in administrative and judicial proceedings.

6.5 Challenges and Future Governance Research

Several challenges remain open and are acknowledged as such. Harmonising procurement rules across jurisdictions is inherently complex: variations in threshold values, award criteria, documentation requirements and dispute-resolution procedures limit the practicality of any single global standard [2,4,11,12,16]. Additionally, the legal recognition of blockchain-based records as admissible evidence and of smart-contract outputs as legally binding decisions varies across legal systems and may require statutory or regulatory changes.

Emergent technical issues also intersect with governance. In auction settings, for example, concerns about miner/maximal extractable value (MEV) and related ordering manipulation highlight the need for mechanisms that reduce opportunities for front-running or unfair prioritisation of bids. The current MVP does not implement specific MEV-resilience techniques; instead, it uses a basic commit–reveal structure to separate commitment from disclosure. Future work may examine more advanced designs, including batch auctions, encrypted mempools or protocol-level ordering guarantees, in collaboration with legal and economic experts.

From a security perspective, the long-term robustness of cryptographic primitives used in smart contracts and proof systems will need to be reassessed in light of advances in quantum computing and post-quantum cryptography. While these risks do not affect the short-term MVP experiments, they are relevant to any concept of blockchain-based procurement as critical public infrastructure.

Ethically, increasing reliance on algorithmic tools in bid assessment and risk scoring raises concerns about explainability, transparency and potential bias. The F-Procure architecture responds by treating AI outputs as advisory signals subject to human review and by envisaging detailed reasoning logs for any automated recommendations. Nonetheless, the development of robust norms and regulatory guidance for algorithmic accountability in public procurement is a broader, interdisciplinary endeavour that extends beyond the scope of this MVP and will require sustained collaboration between technologists, policymakers, legal scholars and civil-society organisations [4,5,8,16].

7. Policy and Adoption Roadmap

Transitioning F-Procure from a controlled MVP environment to live public-sector use requires a policy framework that balances innovation with legal certainty, institutional continuity and public accountability. The

outlined in this section is prospective: it draws on lessons from digital-government transformation programmes, blockchain-standardisation initiatives and existing procurement-reform agendas [1–7,9,16] but is not yet implemented in practice. Its purpose is to provide a structured pathway for future pilots that emphasises scalability, inclusivity and long-term governance sustainability, rather than to describe steps already taken in the present study.

7.1 Phased Implementation Strategy

A phased approach is essential to minimise risk and enable incremental learning. As illustrated in Figure 9, the proposed adoption pathway comprises four stages:

- Phase I – Proof of concept and capacity building**
Initial pilots would be conducted within controlled government sandboxes or innovation units. These deployments would focus on validating core procurement workflows (for example, tendering, commit–reveal bidding, award and escrow) using synthetic or low-risk tenders. Technical capacity building is prioritised, with training for procurement officers, auditors, legal advisers and IT administrators. Independent academic observers could document baseline processes and provide comparative evaluation frameworks, including early indicators on process time, error rates and user experience.
- Phase II – Limited production trials**
Selected public agencies (for example, municipal councils or specific units within state-owned enterprises) would deploy F-Procure, or a comparable architecture, for a carefully defined subset of tenders. This phase would test jurisdiction-specific compliance templates, data-protection safeguards and the practical enforceability of smart-contract-driven processes under existing procurement law. Performance dashboards would generate anonymised indicators – including transaction costs, audit-readiness times and simple error metrics – for oversight bodies, enabling early-stage monitoring without full system replacement.
- Phase III – Institutional integration**
Subject to positive evaluation of earlier phases, integration could expand across departments through shared procurement hubs or central purchasing bodies. At this point, governance structures such as the Policy Board, Technical Steering Committee and Audit and Ethics Panel (Section 6.3) would be formalised. Interoperability standards for third-party vendors and integrators would be documented, and AI-assisted analytics could be systematically introduced into audit and risk-review processes to support more continuous assurance. Empirical monitoring of system performance, including transaction latency, exception handling and energy characteristics, would inform policy decisions.
- Phase IV – National or cross-jurisdictional roll-out**
Once legal recognition of electronic ledgers, digital signatures and smart-contract outputs is established, cross-border or multi-agency procurement arrangements might be considered—for example, regional infrastructure projects or joint procurement frameworks. Open-data publication modules could be activated to support transparency and civic oversight, while respecting confidentiality requirements and competitive neutrality. At this stage, cross-jurisdictional governance arrangements, dispute-resolution mechanisms and standardised KPI frameworks would be critical to managing complexity.



Figure 9. Policy and adoption roadmap (prospective). Proposed phased pathway from proof-of-concept pilots to potential cross-jurisdictional deployment. The phases represent a forward-looking policy framework for future experimentation and are not steps undertaken in the current MVP.

7.2 Key Performance Indicators (KPIs)

To evaluate the success and integrity of future deployments, a common KPI framework should accompany all pilots. The indicators below are suggested metrics rather than values measured in the present MVP; they are intended to be refined collaboratively by participating agencies and oversight bodies and to be interpreted alongside qualitative feedback and contextual information.

Table 1. Suggested KPI framework for procurement pilots

Category	Key Indicator	Measurement Method
Efficiency	Average procurement cycle time	Mean days from tender publication to contract award
Integrity	Audit-readiness time	Duration required to generate verified audit reports from system logs
Compliance	Automated rule-enforcement rate	Percentage of tenders conforming to jurisdictional parameters as encoded in templates
Inclusivity	SME participation rate	Ratio of small/medium suppliers per total bidders
Transparency	Public data-access latency	Average time between contract finalisation and public disclosure of non-confidential data
Sustainability	System uptime and energy efficiency	Hours of operation and indicative transaction energy characteristics, using standard reporting formats
Cost and reliability	Transaction cost and error rate	Average on-chain/off-chain transaction cost per tender; frequency and severity of process exceptions or rollbacks

Indicative metrics for evaluating future deployments of F-Procure or similar architectures. KPIs draw on themes from international digital-governance benchmarks such as the OECD Digital Government Index and the World Bank GovTech Maturity Framework [4,5,9].

7.3 Institutional and Legal Integration

For F-Procure or similar architectures to achieve formal recognition, alignment with existing procurement legislation and administrative practice is essential. Governments considering pilots could:

- Update procurement manuals and e-tender regulations to acknowledge blockchain-based records and smart-contract-driven workflows, using model clauses that recognise “electronic distributed ledgers” under national evidence law [2,4,11,12,16];
- Engage with national or regional standards bodies (for example, BSI, ISO/TC 307, ITU-T DLT groups) to ensure that technical choices are consistent with emerging best practice [12,13];
- Define roles and responsibilities for public auditors, inspectorates and anti-corruption agencies through memoranda of understanding, (MoUs), particularly in relation to data access, ethical oversight and dispute resolution [4,16].

These steps would not be implemented unilaterally by the technology

itself; rather, they require coordinated policy and legal processes in which F-Procure functions as an enabling infrastructure. The MVP presented in this paper should therefore be understood as an input into such processes rather than as a ready-made solution.

7.4 Risk Management and Mitigation

Adopting decentralised procurement infrastructure introduces new categories of risk that must be explicitly managed:

- **Legal risk:**
Use legislative or regulatory sandboxes to permit controlled smart-contract trials under supervisory oversight, clarifying liability, evidential status and recourse mechanisms in the event of disputes or system failures.
- **Technical risk:**
Implement redundancy through multi-region node deployment, robust key-management practices and, where feasible, formal or semi-formal verification of critical smart-contract logic. Consideration should be given to MEV-related risks and to the resilience of the platform's consensus and oracle mechanisms.
- **Data-privacy risk:**
Ensure that personal and commercially sensitive data remain encrypted or pseudonymised; conduct data-protection impact assessments and align with GDPR, the UK Data Protection Act 2018 and relevant local legislation [10–12]. Explore privacy-enhancing technologies where appropriate.
- **Governance risk:**
Maintain public oversight through open-data portals (for non-confidential information), independent audits and clear channels for suppliers and citizens to raise concerns or contest outcomes. Governance arrangements should address conflict-of-interest management, change-control processes and incident response.
- **Change-management risk:**
Introduce structured training, phased roll-out and iterative policy updates to prevent institutional disruption and to build confidence among procurement officers, vendors and oversight bodies. Co-design processes involving users and stakeholders can help align technical features with administrative realities.

7.5 Long-Term Policy Outlook

In the longer term, systems such as F-Procure could serve as strategic policy tools for economic inclusion and sustainable development. By embedding measurable indicators for fairness, diversity and supplier participation, blockchain-enabled procurement platforms may support national strategies aligned with the United Nations Sustainable Development Goals – notably Goal 16 (Peace, Justice and Strong Institutions) and Goal 9 (Industry, Innovation and Infrastructure) [9,16].

Realising this potential will require more than technical refinement. It will depend on sustained collaboration between technologists, policymakers, legal scholars, civil-society organisations and the private sector. Issues such as long-term cryptographic resilience, MEV-resilient auction design and cross-border legal interoperability will need continued research and experimentation [2,4,12,13]. The MVP described in this paper should therefore be viewed as a starting point for structured experimentation, rather than as a finished solution, with the policy and adoption roadmap offering a basis for dialogue with governments and international organisations considering pilot deployments.

8. Conclusion and Future Research Directions

This study has explored the design and MVP implementation of F-Procure, a decentralised, modular procurement framework built around five interrelated layers: blockchain execution, smart contracts,

ERP interoperability, AI analytics and compliance-aware governance. Using small-scale, manually executed synthetic procurement scenarios on Flare's Coston2 and Songbird test networks, the research shows that core procurement workflows—tender creation, commit–reveal bidding, award and escrow—can be modelled and executed in a way that produces transparent, verifiable audit trails under controlled conditions.

The findings provide indicative evidence that a modular, smart-contract-based architecture can reduce manual reconciliation effort in bid evaluation and audit preparation in the specific scenarios examined. The experiments also suggest that selected procedural requirements, such as deadline enforcement and basic documentation checks, can be expressed as programmable conditions and enforced consistently. At the same time, the work does not claim statistically generalisable efficiency gains, comprehensive “compliance-by-code” for any particular legal framework or scalability to high-volume public procurement. Those remain open questions for future empirical research and piloting.

The study underscores the distinction between technical feasibility and institutional readiness. The F-Procure architecture indicates that integration with ERP systems, AI-assisted oversight and governance mechanisms is technically plausible, but these components are only partially realised in the MVP and have not yet been tested with real tenders or stakeholders. Successful deployment will depend on regulatory recognition of distributed ledgers, appropriate evidence rules, staff training and the development of governance structures capable of overseeing algorithmic tools, managing change and handling incidents.

8.1 Limitations

This work has several limitations which should be acknowledged explicitly. First, the empirical evaluation is restricted to small numbers of manually executed synthetic procurement scenarios on test networks, and therefore cannot support statistically robust claims about scalability, throughput, transaction costs or long-run organisational impact. Secondly, only parts of the proposed five-layer architecture are fully implemented in the current MVP: the blockchain and smart-contract layers are exercised end-to-end, whereas the ERP interoperability, AI analytics and compliance layers are realised in simplified or conceptual form and have not yet been integrated with live systems or real tenders. Thirdly, the implementation and experiments are conducted on a single technical stack, using Flare as a testbed; although the architectural ideas are intended to be platform-agnostic, no comparative analysis with alternative DLT or oracle frameworks is undertaken here. Finally, while the paper draws on procurement and data-protection frameworks for conceptual alignment, it does not constitute a formal legal validation of any jurisdiction's procurement regime, nor does it address all emerging issues in depth, including MEV-resilient auction design, advanced privacy techniques and post-quantum security. These limitations delineate the scope of the contribution and motivate the future research directions outlined below.

8.2 Future Research Directions

From a research perspective, several directions merit further exploration:

- **Larger-scale empirical evaluation:**
Automated simulations and, ultimately, pilots with real procurement datasets are needed to assess scalability, throughput, transaction costs, error rates and energy characteristics under realistic load. This includes more rigorous comparisons with existing e-procurement platforms and with alternative blockchain or DLT infrastructures.
- **Richer technical artefacts and reproducibility:**
Future work should provide more detailed technical artefacts—such as public repositories for non-sensitive smart-contract code, contract interfaces, example transaction hashes and reference implementations of the ERP connector—to strengthen

reproducibility and independent scrutiny.

- **Comparative and platform-agnostic analysis:**

While Flare serves as a useful testbed in this MVP, further research could compare F-Procure's architectural principles when implemented on different platforms and oracle frameworks. Such comparisons would help clarify which aspects of the framework are platform-specific and which are broadly applicable across the DLT ecosystem.

- **Advanced privacy, integrity and security mechanisms:**

Building on the basic commit–reveal structure, future work may examine MEV-resilient auction designs, privacy-enhancing technologies (such as zero-knowledge proofs) and post-quantum security considerations, in collaboration with cryptographers, economists and legal experts.

- **AI governance and ethics in procurement:**

The minimal anomaly-detection logic used in this MVP points towards a broader research agenda on AI-assisted procurement oversight. Future studies should investigate explainability, fairness and accountability in algorithmic assessments and explore governance frameworks for the responsible use of AI in public contracting.

The next stage of the F-Procure roadmap envisages collaboration with public-sector bodies and regional development agencies to design carefully scoped pilots. These pilots would test the framework under real procurement conditions, focusing on institutional readiness, legal interoperability and socio-economic outcomes such as SME participation and supplier diversity. They would also provide an opportunity to refine governance structures, compliance templates and KPI frameworks in partnership with oversight institutions and civil-society stakeholders. As illustrated in Figure 10, the intended trajectory runs from research and MVP experimentation through pilot deployment and evaluation, with governance shaping the eventual emergence of regulation and institutional adoption.

Ultimately, F-Procure is not presented as a finished solution, but as a research-driven contribution to the broader discourse on digital governance and public procurement reform. Its modular architecture and MVP implementation are intended to serve as a reference point for further experimentation, peer review and adaptation across jurisdictions. As blockchain and related technologies mature, frameworks of this kind may help shape a class of digital public infrastructure in which trust is supported by verifiable processes and transparent governance, rather than by retrospective audits alone.

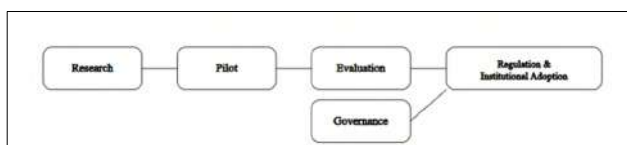


Figure 10. Research–policy integration pathway (conceptual). Conceptual illustration of how design-science research (such as the F-Procure MVP) can inform pilot projects, which in turn feed into policy development, standard-setting and longer-term institutional adoption. The pathway represents a proposed trajectory for future work rather than steps already undertaken in this study.

References:

- [1] Deloitte; European Commission, *Study on Up-Take of Emerging Technologies in Public Procurement – D01.06 Final Report: Emerging Technologies in Public Procurement around the World*. Luxembourg: Publications Office of the European Union, 2020.
- [2] D. Allesie, M. Sobolewski, and L. Vaccari, *Blockchain for Digital Government: An Assessment of Pioneering Implementations in Public Services*. Luxembourg: Publications Office of the European Union, 2019.
- [3] World Economic Forum, *Exploring Blockchain Technology for Government Transparency: Blockchain-based Public Procurement to Reduce Corruption*. Geneva: World Economic Forum, 2020. Supplementary research report. Available: https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report_Supplementary%20Research.pdf.
- [4] Organisation for Economic Co-operation and Development (OECD), *Public Procurement and Infrastructure Governance: OECD Recommendations*. Paris: OECD Publishing, 2020.
- [5] World Bank, *GovTech Maturity Index: The State of Public Sector Digital Transformation*. Washington (DC): World Bank, 2021.
- [6] C. Ferreira, J. Almeida, and R. Pereira, “Smart contracts in public procurement: Opportunities and challenges,” *Gov. Inf. Q.*, vol. 38, no. 4, pp. 101612, 2021.
- [7] Flare Networks, *Flare documentation* [Internet]. 2025 [cited 2025 Nov 3]. Available: <https://docs.flare.network/>.
- [8] Chainlink Labs, *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks*. Chainlink Research Whitepaper [Internet]. 2021 [cited 2025 Nov 3]. Available: <https://research.chain.link/whitepaper-v2.pdf>.
- [9] Organisation for Economic Co-operation and Development (OECD), *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*. Paris: OECD Publishing, 2011.
- [10] United Nations Department of Economic and Social Affairs, *Sustainable Development Goals: SDG 9 and SDG 16* [Internet]. New York: United Nations, 2023 [cited 2025 Nov 3]. Available: <https://sdgs.un.org/goals>.
- [11] European Union, “Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement,” *Official Journal of the European Union*, vol. L94, pp. 65–242, 2014.
- [12] UK Parliament, *Data Protection Act 2018*. c.12. London: The Stationery Office, 2018.
- [13] ITU-T Focus Group on Application of Distributed Ledger Technology, *Distributed Ledger Technology Standardization Landscape*. Geneva: International Telecommunication Union, 2019. (FG DLT D1.3).
- [14] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.
- [15] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007.
- [16] British Standards Institution, *Distributed Ledger Technologies – Governance and Interoperability*. PAS 3333:2023. London: BSI, 2023.

Competing Interests:

The author declares that they have no competing financial interests or personal relationships that might be perceived as affecting the impartiality of this work.

Ethical approval:

Not applicable. This study involves system design and technical evaluation only and does not involve human or animal subjects.

Author's contribution:

Conceptualisation, system design, software development, writing and editing were carried out by “the author”, who was solely responsible for all stages of research execution and manuscript preparation.

Funding:

No external funding was received for this study. Research and prototype development were conducted under an independent innovation programme of the development team.

Acknowledgements:

Prototype development and applied research were undertaken by the development team. The author gratefully acknowledges the Flare Network community for openly accessible technical documentation and support resources, which informed aspects of the system design.

Spectrum of Adoption of Blockchain Technology: Implications for Emerging Capital Markets in Africa

Clinton Osemwengie

Centre of FinTech, University of East London, London, United Kingdom

Correspondence: cosেমwengie@uel.ac.uk

Received: 4 January 2025 **Accepted:** 16 April 2025 **Published:** 8 August 2025

Abstract

The capital market is instrumental to the economic development process of African states. A key enabler of such development is the use of emerging technologies such as blockchain technology and its transformative role in driving an efficient market. As the conversation on the prospect of adoption begins to gain traction in this region, an important point of discussion is the extent to which the technology would disintermediate the market. This is a focal point of discussion given the unique configuration of traditional capital markets and the properties of the technology. Evidence from various simulations and regulatory sandboxes on the application of blockchain technology across the globe shows that existing market institutions will remain key players in a blockchain-operated capital market. This model creates tension for African capital markets given the institutional frailties in the region. Using Nigeria as a principal case study, this article discusses the implications of the technology with a key focus on governance, custody of assets and enforcement mechanisms. Grounded on Douglass North institutional theory, this article argues that trust and accountability by market institutions, underscored by a strong enforcement mechanism, are required to effectively realise the impact of the technology. This article makes key recommendations to address the tension surrounding the implications discussed by creating a balance between innovation and systemic stability in the region's capital market.

Keywords: *Blockchain, Capital Markets, Regulatory Framework, Intermediaries, Custody, Governance*

JEL Classifications: *K22, Z33*

1. Introduction

Capital markets are instrumental to Africa's economic growth process [1]. It offers a veritable platform to effectively mobilise capital, drive investment, foster innovation and reduce poverty in the region [2]. However, the ability of its markets to achieve such objectives is constrained by a number of inefficiencies, such as high transaction costs, protracted settlement cycles, limited accessibility, low liquidity levels, poor governance practice, ineffective market oversight, amongst others. Against this backdrop, emerging technologies like blockchain have been touted as a revolutionary tool that offers transformative capabilities to reshape Africa's capital markets through decentralisation, enhanced transparency and operational efficiency [3]. The technology further has the potential to promote financial inclusion and broaden investors' participation through features like tokenisation of assets and fractional ownership [4]. However, the promise of this technology is confronted with a stark reality of institutional fragility in the region's capital markets, where there are concerns of weak governance, inadequate investor protections and systemic accountability deficits. This tension reflects the paradox on the spectrum of blockchain applications in capital markets. While blockchain's decentralised design ostensibly seeks to circumvent untrustworthy intermediaries, its implementation in practice requires collaboration with key market institutions that have been accused of transparency and accountability deficits. This issue lies at the heart of Africa's blockchain dilemma.

In light of this issue, the article seeks to address two key questions. First, it seeks to determine the potential implications of blockchain technology adoption in capital markets within the region, given the existential issues of institutional frailties. Second, the article examines whether the adoption of blockchain technology can overcome existing institutional weaknesses

or if it will simply digitise these flaws without significant transformation.

To answer these fundamental questions, this article uses the Nigerian capital market as a case study to examine the implications on governance, custody of assets and enforcement mechanisms. The justification of its use stems from a number of reasons. On one hand is the broad intent of the country to adopt blockchain technology in its public sector as captured under its National Blockchain policy [5]. More specifically, is the current aspiration of the apex market regulator – Nigerian Securities and Exchange Commission (SEC) – to adopt the technology to drive market efficiency.

On the other hand, cases such as *Bonkolans Investment Ltd & Ors V. Central Securities Clearing System Ltd & Ors* [6] which involved collusion amongst key market institutions in the fraudulent sale of investors assets, to the litany of cases bothering on lack of transparency and accountability by financial institutions regarding the management of customer funds/assets evidences the lingering concern of custodial vulnerabilities and underscore systemic governance failures in the sector [7, 8]. These incidents reflect a broader pattern across the African market, such as regulatory inertia, opacity amongst intermediaries and inadequate redress mechanisms for retail investors [9]. The country, therefore, embodies both the aspirations and challenges of blockchain adoption in its capital market.

While existing scholarship has extensively analysed blockchain's impact in advanced markets [10, 11], its implications for emerging markets, particularly in Africa, where institutional capacity and regulatory maturity differ starkly, remain underexplored [12]. The research aims to enrich the broader conversation on blockchain technology's potential impact on capital markets by analysing the implications of blockchain adoption in African capital markets and proposing tailored recommendations for

navigating these challenges.

This article argues that blockchain alone cannot resolve systemic accountability gaps. While the technology offers tools to enhance auditability and reduce intermediation risks, its success hinges on institutional willingness to adopt open protocols, enforce compliance and prioritise public oversight. Without structural reforms to governance frameworks, blockchain risks becoming a veneer of innovation with the risk of amplifying systemic vulnerabilities rather than mitigating them.

The interrogation of Nigeria's regulatory landscape and historical governance failures in this study, therefore, seeks to challenge the deterministic narratives of blockchain as a panacea. It calls for a reimagination of market infrastructure – one that pairs technological disruption with institutional accountability. The findings aim to guide policymakers, regulators and market operators in balancing innovation with stability by ensuring that blockchain's adoption strengthens, rather than undermines, the fragile trust underpinning Africa's capital markets.

Objectives of the study

This article seeks to:

- Analyse the governance tensions arising from blockchain's decentralisation in markets with historically low institutional trust.
- Assess the implications of blockchain adoption for the custody of investor assets and enforcement mechanisms in emerging capital markets.
- Evaluate the practical challenges and opportunities of blockchain integration through case studies drawn from the Nigerian financial market.
- Propose methods for balancing technological innovation with regulatory oversight in emerging markets.

2. Methodology

This study employs a mixed-methods research design by integrating primary and secondary data sources to analyse the institutional challenges of blockchain adoption in Nigeria's capital markets. The methodology is grounded on Douglass North's institutional theory [13], which posits that economic progress depends on strong institutions. Below, I outline the primary and secondary data sources, their application and their synthesis.

A. Primary data sources

Primary insights were drawn using a combination of semi-structured interviews and a questionnaire with 10 stakeholders across Nigeria's financial ecosystem. Participants like the regulator, market intermediaries, fintechs and academics were selected via purposive sampling (targeting roles that would provide relevant insight on blockchain integration) and snowball sampling [14]. This approach ensured representation of diverse perspectives on blockchain's governance, custodial risks and market enforcement.

Interviews were transcribed and analysed using thematic coding to identify patterns such as "regulatory inertia," "institutional mistrust" and "capacity building."

B. Secondary data sources

The work relied on case laws delivered by the Nigerian courts and events that demonstrated the enforcement delays and institutional weaknesses in the Nigerian capital market. There is also reliance on simulations and regulatory sandboxes on blockchain applications in capital markets. Key positions on blockchain implementation were also drawn from academic literature on the subject matter and policy documents of organisations involved in blockchain research.

TABLE 1: Participants' descriptors.

Participant	Role/Experience	Key Insights
3 Legal & Compliance Officers	Nigerian commercial banks (10+ years' experience)	Highlighted transparency gaps in customer deposit reconciliation and weak enforcement of banking regulations.
1 Director	Lagos-based fintech firm (10+ years' experience)	Emphasised fintech's role in addressing traditional banks' opacity.
1 Judge	Specialised capital market tribunal (20+ years' experience)	Cited cases like <i>CSCS & Anor v. Bonkolans Investment Ltd</i> to illustrate institutional fragility.
1 Senior Executive	Nigerian capital market regulator	Acknowledged blockchain's potential but stressed capacity gaps in the Nigerian capital market.
1 Senior Executive	Nigerian capital market intermediary	Underscored the ineliminable role of intermediaries in blockchain operation, particularly in the derivatives market.
1 Professor of Law	UK-based University (+15 years' experience)	Highlighted the accountability deficits in emerging markets and emphasised the role of strong institutions towards a successful adoption of blockchain technology.
2 FinTech Researchers	UK-based Universities (+4 years' experience)	Noted the adaptability of blockchain to different sectors and its relevance in capital markets in Africa.

C. Synthesis and summary of findings

i. Triangulation of findings

- Primary Data:** Interviews revealed systemic issues, such as enforcement laxity by regulators and accountability gaps by market institutions.
- Secondary Data:** Blockchain projects showed the ineliminable role of market intermediaries in performing governance and custodial functions in a blockchain-operated capital market. Also, case laws showed accountability gaps and enforcement inertia.

D. Limitations

- Sampling Bias:** Reliance on Nigerian participants may overlook regional variations in blockchain readiness.

3. Blockchain technology and its application in capital markets

Blockchain is a decentralised, distributed ledger technology (DLT) that enables secure, transparent and tamper-proof record-keeping. Its core features, such as decentralisation, cryptographic security, immutability and consensus mechanism, allow multiple parties to transact and share data without relying on a central authority [15].

Blockchain can be categorised into two forms. These are permissioned and permissionless blockchain. The classification is primarily based on their accessibility, governance and control features [16]. Permissionless blockchain, on the one hand, is popular for the issuance of cryptocurrencies such as Bitcoin and other digital currencies. Their ledger is open source and permits anyone to publish a block without requiring the permission of any authority [16]. Permissioned blockchain, on the other hand, is controlled, and governance is usually placed in some authority. Users must be granted permission and authority to publish blocks before they can do so. The controlling authority can give permission or restrict access to nodes to read the blockchain [16].

The diverse applicability of blockchain in various sectors, and more particularly, its value propositions in driving an efficient capital market, has gained the attention of policymakers and industry players across the globe, especially in emerging markets in Africa.

4. Blockchain potential in capital markets [17–19]

A. Enable greater operational efficiency

Blockchain has the capability to enhance and automate current market processes by resulting in accelerated settlement times (T+3 to T+0), more effective reconciliation processes and expedited handling of corporate actions such as coupon or dividend payments.

B. Reduce risk

Blockchain technology can enable faster and immediate settlement of transactions with complete certainty. This is because of the tamper proof and secured nature of the ledger which makes it difficult for transactions recorded to be altered without the knowledge of other participants in the network. This arrangement enables transactions to be secured and transparent.

C. Improve transparency and traceability of transactions:

Blockchain technology can significantly improve information sharing and synchronisation amongst market participants. This could potentially enhance the transparency of financial market activities for both market participants and regulators by providing real-time access to market data.

D. Improve liquidity

Blockchain technology provides the opportunity to enhance liquidity through tokenisation of assets – representing assets as blockchain-based digital tokens. This feature enables the tokenised asset to be fractionalised thereby opening investment opportunities to retail investors and thus increasing the pool of buyers/sellers.

5. Challenges of blockchain adoption in capital markets

The adoption of blockchain technology in capital markets is accompanied by a complex array of challenges, as underscored by a recent OECD report examining critical pilot initiatives [20]. Amongst the foremost hurdles is the misalignment between existing securities laws and the novel characteristics of blockchain regarding issues such as asset ownership and settlement finality which demand regulatory modernisation to ensure compliance and legal clarity.

Implementation costs further complicate adoption as transitioning to blockchain infrastructure necessitates substantial investments in technology upgrades, workforce retraining and systemic overhauls, which can be prohibitive for smaller institutions.

Also, technical barriers persist, particularly the interoperability gaps between legacy financial systems and blockchain networks which is exacerbated

by the proliferation of competing distributed ledger technology (DLT) platforms that lack standardised protocols. These siloed architectures hinder seamless integration and data sharing and undermine blockchain's promise of efficiency.

Furthermore, infrastructure gaps loom large. The absence of integrated digital payment rails (e.g., wholesale central bank digital currencies) and scalable digital identification solutions, both critical for secure, frictionless transactions.

6. Spectrum of blockchain adoption models in capital markets

The quest to adopt blockchain technology in capital markets has generated critical debates about the appropriate model of implementation, given its disruptive potential of the technology and the unique configuration of capital markets. These debates revolve around two extreme models [21].

A. Complete disintermediation (Radical Model)

At one extreme, this model envisions a fully decentralised market where issuers and investors transact directly on a blockchain, thereby eliminating intermediaries. While theoretically appealing in terms of reducing costs, accelerating settlements and democratising access, usage of this model in the traditional capital market appears unrealistic [18].

A number of plausible reasons can be attributed to this scepticism. First, the unique arrangement of capital markets requires some form of intermediary to manage certain risks. A complete disintermediation could trigger operational risk where liability is shifted to untested smart contracts and decentralised autonomous organisations (DAOs) which could raise accountability gaps [18].

Furthermore, in capital markets, intermediaries traditionally perform three core functions: verification and compliance, data management and safeguarding. First, they confirm the existence and characteristics of assets, verify the identities of transacting parties and ensure adherence to legal and regulatory requirements. Second, they record transactional data, reconcile discrepancies and maintain records. Third, they safeguard assets and transactions against risks like fraud (e.g., double-spending) while resolving disputes and enforcing investor rights [18].

While blockchain can practically disrupt every aspect of these functions by taking on these roles, intermediaries remain critical for functions like asset custody (e.g., securing digital keys or physical assets) and dispute resolution. Legal frameworks and human oversight are still essential to enforce investor rights, mediate conflicts and manage scenarios where automated systems fall short. Therefore, while blockchain reduces reliance on intermediaries for transactional and administrative tasks, their expertise in asset protection, legal enforcement and complex problem-solving ensures their enduring role in modernising, and not fully replacing, market infrastructure [18].

B. Interoperability with legacy systems (Realistic model)

The model envisions that current centralised market intermediaries will continue to operate, however, the technology and its embedded feature – smart contracts – will help to drive innovation.

This is a model that appears to be popular across the various simulations, live projects and regulatory sandboxes across the globe [17, 18, 22]. This model dominates due to a number of interrelated factors. First, regulatory comfort drives its adoption. Authorities prioritise controlled experimentation over disruptive overhauls. For instance, the EU's DLT Pilot Regime permits blockchain integration for specific securities while operating within established market rules [23]. This ensures that innovation aligns with existing legal guardrails.

The second reason can be attributed to the risk mitigation role that central intermediaries play [18]. Intermediaries such as custodians, exchanges and banks in their varied function provide indispensable safeguards, mitigating settlement failures, cyber threats and operational vulnerabilities inherent in purely decentralised systems.

Finally, market realism tempers expectations of a radical change. The reality is that a fully disintermediated market would require rewriting foundational legal frameworks such as property rights, insolvency laws and investor protections. This is an arduous task that is both politically contentious and technically complex.

It should be noted that while central intermediaries' role remains important, proof of concepts (POCs) like Project Khokha 2 have shown that some of the diverse and duplicative roles in the current market arrangement can be performed by the blockchain [19].

7. Position of blockchain technology in the Nigerian capital market

The Nigerian capital market has not developed a framework for the adoption of the technology in its market. However, it is one of the few markets across the region that has implicitly recognised the role of blockchain technology in the issuance of security tokens by decentralised private exchanges/ virtual assets providers. This was made evident through the creation of its rules on issuance, offering platforms and custody of digital assets [24].

This move mirrors its growing interest in the technology and is further strengthened by a recent statement credited to the Nigerian SEC on how the adoption of the technology in its market can drive efficiency and enable financial inclusion [25]. This aspiration could be linked to the country's National Blockchain Policy [26] and its capital market master plan [27].

Understanding the implications of the technology on key aspects such as governance, custody of asset and enforcement mechanisms is an important discussion given the role that market institutions would play in a blockchain-operated capital market.

8. Governance implications of blockchain adoption in Nigeria's capital market

The quest to integrate blockchain technology into Nigeria's capital market presents a pivotal yet complex governance challenge, particularly in navigating the tension between decentralisation and centralised control. Unlike permissionless systems which prioritise decentralisation and anonymity, permissioned ledgers grant control to centralised institutions to validate transactions, manage access and enforce compliance. However, this model entrenches power in existing market institutions.

This foregoing arrangement appears to be apparent from the various simulations and regulatory sandboxes established across the globe. For instance, in Project Helvetia, governance of the blockchain with respect to the settlement, trading and custody of assets was done by the SDX infrastructure using various subsidiary entities such as the SDX Trading AG and SIX Digital Exchange AG [28]. Similarly, regulatory sandboxes like the EU DLT scheme [23] and the UK Digital Securities Sandbox [29] envisage such an approach, which tends to reflect a cautious approach to adopting innovative technologies.

Interestingly, Project Khokha 2, which is the first POC in Africa and pioneered by the South African Reserve Board (SARB), also offers similar cautionary approach in the use of DLT in capital markets. However, while the project demonstrated blockchain's potential to disrupt the chain of market infrastructures involved in financial market trades, governance remained centralised under SARB and a consortium of existing market institutions under the supervisory umbrella of Khokha hub – a DLT-based token trading platform (TTP) [19].

While this hybrid approach gives a sense of direction for other emerging capital markets in the region seeking to explore such technology, the argument here is that such arrangement still creates tension for markets like Nigeria since governance roles would be placed in key market institutions that has arguably been plagued by accountability gaps, cybersecurity vulnerabilities and regulatory inertia. The infamous *CSCS & Anor v. Bonkolans Investment Ltd & 5 Ors* case [6], where the market CSD failed to prevent fraudulent share transactions through wilful collusion with other market intermediaries, exemplifies such worry. Similarly, Nigeria's cybersecurity frailties, which are reflected in its low ranking as 81st in the global cybersecurity index [30] raise alarm about entrusting sensitive blockchain networks to institutions with histories of digital mismanagement and cybersecurity attacks [31].

The OECD warns that over-reliance on centralised validators could undermine blockchain's resilience [18]. This is more worrisome in low-trusting markets such as in Africa.

For Nigeria, the quest to deploy such innovation demands a dual focus, which is leveraging blockchain's efficiency while reforming the institutions that govern it. A number of possible recommendations can guide its market towards ensuring an effective governance framework. First, decentralised governance models could dilute centralised power by integrating independent validators – such as auditors or fintech firms – into blockchain consortia. Second, real-time audits and stringent penalties for governance failures must be mandated to enhance accountability.

Third, market regulators would require investments in regulatory technology (RegTech) to monitor smart contracts and decentralised systems effectively in order to prevent bad actors from exploiting gaps in the technology. This should be complemented with training of the staff of the regulators in blockchain forensics and smart contract auditing to bridge technical knowledge gaps.

Fourth, there is the need to strengthen the country's weak digital environment through an enhanced framework for data protection and a coordinated cybersecurity regime. The proposition is that regulators of the Nigerian capital market should capitalise on the recent data protection Act to ensure that customers data are well protected. This is essential because findings from Project Khokha 2 cautions that while DLTs provide data transparency, it also highlights privacy concerns [19]. It is also noted that the current cybersecurity regime in Nigeria appears to be staggered with different institutions left to develop their own cybersecurity strategy. To address this, there should be an overarching and coordinated cybersecurity framework similar to what is prevalent in the UK [32]. This would guarantee standards of operation across all parastatals and relevant bodies that engages with relevant market operators since market institutions would remain key players under the blockchain. This should also be supported with an effective implementation by relevant stakeholders.

It is submitted that blockchain's success in Nigeria hinges on reconciling its disruptive potential with the realities of institutional frailty. While permissioned ledgers offer stability, their viability depends on addressing cybersecurity weaknesses, regulatory inertia and accountability deficits. For Nigeria, blockchain adoption must be paired with institutional reforms – transparent governance, robust cybersecurity frameworks and agile regulation – to avoid digitising dysfunction. Without this, blockchain risks becoming another layer of fragility in a market already grappling with systemic trust deficits.

9. Custody implications of blockchain adoption in Nigeria's capital market

The integration of blockchain technology into Nigeria's capital market could introduce complex custody challenges, particularly in reconciling the decentralised ideals of blockchain with the centralised realities of

asset management. Tokenised securities – digital representations of real-world assets like equities or bonds – require a trusted intermediary to anchor these tokens to tangible off-chain assets [18]. While blockchain's promise of decentralisation suggests a future where investors self-custody assets through private wallets [18], the practical demands of regulatory compliance, legal enforceability and systemic stability necessitate reliance on centralised custodians [18].

This hybrid model where blockchain tracks ownership but legal custody remains with centralised institutions dominates global pilots [19, 28]. Their involvement in a blockchain environment is also borne out of the argument that centralised institutions like CSDs have expertise in the management and settlement of securities transactions. This was evident in the approach taken by the Bank of France experimentation of the settlement of government bonds in Central Bank Digital Currency with blockchain technology [33]. There, Euroclear France – (a legacy CSD) was selected to play a custodial role for the off-chain asset.

However, the case of Project Khokha 2 presented a unique opportunity for African markets to learn from. The POC sought to reimagine the custodial responsibilities of traditional central securities depositories (CSD) and the role of other financial market infrastructure (FMIs) in a blockchain-operated capital market. The POC developed a specialised decentralised DLT-based token trading platform (TTP) named the “Khokha hub” which sought to compose and combinedly perform key roles in the capital market, such as a trading platform, central securities depository (CSD), securities settlement system (SSS) and elements of the payment settlement system. However, while the POC showcased that various market intermediaries can be streamlined (which can reduce settlement times and errors) and custodial activities can be performed solely by the DLT, the practical realities as envisioned by SARB is that the TTP would still be controlled by a consortium of market institutions but with a more decentralised governance model [19]. This is a sensible approach that aligns with the hybrid approach on custody of assets.

For Nigeria, the possible reliance on market institutions would raise profound concerns about accountability and trust. The antecedent of legacy market institutions in handling and management of investors' assets has been fraught with transparency issues. The case of *CSCS & Anor v. Bonkolans Investment Ltd & 5 Ors* [6] starkly illustrates these concerns. The case revealed systemic negligence and collusion on the part of market institutions like the Central Securities Clearing System (a CSD) to syphon the asset of investors. In that case, the staff of the CSD colluded with stockbrokers to inject forged share certificates into its depository to enable unauthorised sales. The CSCS, which is tasked with safeguarding investor assets under Section 34 of *Nigeria's SEC Consolidated Rules and Regulations (2013)* failed to verify broker declarations, thereby violating its fiduciary duty. During litigation, the CSCS attempted to downplay its role by framing itself as a passive “complement” to market intermediaries. This evasion of accountability underscores a deeper institutional malaise.

Further examples can be drawn from market institutions like commercial banks in Nigeria which may likely take on custodial responsibilities in a blockchain-operated market. There have been a number of instances where customers have complained about unauthorised deductions of their deposits or investments [7]. There are also cases where staff of the bank have colluded to hack the bank's system and fraudulently convert customers' funds [8]. Insights from the legal and compliance officers of top commercial banks interviewed in this study noted how entrenched these issues were. This is coupled with a weak digital infrastructure which has been subject to incessant cyber-attacks [34]. Their perspective coincides with the data presented by the Nigeria Inter-Bank Settled System (NIBSS) which noted a +23% increase in the value of fraudulent transactions perpetuated in the Nigerian financial system from 2019 to 2023 [35]. All of these issues showcase the custodial fragility and integrity of market institutions in the country. It raises a logical concern that if market institutions cannot uphold

integrity in the traditional market, entrusting it with blockchain-based custody risks digitising existing flaws with a tendency to erode investors' confidence and market integrity.

While blockchain technology is transformative, it does not replace existing infrastructures, rather it augments it. As noted by the Boston Consulting Group, CSDs in tokenised markets will likely retain governance roles by enforcing standards and resolving disputes [11]. However, this requires custodians to operate with unprecedented accountability. In Nigeria, reforms are critical for the successful implementation of the technology in its market. There may be a need to integrate independent validators into custody systems to audit transactions and asset holdings in real time to reduce opacity. Second, there is a need to develop standardised guidelines for hybrid custody models to address vulnerabilities, such as enabling third-party audits.

The tension for emerging markets in Africa is concerning as custody frameworks under a blockchain-operated market will likely remain tethered to the same institutions that have historically struggled with accountability. For Nigeria, this means that technological adoption must parallel institutional reform. Rebuilding trust in custodians like the CSCS, commercial banks and other market institutions demands not just an upgraded technology but a cultural shift towards transparency, rigorous enforcement of fiduciary duties and participatory governance. Without these steps, blockchain risks becoming a digital veneer over systemic dysfunction, which may leave investors vulnerable in a new era of market infrastructure. Thus, the promise of blockchain lies not in its codes but in the integrity of those who govern it.

10. Enforcement framework and supervisory mechanisms: A critical pillar for blockchain adoption

The integration of blockchain technology into Nigeria's capital market will demand a supervisory and enforcement framework capable of operating at the speed of code. Prescriptive rules commanding market institutions to comply with transparency and accountability market rules without active enforcement will not suffice. Blockchain's promise of real-time settlements, 24/7 market operations and immutable transaction records [18] therefore hinges on regulators who can enforce rules with equal precision and agility. However, Nigeria's SEC has in some instances exhibited systemic inefficiencies that threaten to undermine this vision. An illustration of this challenge is the *Prof Anthony Asiwaju v. SEC & Anor case* [36], where the SEC imposed a four-year lien on shares during an investigation without resolving the underlying dispute. While the Investment and Securities Tribunal upheld the SEC's authority, it rebuked the regulator for its inertia. This case spotlights a culture of delayed enforcement that clashes with blockchain's instantaneous nature.

This enforcement laxity is not an isolated flaw but a symptom of institutional inertia. Under Section 304 of the Investment and Securities Act, the SEC collaborates with law enforcement agencies like the police to address criminal market activities. However, cases involving fraud or asset mismanagement often languish in bureaucratic limbo. Furthermore, the illegal dissolution of the Investment Securities Tribunal (IST) – the arbiter for entertaining securities dispute in the Nigerian capital market – in 2015 contrary to the provisions of Sections 277 and 278 of the Investment and Securities Act, mirrors the institutional fragility in the system, and if repeated, could affect the ability of the regulators to effectively exercise their powers using judicial pathways. In a blockchain-driven market where transactions settle irrevocably in minutes, such delays could render enforcement actions obsolete, leaving investors with irreversible losses.

The stakes are further heightened by blockchain's automated architecture. Features like smart contracts are capable of executing transactions without human intervention, thereby leaving regulators with no room for post-hoc

corrections. If a fraudulent transaction occurs on-chain – say, a manipulated tokenised bond sale – the regulator must be able to act instantly to freeze assets or reverse actions. However, it would appear that the market regulators lack the institutional culture to meet this demand. Traditional enforcement timelines, measured in months or years, are incompatible with blockchain's real-time ecosystem. This mismatch risks would erode investor confidence in the ability of the regulators to protect them in a digitised environment. These enforcement gaps compound Nigeria's preexisting governance and custody challenges. As explored earlier, entrusting blockchain governance to its traditional CSD, as already criticised for negligence in the Bonkolans case, creates vulnerabilities. Consider a scenario where the CSD, acting as a blockchain validator, approves a fraudulent transaction. The SEC's ability to investigate and remediate such an incident in real time becomes critical. In a hybrid custody model where blockchain tracks ownership but assets are held by market institutions like the CSDs, such an arrangement would demand rigorous oversight by regulators to prevent collusion. Without agile enforcement, blockchain's transparency becomes a façade and runs the risk of digitising corruption rather than deterring it.

The path towards a successful adoption of blockchain in Nigeria's capital market would likely involve a radical reimagining of Nigeria's regulatory framework. First, as earlier suggested, regulators must integrate regulatory technology (RegTech) tools – AI-driven surveillance systems and blockchain analytics platforms to monitor transactions in real time and flag anomalies. Second, there may be a need to introduce statutory timelines for resolving blockchain-related disputes to avoid enforcement inertia. Finally, collaborative oversight models, such as fintech sandboxes (similar to initiatives like the FCA digital sandbox [37]) or POCs such as that in Project Guardian (led by the Monetary Authority of Singapore (MAS) and a consortium of market institutions) [38] could be developed to foster innovation while allowing regulators to co-develop enforcement protocols with market participants.

Furthermore, there should be protection and independence of the adjudicatory body that entertains securities disputes such as the IST. The reason for this is because resolution of disputes that occur on-chain would still have to be entertained off-chain, and a dissolution of the IST as was seen in 2015 by the executive arm would threaten systemic stability under a blockchain-operated capital market. The proposal is to remove the IST from the appendage of the executive arm and place it under the judiciary to be overseen by the National Judicial Council (NJC) and also specifically capture it under the Constitution of the Federal Republic of Nigeria. This would give it the protection, stability and independence it needs to resolve market disputes without undue interference.

11. Conclusion: The pathway forward and the role of strong institutions

The quest to adopt blockchain in capital markets in emerging economies in Africa presents tension between balancing innovation and systemic stability due to institutional fragility in the region.

Blockchain's promise of transparency, efficiency and reduced costs is undeniable, but its potential remains shackled in markets where weak governance, lax enforcement and cultural tolerance for opacity persist. For emerging markets in Africa, the path forward demands more than adopting blockchain – it requires rebuilding the very systems that sustain trust. Douglass North's institutional theory underscores this position by positing that economic progress depends on formal institutions (laws, regulations) and informal norms (trust, transparency) that reduce transaction costs and uncertainty [13]. For blockchain, this translates to a foundational need for robust institutions capable of enforcing contracts, protecting property rights and fostering trust – prerequisites that appear to be deficient within markets in the region.

Advanced economies appear to exemplify North's thesis with the presence of strong institutions like regulators who enforce stringent transparency norms, such as transaction reporting and strict anti-money laundering

(AML) protocols, amongst others. It is stated that these frameworks can only thrive on cultural norms of accountability, and as Elinor Ostrom's work on collective governance emphasises, trust is not legislated but cultivated through consistent, transparent practices [39]. The various recommendations offered in this article can help douse the tension that blockchain adoption would create in the capital market in Nigeria and within the region.

References:

- [1] J. J. Aduda, R. Chogii, and M. T. Murayi, "The effect of capital market deepening on economic growth in Kenya," *Journal of Applied Finance & Banking*, vol. 4, no. 1, pp. 141–159, 2014.
- [2] E. Yadirichukwu and E. E. Chigbu, "The impact of capital market on economic growth: the Nigerian perspective," *International Journal of Development and Sustainability*, vol. 3, no. 4, pp. 838–864, 2014.
- [3] M. Dowelani, C. Okoro, and A. Olaleye, "Factors influencing blockchain adoption in the South African clearing and settlement industry," *South African Journal of Economic and Management Sciences*, vol. 25, no. 1, p. a4460, 2022.
- [4] OECD, "The tokenization of assets and potential implications for financial markets," *OECD Blockchain Policy Series*, 2020. Accessed: Mar 12, 2024. [Online]. Available: www.oecd.org/finance/The-Tokenisation-of-Assets-and-PotentialImplications-for-Financial-Markets.htm.
- [5] National Information Technology Development Agency, "National blockchain policy for Nigeria," 2023. Accessed: Mar 12, 2024. [Online]. Available: <https://nitda.gov.ng/wp-content/uploads/2023/05/National-Blockchain-Policy.pdf>.
- [6] Bonkolans Investment Ltd & Ors V. Central Securities Clearing System Ltd & Ors (2009) LLJR-CA.
- [7] S. A. Owolabi, "Fraud and fraudulent practices in Nigeria banking industry," *African Research Review*, vol. 4, no. 93b, pp. 240–256, 2010.
- [8] O. Tade, "Nature of frauds in Nigeria's banking ecosystem, 2015-2019," *Journal of Financial Crime*, vol. 29, no. 4, pp. 1241–1248, 2022.
- [9] U. Nwoke and I. H. Onoh, "Rule of law and preventing fraud in Nigeria's capital market," *Journal of Financial Crime*, vol. 29, no. 3, pp. 951–996, 2022.
- [10] UK Finance & Oliver Wyman, "Unlocking the power of securities tokenization: How the UK can lead digital transformation and consolidate the role as a global financial centre," 2023. Accessed: July 8, 2023. [Online]. Available: <https://www.ukfinance.org.uk/system/files/2023-07/Unlocking%20the%20power%20of%20securities%20tokenisation.pdf>.
- [11] BCG, Clifford Chance et al., "Impact of distributed ledger technology in global capital markets." Accessed: Nov 8, 2024. [Online]. Available: <https://www.afme.eu/Portals/0/DispatchFeaturedImages/20230512%20GFMAImpactofDLT%20FullReport%20FINAL%20FULL.pdf>.
- [12] M. Dowelani, C. Okoro, and A. Olaleye, "Blockchain technology in the clearing and settlement industry in South Africa," *Acta Commercii*, vol. 23, no. 1, pp. 1–12, <https://doi.org/10.4102/ac.v23i1.1097>.
- [13] D. C. North, *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press, 1990.
- [14] N. Mabin, G. Hamideh, and G. Fereshteh, "Snowball sampling: A purposeful method of sampling in qualitative research," *Strides in Development of Medical Education*, vol. 14, no. 3, p. e67670, 2017.
- [15] A. A. Mohamed et al., "Characteristics of Blockchain and Smart Services, for Smart Governments: A systematic review of the literature," *International Journal of Information Systems and Project Management*, vol. 10, no. 3, pp. 30–55, 2022.
- [16] OECD, "Blockchain Primer." Accessed Jan 4, 2025. [Online]. <https://cdn.github.org/umbraco/media/2431/oecd-blockchain-primer.pdf>
- [17] BCG, Clifford Chance et al., "Impact of distributed ledger technology in global capital markets." Accessed: Nov 8, 2024. [Online]. Available: <https://www.afme.eu/Portals/0/DispatchFeaturedImages/20230512%20GFMAImpactofDLT%20FullReport%20FINAL%20FULL.pdf>.
- [18] OECD, "The tokenization of assets and potential implications for financial markets, OECD blockchain policy series," 2020. Accessed: Mar 12, 2025. [Online]. Available: www.oecd.org/finance/The-Tokenisation-of-Assets-and-PotentialImplications-for-Financial-Markets.htm.

- [19] South African Reserve Bank, "Project Khokha 2: Exploring the implications of tokenization in financial markets." Accessed: Mar 8, 2025. [Online]. Available: <https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2022/project-khokha-2/Project%20Khokha%20%20Full%20Report%206%20April%202022.pdf>.
- [20] OECD, "Tokenisation of assets and distributed ledger technologies in financial markets potential impediments to market development and policy implications," OECD Business and Finance Policy Papers, No. 75, 2025.
- [21] World Economic Forum & Boston Consulting Group, "Digital assets, distributed ledger technology and the future of capital markets," 2021. Accessed: Nov 15, 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_Digital_Assets_and_the_Future_of_Capital_Markets.pdf.
- [22] R. Priem, "Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications," *Financial Innovation*, vol. 6, no. 11, pp. 1–25, 2020.
- [23] Regulations (EU) 2022/858 of the European Parliament of the Council, "Pilot regime for market infrastructures based on DLT," *Official Journal of the European Union*, vol. L 151, pp. 1–33, 2022.
- [24] Nigerian Securities and Exchange Commission Rules for Virtual Asset Providers in: SEC, "Statement on digital assets and their classification and treatment," 2020. Accessed: July 3, 2024. [Online]. Available: <https://sec.gov.ng/statement-on-digital-assets-and-their-classification-and-treatment/>.
- [25] N. Chiejina, "SEC to regulate capital market with Blockchain technology," 2025. Accessed: Jan 4, 2025. [Online]. Available: <https://thenationonline.ng.net/sec-to-regulate-capital-market-with-blockchain-technology-2/#:~:text=The%20Securities%20and%20Exchange%20Commission,regulation%20of%20Nigeria's%20capital%20market.>
- [26] National Information Technology Development Agency, "National blockchain policy for Nigeria," 2023. Accessed: Jan 14, 2024. [Online]. Available: <https://nitda.gov.ng/wp-content/uploads/2023/05/National-Blockchain-Policy.pdf>.
- [27] SEC, "Nigeria capital market master plan," 2021. Accessed: Jan 14, 2024. [Online]. Available: <https://sec.gov.ng/nigerian-capital-market-masterplan/>.
- [28] Bank for International Settlements, SIX Group AG and Swiss National Bank, "Project Helvetia settling tokenised assets in central bank money," 2020. Accessed: Mar 5, 2025. [Online]. Available: <https://www.bis.org/publ/othp35.pdf>.
- [29] Bank of England, "Guidance on the operation of the digital securities sandbox," 2024. Accessed: Jan 4, 2025. [Online]. Available: <https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox/guidance-on-operation-digital-securities-sandbox>.
- [30] International Telecommunication Union, "Global cybersecurity index," 2024, 5th ed. Accessed: Mar 1, 2025. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.
- [31] G. A. N. Ama, C. O. Onwubiko, and H. A. Nwankwo, "Cybersecurity challenge in Nigeria deposit money banks," *Journal of Information Security*, vol. 15, pp. 494–523, 2024.
- [32] National Cyber Security Centre, "Introduction to the Cyber Assessment Framework (CAF)," 2024. Accessed: Mar 4, 2025. [Online]. Available: <https://www.security.gov.uk/policy-and-guidance/introduction-to-the-cyber-assessment-framework-caf/>.
- [33] The Banque De France et al., "Experimenting settlement of French government bonds in Central Bank digital currency with blockchain technology," 2021. Accessed: Jan 15, 2024. [Online]. Available: [settlement-french-government-bonds-in-cbdc-with-blockchain.pdf \(euroclear.com\)](https://www.euroclear.com/~/media/Files/2021/01/20210120_French_government_bonds_in_cbdc_with_blockchain.pdf).
- [34] F. Ogene, "Cybersecurity and IT governance challenges in Nigeria: Strategic investment needs and the path forward for a resilient digital economy," *International Journal of Computer Applications*, vol. 186, no. 55, pp. 41–46, 2024.
- [35] NIBSS., "Annual fraud landscape in Jan-Dec 2023," 2023. Accessed: Jan 15, 2024. [Online]. Available: <https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf>.
- [36] Prof Anthony Asiwaju v. SEC & Anor Suit No. IST/LA/OA/05/16 (unreported).
- [37] Financial Conduct Authority, "Digital sandbox." Accessed: Mar 4, 2025. [Online]. Available: <https://www.fca.org.uk/firms/innovation/digital-sandbox>.
- [38] Monetary Authority of Singapore, "Project guardian," 2024. Accessed:

Mar 4, 2025. [Online]. Available: <https://www.mas.gov.sg/schemes-and-initiatives/project-guardian>.

[39] O. Elinor, *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press, 1990.

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

Clinton Osemwengie is the sole author of this paper.

Funding:

None declared.

Acknowledgements:

The author would like to thank Priya Dozier, Assistant Professor, University of South Florida for offering to review the initial draft of this paper during the University of South Florida and University of East London at the Joint FinTech Research Symposium in February 2025. All errors are solely mine.

ESSAY

OPEN ACCESS

ISSN Print: 2516-3949

[https://doi.org/10.31585/jbba-9-2-\(1\)2026](https://doi.org/10.31585/jbba-9-2-(1)2026)

Ancient Philosophers Understand Blockchain Better Than Most of Us

Naseem Naqvi MBE

*Centre for Evidence-Based Blockchain, The British Blockchain Association, UK***Correspondence:** cebb@britishblockchainassociation.org**Received:** 26 January 2026 **Accepted:** 21 February 2026 **Published:** 14 March 2026

Abstract

This essay argues that blockchain technology is best understood not just as a socio-political and financial instrument, but as a philosophical proposition — one that resurrects the oldest questions in human civilisation concerning power, truth, sovereignty, and justice. Drawing on the intellectual traditions of Socrates, Aristotle, Heraclitus, Epictetus, Plato, Marcus Aurelius, and Seneca, the essay contends that ancient philosophy provides a more penetrating analytical framework for evaluating blockchain's promise and limitations than contemporary regulatory or technical discourse alone.

Keywords: *Bitcoin, Blockchain, Digital Assets, Cryptocurrency, Philosophy, Decentralisation, Stoic, Evidence Based Blockchain*

JEL Classifications: *A10, B41, O33, G28, D63*

Most blockchain advocates quote Satoshi. I went further back. 2,500 years further.

Socrates was killed for questioning authority. Epictetus built a philosophy of freedom from inside slavery. Marcus Aurelius ruled the most powerful empire on earth and spent his private hours writing reminders to himself not to abuse it. These were not theorists. They were people who lived the problems that blockchain is now attempting to solve architecturally.

I have been thinking about what they would make of this technology. Not as a thought experiment, but as a serious provocation. Because if you strip blockchain back to its first principles, what you find is not a technology story. You find a philosophy story; one that is at least 2,500 years old.

Socrates spent his life doing one thing: questioning the legitimacy of authority. He was executed for it [1]. His entire method rested on the premise that truth is not handed down by rulers or institutions; it emerges through open, rigorous, adversarial inquiry. Blockchain, at its core, does something structurally similar. It removes the need to trust an institution by replacing institutional authority with cryptographic proof and distributed consensus. Bitcoin's network has maintained over 99.99% uptime since 2009 without a single central authority managing it. Ethereum, now processing billions of dollars in transactions daily across finance, identity, and digital ownership, has operated continuously since 2015. Zcash has run without interruption since 2016, adding the dimension of privacy as a fundamental right rather than a privilege. These are not experiments. They are existence proofs. Socrates would not have needed convincing. He would have understood it immediately, because he lived the problem it solves.

Aristotle would take a different approach [2] [3]. He was interested in systems, in how communities organise themselves, in what makes governance just rather than merely functional. His concept of distributive justice was precise: people should receive what the rules actually entitle them to, not what those administering the rules decide they deserve. That distinction matters enormously when you look at what has happened inside centralised financial systems. The 2008 crisis was not just an economic failure. It was a justice failure. Over 8 million Americans lost their jobs,

millions more lost their homes, and the institutions responsible were recapitalised with public money while counterparties received what those in power decided, not what the rules said they should. Aristotle would have been deeply interested in the idea that a protocol can enforce rules without a sovereign interpreting them. He would also have been the first to scrutinise on-chain governance carefully, because he knew that rule by the majority is not automatically just, and that centralised components within a decentralised protocol can still produce oligarchy, regardless of what you call it.

Heraclitus believed that the universe is governed by a hidden logos, a rational principle underlying all apparent chaos, and that the only constant in existence is change [4]. He famously argued that you cannot step into the same river twice. Blockchain encodes both insights simultaneously. Its ledger is permanently changing, every block a new state of the world, yet the underlying logic is immutable and universally verifiable. No single actor decides what the river looks like next. The protocol does. Heraclitus spent his life arguing that most people sleepwalk through reality, mistaking surface appearances for truth. He would look at the global financial system and see exactly that: billions of people accepting the word of institutions as truth, without any mechanism to verify it independently. He would have found in blockchain the first technology in human history capable of making the logos visible, auditable, and shared.

Epictetus is the one I find most striking in this context. He was born a slave. He built an entire philosophical system around one idea: distinguish what is within your control from what is not, and build your life accordingly [5]. Managing peer-to-peer transactions from a digital wallet, without intermediaries is, in philosophical terms, an act of radical autonomy. The World Bank estimates that around 1.3 billion adults globally remain unbanked, excluded from financial systems entirely through no fault of their own [6]. For those people, a digital wallet on a blockchain is not a technical feature. It is the first financial instrument they have ever owned and controlled. And stablecoins extend that further. A farmer in sub-Saharan Africa or a small business owner in a hyperinflationary economy can now hold a dollar-denominated asset on a phone, without a bank account, without a credit history, without permission. That is not a fintech product. That is economic sovereignty made accessible for the first time in

history. Epictetus would have recognised that immediately.

Plato argued that a just society rests on truth being verifiable and shared [7]. Blockchain makes that possible in domains we have barely begun to explore. A patient's medical records on an immutable ledger, controlled by them rather than a hospital system. A supply chain where every step from raw material to shelf is permanently audited and cannot be falsified. Intellectual property rights recorded at the moment of creation, removing the need for costly intermediaries to establish authorship. Digital identity that belongs to the individual, not to a government database or a technology platform. These are not peripheral applications. They are the philosophical core of what a sovereign world looks like when its infrastructure is honest by design rather than by promise. Aristotle would have called this the foundation of a truly just polis. We are only beginning to build it.

Marcus Aurelius ruled the most powerful empire on earth and spent his private hours writing reminders to himself not to abuse that power [8]. His *Meditations* are not the writings of a man comfortable with authority. They are the writings of a man who understood that power concentrated in a single point is always one moral failure away from tyranny. He wrote that the purpose of power is to serve, not to possess. He would have been profoundly interested in a governance architecture where no single emperor, no single institution, no single node can override the rules that everyone agreed to follow. He would also have been its most rigorous internal critic, because he knew better than anyone that good systems do not guarantee good actors. He spent his reign fighting the corruption of his own court while writing philosophy in his tent. Blockchain gives us better architecture. It does not give us better human beings. Marcus Aurelius would have insisted we remember the difference.

This is, in fact, the internet that Sir Tim Berners-Lee originally envisioned [9]. A decentralised web where individuals, not corporations or governments, control their own data. What emerged instead was the opposite: a handful of platforms capturing, monetising, and surveilling the digital lives of billions. Berners-Lee has said so himself, describing his creation as having been taken in a direction he never intended, and his subsequent Solid project is a direct attempt to restore individual data sovereignty through decentralised architecture. Blockchain is not a departure from that original vision. It is its most credible continuation.

I have been making this argument since 2018, when I coined the term Evidence-Based Blockchain (EBB), precisely because the philosophical case was never enough on its own [10][11]. EBB is a structured intellectual methodology for how we ask better questions about this technology, how we frame problems rigorously before attempting to solve them, how we cite the highest quality of filtered evidence, how we apply frameworks like PCIO (*Problem-Comparison-Intervention-Outcome*), and the "5As" - (*Ask, Acquire, Appraise, Apply, Assess*) to evaluate real-world applications, publish findings, subject them to peer review, and build a cumulative body of valid knowledge that policymakers, clinicians, regulators, and industry practitioners can actually rely on. It is, in short, the application of scientific discipline to one of the most consequential technological shifts of our time. From blockchain-verified pharmaceutical supply chains reducing counterfeit medicines entering patient care, to immutable academic credential records eliminating degree fraud, to land registry pilots in emerging economies giving smallholder farmers legally defensible proof of ownership for the first time, the applications are not theoretical. They are operational. The sovereign world the philosophers described is not built on promises. It is built on verifiable truth. That is what Evidence-Based Blockchain demands, and that is what makes it a philosophical commitment as much as a technical one.

Seneca would have understood the systemic critique just as quickly. He wrote extensively [12] about how wealth corrupts institutions, how proximity to power distorts judgment, and how the powerful construct systems that perpetuate their own privilege. The fact that the top 1% of

the global population controls a disproportionate share of personal wealth, largely through instruments designed and administered by centralised institutions, is not an accident of markets. It is a structural outcome. Seneca would have recognised what blockchain is attempting to dismantle.

Yet the philosophers would not have been content with technological advancements alone. They would have demanded evidence that this sovereignty reaches those who need it most. And herein lies the technology's most glaringly challenging problems.

The 1.3 billion unbanked people [13] this technology is supposed to liberate are not always digitally literate enough to operate a wallet, navigate a decentralised application, or understand what they are signing when they approve a transaction. Self-sovereignty sounds like liberation until you realise it also means self-responsibility. There is no help desk when you lose access to your funds in a permission-less decentralised finance pool. No institution to call when the distributed code fails. With great power of self-sovereignty comes great responsibility, and responsibility without education is not freedom, it is exposure. The printing press did not democratise knowledge because it was philosophically correct. It democratised knowledge because anyone could read a page. With the emergent need for trust and efficiency, Blockchain will soon find its equivalent moment, the point where the depth of the idea and the simplicity of the experience become one and the same. And beneath the literacy problem sits a deeper structural one. Approximately 2.2 billion people worldwide still lack access to the internet [14]. A sovereign digital world that requires connectivity to participate is not yet sovereign for a significant portion of humanity. Until mobile internet access is treated as infrastructure on par with roads and electricity, and until blockchain education is embedded in school and college curricula rather than confined to conference halls and technical whitepapers, the technology's liberating potential remains unrealised and inaccessible to those who need it most.

These are not abstract questions. They are the questions that serious policymakers and regulators are now asking, often without the philosophical vocabulary to articulate them precisely. The EU's MiCA framework [15], the FCA's ongoing cryptoasset consultations [16], the IMF's repeated warnings about systemic risk [17], all of them are wrestling, in regulatory language, with questions Aristotle posed in political philosophy two and a half millennia ago.

Blockchain is the most radical socio-political idea of the 21st century, often disguised as an economic instrument. It challenges the notion of power, trust, identity, sovereignty, societal rules and regulations. Those are not technology questions. They are the oldest questions in human civilisation. And we are answering them right now, in real time, mostly without realising it.

Socrates was killed for asking them.

We have the luxury of a keyboard and a choice. The question is whether we are using it wisely, or simply repeating the same mistakes with better software. The ancient philosophers would not have been impressed (yet) by the technological advancements alone; they would have been watching what the humans do with the technology.

References

- [1] G. Vlastos, *Socrates: Ironist and Moral Philosopher*. Cambridge: Cambridge University Press, 1991.
- [2] Aristotle, *Nicomachean Ethics*, R. Crisp, Trans. Cambridge: Cambridge University Press, 2000.
- [3] Aristotle, *Politics*, C.D.C. Reeve, Trans. Indianapolis: Hackett Publishing, 1998.
- [4] Heraclitus, *Fragments*, B. Haxton, Trans. London: Penguin Classics, 2003.
- [5] Epictetus, *Discourses and Selected Writings*, R. Dobbin, Trans. London: Penguin Classics, 2008.

- [6] World Bank, *Global Findex Database 2025: Financial Inclusion at Record High*. Washington DC: World Bank Group, 2025. [Online]. Available: <https://openknowledge.worldbank.org/entities/publication/8b9002b6-d8dd-426c-aa7c-6d7d16902cd7> [Accessed: Mar. 14, 2026].
- [7] Plato, *The Republic*, D. Lee, Trans. London: Penguin Classics, 2007.
- [8] Marcus Aurelius, *Meditations*, G. Hays, Trans. New York: Modern Library, 2002.
- [9] T. Berners-Lee, *World Wide Web Foundation, and Solid*. [Online]. Available: <https://solidproject.org/about>
- [10] N. Naqvi, et al., "Evidence-based blockchain: Findings from a global study of blockchain projects and start-up companies," *Journal of the British Blockchain Association*, vol. 3, no. 2, 2020. [https://doi.org/10.31585/jbba-3-2-\(8\)2020](https://doi.org/10.31585/jbba-3-2-(8)2020)
- [11] The CEbb, EBB, and PICO framework for evidence-based blockchain: <https://britishblockchainassociation.org/cebb/>
- [12] Seneca, *Letters from a Stoic*, R. Campbell, Trans. London: Penguin Classics, 2004.
- [13] World Bank, *Global Findex Database 2025: Financial Inclusion at Record High*, Washington DC: World Bank Group, 2025. [Online]. Available: <https://openknowledge.worldbank.org/entities/publication/8b9002b6-d8dd-426c-aa7c-6d7d16902cd7> [Accessed: Mar. 14, 2026].
- [14] International Telecommunication Union, "Measuring digital development: Facts and figures 2025," ITU, Geneva, 2025. [Online]. Available: <https://www.itu.int>
- [15] European Parliament, "Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)," *Official Journal of the European Union*, 2023.
- [16] Financial Conduct Authority, "CP25/14: Cryptoasset custody and stablecoin issuance," FCA, London, 2025. [Online]. Available: <https://britishblockchainassociation.org/wp-content/uploads/2026/02/FCA-BBA-2026-CP2540-FINAL.pdf>
- [17] International Monetary Fund, "Elements of effective policies for crypto assets," *IMF Policy Paper*, Washington DC, 2023. [Online]. Available: <https://www.imf.org>

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

NN drafted this essay in its entirety.

Funding:

None declared.

Acknowledgements:

None.

CONFERENCE PROCEEDINGS

8th Blockchain International Scientific Conference - 27 March 2026, ISC2026, London

1. What Trump's Crypto Endorsement Means for Retail Adoption

Dr Larisa Yarovaya, Dr Marion Laboure

University of Southampton, UK

Category: Oral Presentation

Abstract

This paper investigates whether President Trump's political endorsement of the cryptocurrency industry – and the associated expectations of a lighter regulatory stance in the U.S. – has meaningfully influenced retail cryptocurrency adoption across advanced economies. Using 78,200 responses from Deutsche Bank's proprietary and unique monthly consumer survey, conducted between August 2023 and June 2025, covering 3,400 consumers per wave across the U.S., the U.K., and the EU, we find little evidence that retail adoption has increased during this period, despite Bitcoin reaching new all-time highs. Both before and after the 2024 U.S. election, public understanding and usage of cryptocurrencies remain limited. Overall, this paper provides a comprehensive analysis of the evolving demographics, attitudes, and behaviors of crypto users across six major economies, offering new insights into the political and psychological drivers of digital asset regulation.

2. Evaluating Blockchain-Based Consortia for Enhancing Open Banking and Banking-as-a-Service Ecosystems

Irem Akinci

Bahçeşehir University, Türkiye

Category: Oral Presentation

Abstract

The financial sector is experiencing a profound transformation driven by innovations such as open banking and banking as a service (BaaS), which aim to create more accessible, interoperable, and innovative financial ecosystems. Despite their potential, these models face significant challenges related to trust, data integrity, interoperability, and operational efficiency across multiple institutions. Blockchain technology offers a decentralized infrastructure that addresses these challenges by ensuring trust, transparency, traceability, and transaction integrity, while enabling the formation of blockchain-based consortia. This study investigates the applicability of blockchain in enhancing open banking and BaaS frameworks, focusing on the integration of APIs, smart contracts, and decentralized governance mechanisms. By analyzing sectoral applications and potential use cases, the study highlights how blockchain-enabled consortia can provide a robust, scalable, and secure foundation for next-generation financial services. The findings suggest that the integration of blockchain not only facilitates innovation and collaboration but also contributes to systemic reliability and sustainable financial transformation.

Keywords: *Blockchain, Capital Markets, Regulatory Framework, Intermediaries, Custody, Governance*

3. Implied Impermanent Loss for Concentrated Liquidity

L. Alberici, A. Papanicolaou, L. Schönleber

Bayes Business School, City St George's, University of London & Fondazione Collegio Carlo Alberto, University of Turin, Italy

Category: Oral Presentation

Abstract

We extend the option-implied valuation of impermanent loss for liquidity provision on decentralized exchanges (DEXs), where concentrated liquidity and varying maturities alter risk exposures. Our framework quantifies implied impermanent loss (IIL) using option prices, allowing us to measure the cost of providing liquidity across token pairs—including BTC, ETH, SOL, XRP, and PAXG, along with their stablecoin counterparts—and by incorporating the full option term structure to span short-, medium-, and long-horizon expectations. Since options on relative prices are not directly traded, we introduce a model for the joint distribution of token returns and derive a valuation formula via a change of numéraire. We empirically investigate IIL across multiple pairs and maturities, documenting a systematic risk premium as the wedge between implied and realized impermanent loss. Our results show that IIL reflects token-specific risks, correlation risk, and liquidity concentration, which are inversely related to pool depth and vary across maturities. Together, these findings establish a general framework for quantifying risk and expected compensation in AMM markets.

Keywords: *Decentralized Exchanges, Decentralized Finance, Impermanent Loss, Derivatives, Risk-Neutral Pricing, Risk Premium, Staking, Yield Farming.*

JEL Classification Codes: *G10, G11, G13, G20*

4. Digital Twins In Blockchain Environments

O. Letychevskiy - *Heriot-Watt University, Scotland*

Category: Oral Presentation

Abstract

In blockchain environments, particularly blockchain protocols and smart contracts, security—both economic and cyber—is a critical aspect of their reliability. One promising approach to increasing the resilience of such systems is the use of digital twins that replicate the behavior of blockchain environments in real time. A digital twin is capable of predicting and analyzing deviations from normal operation behavior, detecting potential cyberattacks, and providing adaptive responses to market volatility based on analysis of data equivalent to those received by blockchain agents. A two-component architecture of a digital twin is proposed, consisting of an algebraic component built on the basis of behavioral algebra specifications and a neural component implemented as an AI model. The neural model is trained on scenarios of normal operation of smart contracts or blockchain protocol, as well as on simulated attacks generated by the algebraic component. In case of detection of anomalous or malicious activity, transactions can be temporarily blocked or marked as malicious and verified by simulation in the algebraic model to reduce the false positives. The presentation will demonstrate the results of experiments on the detection of known attacks in the environments of Solidity smart contracts and the Delegated Proof of Stake protocol, aimed at preventing malicious actions that can lead to centralization or disruption of the stability of the system.

Keywords: *digital twin, smart contract, behavior algebra, neuron networks, machine learning, simulation, cyberattacks*

JEL Classification: C680

5. Stochastic Modeling of Liquidity Provider Returns in Uniswap: The Role of Volatility and Arbitrage Dynamics

¹Vladimir V. Gorgadze, ¹Roman I. Vlasov, ²Artem Barger - ¹*Moscow Institute of Physics and Technology*, ²*Artem Barger, University of Haifa, Israel*

Category: Oral Presentation

Abstract

Our work introduces a theoretically grounded framework for estimating returns of liquidity providers (LPs) in automated market makers (AMM), with a focus on Uniswap v3 (Concentrated Liquidity AMM) and Uniswap v2 (Constant Product AMM). We explicitly model returns as the sum of fee income and impermanent loss, deriving theoretical mathematical expectations for both components under geometric Brownian motion price dynamics. While existing models often estimate fees as a simple function of historical trading volume or arbitrage dynamics entirely, our approach bridges market microstructure theory and decentralized finance mechanics to provide a practical valuable tool. The proposed framework decomposes fee income into ordinary user transactions and arbitrage flows, explicitly accounting for position activation probability within user-defined price ranges under stochastic price dynamics. To address real-world complexities - such as variable swap sizes and fluctuating pool liquidity - we introduce interpretable correction factors that adapt to market conditions. Validating through extensive Monte-Carlo simulations with realistic market microstructure, our model demonstrates robustness across diverse volatility regimes and pool configurations. For practitioners, the proposed framework enables LPs to optimize price ranges, compare fee tiers, and predict returns under different market conditions. For researchers, it establishes a foundational methodology for analyzing liquidity provision in AMMs that connects theoretical price dynamics to impermanent loss and fee generation. This work advances the understanding of sustainable liquidity provision in decentralized exchanges and offers practical recommendations for rational capital allocation in DeFi protocols.

Keywords: *Automated Market Makers (AMMs), Concentrated Liquidity, Uniswap V3, Liquidity Provision, Impermanent Loss, Stochastic Price Dynamics, Arbitrage Dynamics*

JEL Classification: D40, D47, D53, D01, D02

6. Value chain, Regulation of sustainable finance, and DeFi

Wiktor Gawłowicz - *Urząd Komisji Nadzoru Finansowego, Poland* - Category: Oral Presentation

Abstract

This paper on regulatory policies is inspired by the theory that DeFi regulation must focus on the re-concentrated segments of the value chain to ensure effective oversight and risk control (Buckley, Arner and Zetzsche, 2024). Regulation commonly targeted at the value chain is regulation of sustainable finance, it has not been so far the DeFi regulation. So the purpose of the study is to assess, through up-to-date legal literature, whether current European Union (EU) financial market legislation, policies, and regulatory frameworks sufficiently exploit potential interconnections between environmental, social and governance (ESG) regulation and emerging DeFi solutions. The methodology consisted of a structured review of EU sustainable finance instruments and policy frameworks, including the Sustainable Finance Disclosure Regulation (SFDR) and international initiatives such as the UN Global Compact. The analysis sought, first, to identify areas within sustainable finance regulation that could be enhanced through the application of distributed ledger technology (DLT) and, second, to explore opportunities for stronger alignment between sustainable finance regulation and DeFi-specific frameworks such as the Markets in Crypto-Assets Regulation (MiCA). The conclusions present a set of de lege lata observations and de lege ferenda proposals addressing the identified regulatory intersections. The results consist of concrete recommendations for EU financial market regulators, encouraging a reconsideration of existing policies to strengthen the coherence and effectiveness of both sustainable finance and DeFi regulatory architectures.

7. F-Procure: A Decentralised, Modular Framework for Transparent, Compliant and Efficient Procurement on the Flare Network

Pax Ola

Caypax Inc., Cayman Islands

Category: Oral Presentation

Abstract

Procurement remains constrained by centralised digital architectures that increase administrative effort, limit transparency and complicate compliance management. This paper presents F-Procure: a decentralised, modular procurement framework organised into five layers: blockchain execution, smart contracts, ERP interoperability, AI-assisted analytics and compliance-aware governance. The framework is implemented as a minimum viable prototype on the Flare Network's Coston2 and Songbird test environments, which are used here as technical testbeds rather than as platforms under evaluation in their own right.

Using small-scale, manually executed synthetic procurement scenarios, the study examines whether core stages – tender creation, sealed-bid commit–reveal, award and escrow – can be encoded in smart contracts and traced through verifiable on-chain audit trails. An illustrative comparison with a conventional database-driven workflow suggests that the modular, event-driven design can reduce manual reconciliation effort in bid evaluation and audit preparation within the controlled scenarios tested, although no statistically generalisable performance benchmarks are reported. The prototype also demonstrates how basic procedural requirements (such as submission deadlines and documentation flags) can be expressed as programmable conditions, and how a minimal anomaly-detection layer can flag constructed irregular bidding patterns for human review.

The paper positions F-Procure within existing international experiments in blockchain-enabled procurement and related digital-government initiatives and sets out a governance model and policy-oriented adoption roadmap for future public-sector pilots. It concludes that F-Procure should be viewed as an early-stage reference architecture that suggests the potential feasibility of decentralised, compliance-aware procurement, while highlighting the need for larger-scale empirical evaluation, richer technical artefacts and comparative, platform-agnostic analysis in subsequent research.

Keywords: *Lending, Blockchain, DeFi, Interest Rate*

JEL Classifications: *G20, G23*

8. Blockchain Innovation in Derivatives Trading: Convergence Mechanisms Between Digital Asset and Traditional Derivative Markets

Claudia Tarabù

IÉSEG School of Management, France

Category: Oral Presentation

Abstract

Background. Blockchain technology has fundamentally transformed derivative instrument architecture, enabling cryptocurrency derivatives as a novel financial product class integrating distributed ledger infrastructure with conventional derivative mechanisms. These blockchain-based instruments leverage decentralized network protocols, challenging established paradigms of asset custody, settlement finality, and regulatory jurisdiction in traditional derivative markets.

Purpose. This research investigates blockchain-specific mechanisms driving cryptocurrency derivative integration within traditional financial structures, emphasizing how distributed ledger technology reconfigures derivative instrument design, execution, and settlement processes. The study analyzes distinctive architectural features — smart contracts, decentralized oracles, and on-chain settlement protocols — examining how blockchain's transparency, immutability, and disintermediation influence market efficiency and regulatory frameworks.

Methodology. Employing comparative case study analysis, this research examines three major blockchain-based derivative platforms representing decentralized exchanges, centralized cryptocurrency exchanges, and hybrid models. Primary data collection involves systematic documentation of smart contract functionalities, settlement mechanisms, and custody protocols through technical documentation and blockchain explorer data, focusing on decentralization degree, automation levels, transparency, and interoperability.

Results. Analysis reveals blockchain reconfigures derivative infrastructure through clearinghouse disintermediation, enhanced transparency, and accelerated settlement. Decentralized platforms achieve near-instantaneous settlement versus traditional T+2 cycles. However, hybrid architectures dominate, with blockchain serving primarily as custody and settlement layers. Interoperability constraints fragment liquidity across isolated ecosystems.

Conclusion. Blockchain represents a transformative yet evolutionary force characterized by selective integration rather than comprehensive disruption. Findings indicate gradual convergence where decentralized infrastructure complements established mechanisms, necessitating future research on regulatory frameworks and cross-chain functionality development.

9. Pricing With Multiple Currencies

Nicola Dimitri

Department of Economics and Statistics, University of Siena-Italy

Category: Oral Presentation

Abstract

Since the advent of Bitcoin (Nakamoto, 2008), a large number of privately issued cryptocurrencies have been introduced in the economy. However, as of now, cryptocurrencies are rarely accepted for payments in the retail and wholesale sectors, although a trend is emerging where acceptance of private currencies appears to increase also on those sectors. If such trend would continue it will not be surprising that within few years, from today, people could have available a variety of currencies to pay for products. This future scenario would raise a number of economic issues, some of which are the following. First, and foremost, if and under what conditions a seller would find it convenient to accept payments in a plurality of currencies? Moreover, for each currency, how would the price of a product be determined? Furthermore, which cryptocurrencies may in general be accepted by retailers and wholesalers? In particular, are stablecoins the main candidate, in which case currencies such as Bitcoin and Ethereum would not be accepted, or currencies other than stablecoins would also be used? Last, but not least, Central Banks are also considering the possibility of issuing the legal currency in its digital form, that is the so called Central Bank Digital Currency (CBDC), which will compete with the accepted private digital currencies for payment services. In the paper we sketch an initial, simple, framework for discussing some of the above issues, with specific reference to why should a seller accept multiple coins for payment and what prices would emerge for each currency.

10. Bitcoin Ordinals and Inscriptions: An Analysis of Bitcoin's Evolving Network Dynamics

Alexander Wiedenmann¹, Andre Guettler^{1,2}

¹ *Ulm University, Institute of Strategic Management and Finance, Germany* - ² *Halle Institute for Economic Research (IWH), Germany*

Abstract

Bitcoin Ordinals and inscriptions facilitate the on-chain storage of arbitrary data on the Bitcoin blockchain. In this study, we analyse the impact of inscriptions on the Bitcoin network. We find that inscriptions have significantly increased network activity, created additional demand for blockspace, and influenced Bitcoin's fee market dynamics. Furthermore, we find that the rise of inscriptions coincided with an increased utilisation of Taproot, a notable increase in block size, and the longest sustained period of high blockspace utilisation in Bitcoin's history. Our study shows that inscriptions have reshaped how Bitcoin's blockchain is utilised and underscores the growing number of use cases beyond its original function as a peer-to-peer financial network.

Keywords: *Bitcoin, Blockchain, Ordinals, Inscriptions, Digital Assets, Network Dynamics*

JEL Classifications: *D85, O33*

11. Beyond a Critical Reflection on the Nature of Money: A New Heterodoxy Anchored in Moldovan and Albanian Laboratories

Marc Pilkington FBBA - *University of Burgundy, France*

Abstract

This habilitation thesis proposes a renewed heterodox perspective on money in the era of cryptocurrencies and blockchain technology. It challenges the limitations of traditional monetary theories and develops an original framework for understanding money within a globalized, digital context. The research is grounded in areal studies, focusing on two transitional economies—the Republic of Moldova and Albania—as living laboratories for monetary and technological innovation. Through a multidisciplinary approach combining economics, technology, philosophy, and mythology, the thesis explores how blockchain and cryptocurrencies are reshaping monetary sovereignty, trust, and governance in contexts marked by institutional fragility, corruption, and dependence on diaspora remittances.

Central to the thesis is the development of a New Monetary Heterodoxy (NMH), inspired by the foundational myths of Moldova—contrasting the institutional sovereignty of Bogdan with the bottom-up, narrative legitimacy of Dragoș. This analogy is extended to the emergence of Bitcoin and Satoshi Nakamoto as a modern, decentralized monetary myth.

Key contributions include:

- A formalization of the NMH as an areally anchored theoretical framework.
- Critical analysis of endogenous money creation and its distortion in captured states (e.g., Moldova's 2014–2015 banking fraud).
- Examination of blockchain's potential to foster transparency, financial inclusion, and trust in transitional economies.
- Comparative study of Moldova and Albania as complementary cases of regulatory innovation and technological adoption.
- A prospective research agenda on hybrid monetary systems, algorithmic governance, and the geopolitics of digital finance.

The thesis concludes that peripheral economies like Moldova and Albania are not merely case studies but active sites of monetary reinvention, offering insights into the future of money, sovereignty, and financial governance in a digital world.

Countries with a National Blockchain Roadmap:

(as of July 2025)

UNITED KINGDOM



CHINA



www.GOV.cn

USA



GERMANY



UNITED ARAB EMIRATES



REPUBLIC OF IRELAND



ESTONIA



AUSTRALIA



Australian Government
Department of Industry, Science,
Energy and Resources

BANGLADESH



INDIA



NIGERIA



QATAR



Communications
Regulatory Authority
State of Qatar
مملكة تنظيم الاتصالات
دولة قطر

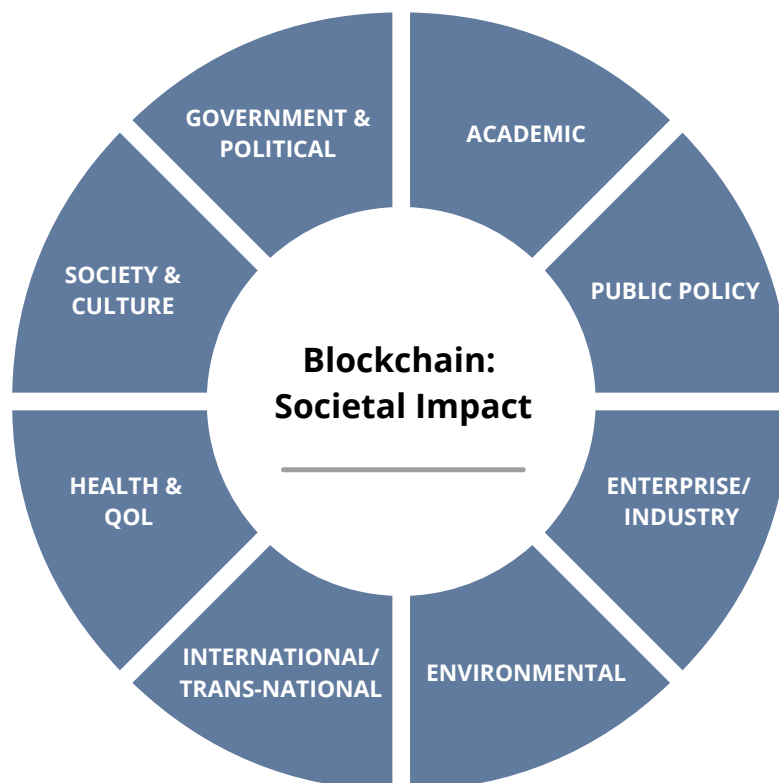
VIETNAM



MALAYSIA



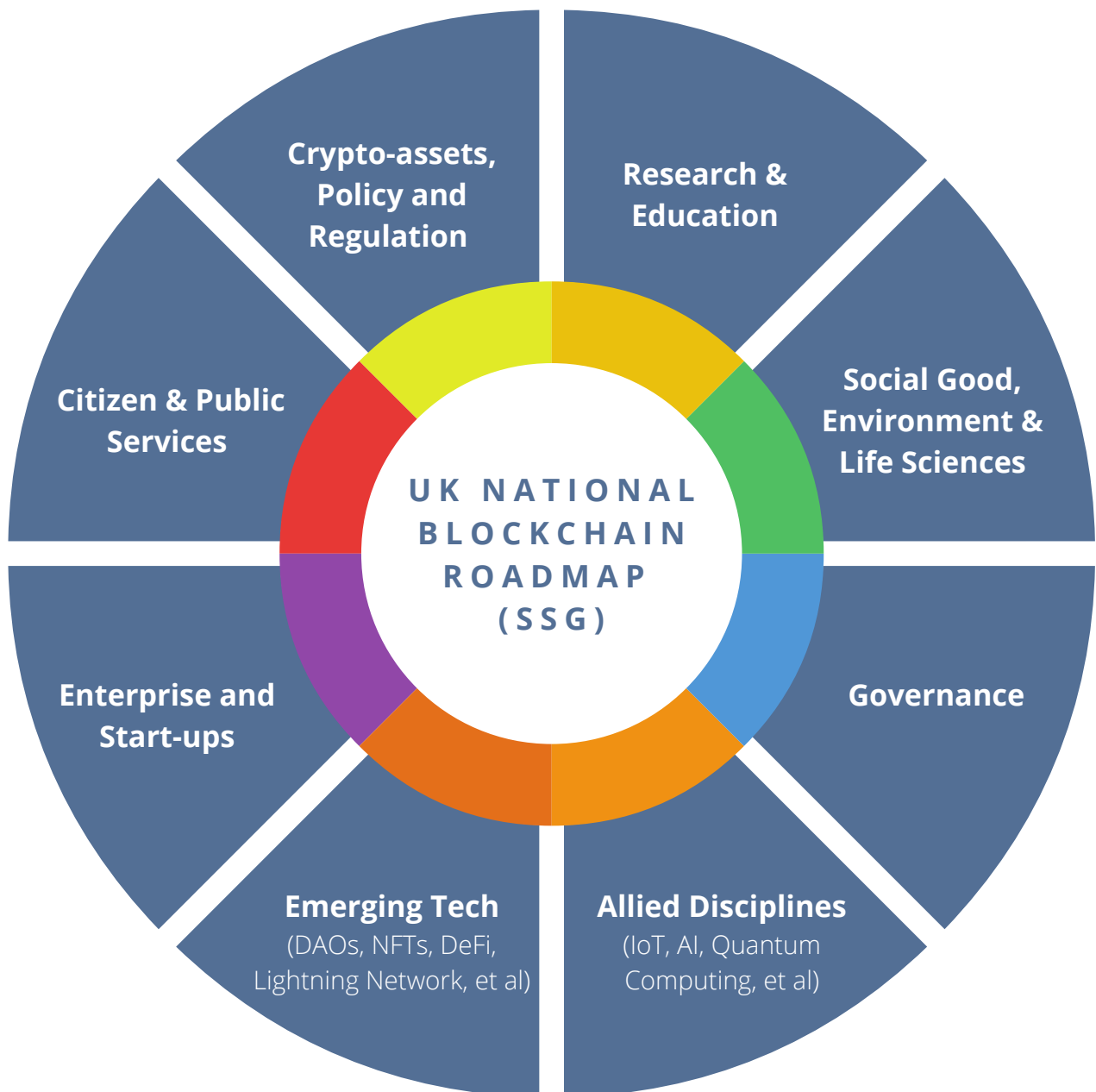
JORDAN



UK NATIONAL BLOCKCHAIN ROADMAP (NBR)

UK NATIONAL BLOCKCHAIN ROADMAP (NBR)

(VISION 2030)



SUB-SPECIALITY STEERING GROUPS (SSG)

Contribute to the UK National Blockchain Roadmap and join a Sub-Speciality Steering Group (SSG)

Contact us at cebb@britishblockchainassociation.org

Or visit:

<https://britishblockchainassociation.org/national-blockchain-roadmap-vision-2030/>



The British Blockchain Association
Advocating Evidence Based Blockchain

BBA FORUM | JULY 2024
WEDNESDAY, 3 JULY 2024, 3:30 PM UK

Venue: **BBA Metaverse Headquarters**
<https://britishblockchainassociation.org/Metaverse>

3:30 PM - 3:35 PM

BBA Ecosystem Updates

Deborah Cleary, Head of Partnerships, The BBA

3:35 PM - 3:42 PM

Decentralised Capabilities for B2B Commerce on Permissionsless Blockchains

Professor Dr Mary Lacity FBBA, Senior Editor, The JBBA

Professor of Information Systems, University of Arkansas, USA

3:42 - 3:50 PM

How to Review a Blockchain and Web3 Research Paper

Dr Sebastian Cochinescu, Senior Review Editor, The JBBA, Romania

3:50 - 4:00 PM

Blockchain for Transparent Procurement Processes between SMEs & Government

Dr Stella Bvuma, JBBA Author (doi.org/10.31585/jbba-7-1-1)2024)

Director, School of Information Systems, University of Johannesburg, South Africa

4:00 PM - 4:10 PM

How to Become a BBA Student Forum Lead

Professor Dr Naseem Naqvi MBE, President, The BBA, UK

Joey Vitale, BBA Student Forum Lead, University of Pennsylvania, USA

Khansa Rahim, BBA Student Forum Lead, COMSATS Institute of Technology, Pakistan



CEBB: Centre for Evidence-Based Blockchain



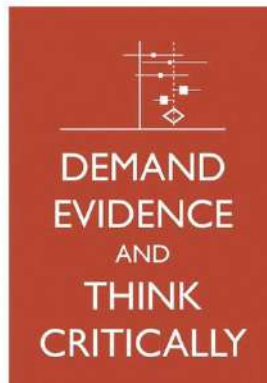
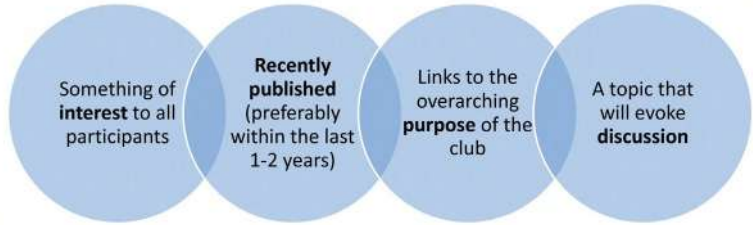
The British Blockchain Association
Advocating Evidence Based Blockchain

THE JBBA
THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION

BLOCKCHAIN
ASSOCIATIONS
FORUM

DISCLAIMER: The views, opinions and factual statements expressed during this webinar are the personal views of the speaker only and do not necessarily represent the official policy, position or views of their organisations.

Blockchain and Crypto-assets Journal Club:



The What & The Why

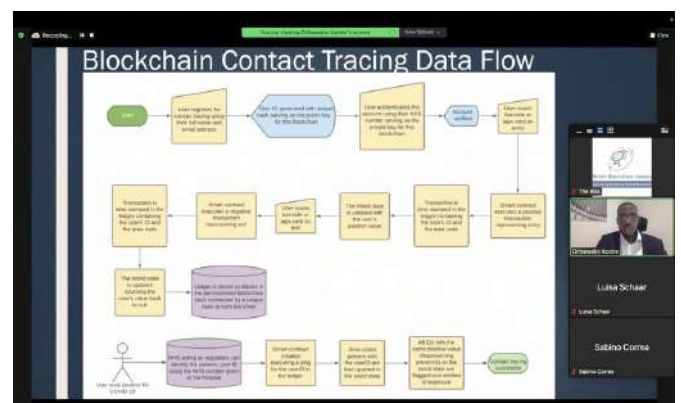
This research is about analysing the Crypto Trading environment under the fundamentals in terms of governance for any business:

Topic	Minimum Points	Maximum Points
Legal Compliance:		
Company name and Registry Identification	0	1
Key personnel and Management identification	0	1
Consent and Inconsent identification	0	1
Years of Activity		
Number of Years	0	3
Jurisdiction of Incorporation:		
Clear Jurisdiction of Incorporation	0	1
Clarity about Controller Jurisdiction Authority Regulation	0	1
Clearly presents as Authority regulated	0	3
Number of Points	0	11

Table 2 - KPI Score Summary

- Sample: Sample representing 99% of the daily trading volume as of 01-Jan-2020
- KPI: 78 Exchanges assessed under the KPI
- Fees: Analyse the fee structure of the group

Cross Results



BBA FORUM | MARCH 2022
SUNDAY, 27 MARCH 2022 (5 PM BST)

Sabino Correa
Eng. Master in Finance
CLSBE Lisbon
Certified Blockchain Expert
Frankfurt School of Finance & Management
MSc Sloan in Strategy and Leadership
London Business School

Crypto Governance: Analysing and Comparing Crypto Assets Trading Platforms

Published at the Journal of the British Blockchain Association Volume 3 - May/2020

Ortensio Ipkobe, Luisa Schaar





STUDENT FORUM

UNIVERSITY REPRESENTATIVE



britishblockchainassociation.org

THE BBA STUDENT FORUM

A BBA student chapter helps reinforce classroom and experiential learning. In addition to the learning that occurs during chapter meetings, the submission of research articles to the JBBA journal helps develop industry-specific skills, along with skills in project management, technical writing and interpersonal communications.

Chapter activities culminate at the annual scholars in Blockchain conference, where students interact with students from other chapters, BBA members and advisors and network with industry leaders, scientists, and researchers.

The BBA recognises that students are the future leaders of the industry, and treats them as such. Chapters instil future professionals with an understanding of the role that collaboration, research, development and networking plays in blockchain developments and industry progress.

REASONS TO START THE BBA STUDENT CHAPTER

Encourage student collaboration

Foster dialogue about trends, issues, movements, opportunities impacting the blockchain industry

Connect to industry professionals and career opportunities

Obtain leadership experience driving BBA student chapter activities

Form student and professional relationships across the BBA including those with students from other chapters

Compete in hacking events

Publish papers in the JBBA

DISCLAIMER

Publication in this journal of scientific, technical and literary material is open to all authors and readers. While every effort has been made to ensure articles published are free from typing, proof reading and formatting errors at the time of going to press, the publisher will be glad to be notified of any errors or omissions brought to our attention after the journal is published in the print format. Articles should not be taken to represent the policy or opinion of the British Blockchain Association, unless this is specifically stated. The publisher, affiliates of the British Blockchain Association, reviewers and editors assume no responsibility for any claims, instructions, methods or recommendations contained in the manuscripts. This publication is not a substitute for professional advice. The contents herein are correct at the time of printing and may be subject to change.

© The British Blockchain Association and The JBBA. All rights reserved.



is a trade mark of the Journal of the British Blockchain Association.

The JBBA is legally deposited at all 6 National Libraries of the UK and has become a part of the "British Heritage":

- British Library
- National Library of Scotland
- National Library of Wales
- Bodleian Libraries, University of Oxford
- Cambridge University Library
- Library, Trinity College Dublin

The JBBA is indexed in: **Directory of Open Access Journals (DOAJ)**, **Google Scholar** and **Web of Science**



Articles are indexed in **Semantic Scholar**, **Microsoft Academic** and available at online repositories at some of the most prestigious universities, worldwide.

The British Blockchain Association is a Publisher Member of:



The JBBA employs a plagiarism detection system. The JBBA is a peer reviewed journal. All manuscripts are reviewed by leaders in the appropriate field.

ISSN: 2516-3949

E-ISSN: 2516-3957

Online publication:

The articles published in this issue can be viewed Open Access on the JBBA website: jbba.scholasticahq.com

Advertising

All advertisements and sponsorships are expected to conform to ethical and business standards. The appearance of an advertisement or sponsorship material does not constitute an endorsement by the British Blockchain Association or by the Editor of this Journal.

Distribution

Print copies of the journal are sent worldwide to selected university libraries, policymakers, government officials, fin-tech organisations, eminent scholars, and major conferences. To request a print copy, please visit the journal website for more details.

Article Submission

To submit your manuscript to The JBBA, please visit:

<https://jbba.scholasticahq.com/for-authors>



FELLOWSHIP of The British Blockchain Association of The United Kingdom (FBBA)

An award of the Fellowship is recognition of exceptional achievement and contribution to Blockchain and allied disciplines. The Fellowship demonstrates a commitment to excellence, leadership, advancing standards and best practice, evidenced by a track record of outstanding contribution to the discipline of Blockchain or other Distributed Ledger Technologies.

FELLOWSHIP PRIVILEGES

- The use of 'FBBA' post-nominal
- Exclusive opportunity to officially represent the BBA by playing an active role in the direction and governance of the Association
- Privilege to take on a leadership role within the BBA and the profession as a whole
- Opportunity to represent the BBA at International Blockchain Conferences
- Significant discounts on BBA conferences and events
- Opportunity to join the Editorial Board of the JBBA
- Complimentary copy of the JBBA posted to your mailing address

The new Fellow appointments will be made twice a year (September and March).

Next Round of Fellowship Applications has been commenced (Applications submission Deadline: 15 July 2026)

For more information visit: britishblockchainassociation.org/fellowship or contact: fellowship@britishblockchainassociation.org

ENGAGE WITH THE BRITISH BLOCKCHAIN ASSOCIATION AND THE JBBA



'Like' and Share the latest JBBA and BBA updates on Facebook



Follow @Brit_blockchain to stay up-to-date on the latest news and announcements



Subscribe to our channel and view latest updates, research & education webinars, and cutting-edge scholarly content



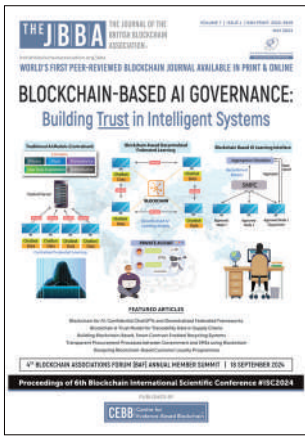
Follow us on Nostr, a fully decentralised, censorship resistant communications protocol with Bitcoin Lightning payments
@TheBBA@nostrplebs.com



Follow us on Medium to receive exclusive content and stories from the JBBA



Connect with the BBA's LinkedIn organisation profile and Follow us to receive real-time official updates



Volume 7 - Issue 1
May 2024



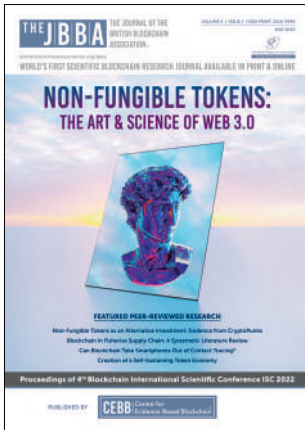
Volume 7 - Issue 2
November 2024



Volume 8 - Issue 1
May 2025



Volume 8 - Issue 2
November 2025



Volume 5 - Issue 1
May 2022



Volume 5 - Issue 2
November 2022



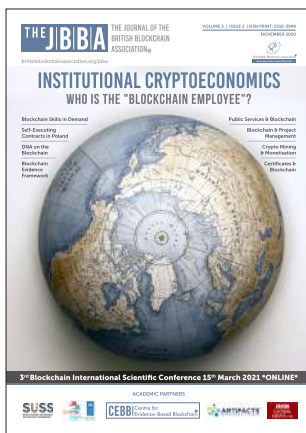
Volume 6 - Issue 1
May 2023



Volume 6 - Issue 2
November 2023



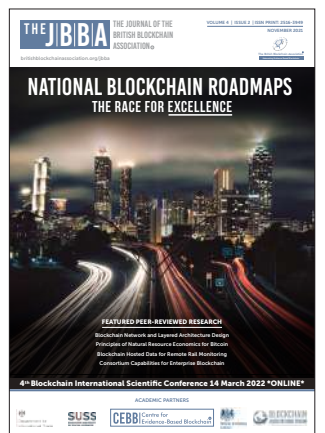
Volume 3 - Issue 1
May 2020



Volume 3 - Issue 2
November 2020



Volume 4 - Issue 1
May 2021



Volume 4 - Issue 2
November 2021



Volume 1 - Issue 1
July 2018



Volume 1 - Issue 2
December 2018



Volume 2 - Issue 1
May 2019



Volume 2 - Issue 2
October 2019



The British Blockchain Association[®]

Advocating Evidence Based Blockchain

www.britishblockchainassociation.org



THE J|B|B|A THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION[®]