



IntechOpen

Cryptocurrencies

Innovations, Challenges, and Future Prospects

Edited by Sam Goundar



Cryptocurrencies - Innovations, Challenges, and Future Prospects

Edited by Sam Goundar

Published in London, United Kingdom

Cryptocurrencies – Innovations, Challenges, and Future Prospects
<http://dx.doi.org/10.5772/intechopen.1008005>
Edited by Sam Goundar

Contributors

Andrea Romaoli Garcia, Basetty Mallikarjuna, Charles Chan, Karisma Karisma, Michael Lloyd, Nikolaos Eriotis, Nikolaos Papanikolaou, Paraskevi Boufounou, Puspaltha Chittem Setty, Sam Goundar, Sam Goundar

© The Editor(s) and the Author(s) 2026

The rights of the editor(s) and the author(s) have been asserted in accordance with the Copyright, Designs and Patents Act 1988. All rights to the book as a whole are reserved by INTECHOPEN LIMITED. The book as a whole (compilation) cannot be reproduced, distributed or used for commercial or non-commercial purposes without INTECHOPEN LIMITED's written permission. Enquiries concerning the use of the book should be directed to INTECHOPEN LIMITED rights and permissions department (permissions@intechopen.com).

Violations are liable to prosecution under the governing Copyright Law.



Individual chapters of this publication are distributed under the terms of the Creative Commons Attribution 4.0 License which permits commercial use, distribution and reproduction of the individual chapters, provided the original author(s) and source publication are appropriately acknowledged. If so indicated, certain images may not be included under the Creative Commons license. In such cases users will need to obtain permission from the license holder to reproduce the material. More details and guidelines concerning content reuse and adaptation can be found at <http://www.intechopen.com/copyright-policy.html>.

Notice

Statements and opinions expressed in the chapters are these of the individual contributors and not necessarily those of the editors or publisher. No responsibility is accepted for the accuracy of information contained in the published chapters. The publisher assumes no responsibility for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained in the book.

First published in London, United Kingdom, 2026 by IntechOpen
IntechOpen is the global imprint of INTECHOPEN LIMITED, registered in England and Wales, registration number: 11086078, 167-169 Great Portland Street, London, W1W 5PF, United Kingdom

For EU product safety concerns: IN TECH d.o.o., Prolaz Marije Krucifikse Kozulić 3, 51000 Rijeka, Croatia, info@intechopen.com or visit our website at intechopen.com.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Cryptocurrencies – Innovations, Challenges, and Future Prospects
Edited by Sam Goundar

p. cm.

Print ISBN 978-1-83635-719-3

Online ISBN 978-1-83635-718-6

eBook (PDF) ISBN 978-1-83635-720-9

If disposing of this product, please recycle the paper responsibly.

Meet the editor



Professor Dr. Sam Goundar is an internationally recognised academic, researcher, and keynote speaker with over 30 years of teaching experience across 14 universities in 12 countries. His expertise spans emerging and transformative technologies, including Artificial Intelligence, Blockchain, Cryptocurrencies, Educational Technologies, Data Science, and Cyber Security. He is a Senior Member of the IEEE and a member of the Association

for Computing Machinery and the Australian Computer Society. Professor Goundar serves as Editor-in-Chief of multiple international peer-reviewed journals and has played a significant role in advancing scholarly research in digital technologies and computational innovation. He has authored and edited 21 academic books and published more than 156 peer-reviewed journal articles and book chapters in reputable international outlets. His research focuses on the governance, security, and interdisciplinary integration of advanced digital systems, particularly within decentralised and blockchain-based infrastructures. Through global research collaborations, invited keynote addresses, and editorial leadership, Professor Goundar continues to contribute to the evolution of technology-driven innovation, digital governance frameworks, and transformative education in emerging technological ecosystems.

Contents

Preface	IX
Chapter 1	1
Introductory Chapter: Cryptocurrencies – Innovations, Challenges, and Future Prospects <i>by Sam Goundar</i>	
Chapter 2	13
Integration of AI and ML in Cryptoeconomics <i>by Basetty Mallikarjuna, Pupalatha Chittem Setty and Sam Goundar</i>	
Chapter 3	27
Determinants of Fintech Adoption: A Systematic Review Integrating Trust, Security, and User Perceptions within Technology Acceptance Frameworks <i>by Nikolaos Papanikolaou, Paraskevi Boufounou and Nikolaos Eriotis</i>	
Chapter 4	61
Regulating the Future: Global Infrastructure, Compliance, and the Role of Digital Currencies <i>by Andrea Romaoli Garcia</i>	
Chapter 5	81
Perspective Chapter: Central Bank Digital Currency and Financial Crime Regulations <i>by Charles Chan</i>	
Chapter 6	101
Perspective Chapter: The Future of Wholesale CBDCs in a Tokenizing and Trumpian World <i>by Michael Lloyd</i>	
Chapter 7	125
Blockchain Reshaping Energy Markets: Regulatory Frameworks for Sustainability-Driven Energy Tokens <i>by Karisma Karisma and Sam Goundar</i>	

Preface

Cryptocurrencies have emerged as transformative forces in the global financial ecosystem, offering innovative solutions for transactions, investments, and decentralized operations. What began as a cryptographic experiment has gradually evolved into a serious infrastructure discussion that now engages governments, regulators, technologists, financial institutions, and scholars worldwide. This book, *Cryptocurrencies – Innovations, Challenges, and Future Prospects*, provides a comprehensive exploration of the cryptocurrency landscape, combining foundational concepts with contemporary research and practical applications, while situating these developments within a broader governance and institutional context.

The rise of cryptocurrencies goes beyond the appearance of new digital assets. It reflects a structural shift in how value is conceptualised, verified, and exchanged in digitally interconnected societies. Distributed ledger technologies have introduced alternative models of trust that do not rely exclusively on centralised intermediaries. At the same time, these systems raise profound questions concerning regulation, accountability, compliance, and long-term sustainability. The global financial system is being reimaged in real time, and cryptocurrencies stand at the centre of that reconfiguration.

This volume is conceived primarily as a governance and infrastructure-oriented contribution to the field. While much public discourse focuses on market volatility or speculative investment, the enduring relevance of cryptocurrencies will depend on the maturity of their regulatory frameworks, security architectures, institutional safeguards, and integration with national and transnational financial systems. Without coherent governance structures, technological innovation alone cannot sustain long-term legitimacy.

The chapters in this book explore the technological underpinnings of cryptocurrencies, including blockchain architectures, cryptographic mechanisms, decentralised networks, and the emerging integration of artificial intelligence and machine learning within cryptoeconomic systems. These technological foundations are examined alongside persistent challenges, including security vulnerabilities, scalability constraints, interoperability concerns, and regulatory compliance requirements. By placing innovation and risk within the same analytical frame, the book acknowledges both the transformative potential and the structural fragilities of contemporary cryptocurrency ecosystems.

Beyond foundational technologies, the volume addresses the expanding use cases of cryptocurrencies in payment systems, tokenisation frameworks, decentralised finance, and sector-specific applications. The reshaping of energy markets through blockchain-enabled systems illustrates how distributed infrastructures are beginning to influence industries beyond traditional finance. Such developments underscore a

central theme of this book: cryptocurrencies are not isolated financial instruments but components of a broader digital transformation that intersects with economic governance, sustainability, and global coordination.

Regulation and monetary policy form a critical axis of discussion throughout the volume. The emergence of Central Bank Digital Currencies introduces new dynamics in sovereign monetary control, financial crime prevention, and cross-border interoperability. At the same time, regulatory harmonisation remains uneven across jurisdictions, creating both innovation opportunities and compliance uncertainties. The analysis presented here recognises that future cryptocurrency ecosystems will operate within increasingly complex legal and geopolitical environments.

Emphasising forward-looking trends, the book also examines quantum-safe encryption, interoperability architectures, algorithmic intelligence within blockchain networks, and the long-term implications of digital currencies for emerging markets. As computational capabilities advance and artificial intelligence becomes further embedded within financial systems, the security assumptions underlying current cryptographic protocols must be reassessed. Questions of resilience, adaptability, and technological foresight become central to responsible innovation.

Importantly, this volume adopts an interdisciplinary perspective. Cryptocurrencies cannot be adequately understood through a single disciplinary lens. They involve technological engineering, behavioural adoption models, regulatory theory, monetary economics, security architecture, and ethical governance considerations. The contributors to this book approach the subject from diverse academic and professional backgrounds, collectively reflecting the complexity of a rapidly evolving digital ecosystem.

As editor, I have intended to curate a collection of chapters that move beyond surface-level commentary. The objective is neither to promote uncritical enthusiasm nor to dismiss the transformative capacity of decentralised systems. Rather, this book seeks to examine how innovation, governance, institutional design, and public trust must evolve together if cryptocurrencies are to contribute meaningfully to global digital infrastructure.

Cryptocurrencies remain contested. They generate optimism about financial inclusion, transparency, and decentralisation, while simultaneously raising concerns about volatility, illicit use, systemic risk, and regulatory arbitrage. However, it is precisely within this tension that rigorous scholarship becomes necessary. The future of cryptocurrencies will not be determined solely by technological breakthroughs, but by the alignment of policy, institutional frameworks, ethical standards, and global cooperation.

Designed for academics, researchers, industry professionals, regulators, and policy-makers, this volume aims to bridge theoretical advancement and practical implementation. It provides structured insight into the evolving governance architecture of digital currencies while anticipating the next phase of infrastructural transformation. In an era increasingly defined by digital sovereignty, tokenised assets, and algorithmically mediated financial systems, thoughtful engagement is essential.

We are entering a period in which digital currencies, decentralised infrastructures, and intelligent computational systems will intersect more deeply with questions of sovereignty, sustainability, and economic resilience. Whether cryptocurrencies mature into stable components of global financial architecture will depend on how effectively governance mechanisms, technological safeguards, and interdisciplinary collaboration evolve. I hope that this book contributes, in a considered and forward-looking manner, to that ongoing conversation.

Sam Goundar
University of Central Asia,
Naryn, Kyrgyzstan

Introductory Chapter: Cryptocurrencies – Innovations, Challenges, and Future Prospects

Sam Goundar

1. Introduction

Over the past decade, the global financial landscape has undergone an unprecedented transformation driven by advances in distributed ledger technologies and the growing appetite for decentralized systems of trust. Cryptocurrencies are digital assets built on blockchain infrastructures that have evolved from a fringe innovation into a catalyst for re-imagining money, governance, and data integrity. As Goundar and Anandan [1] observe, emerging technologies such as blockchain and artificial intelligence are not merely altering how systems operate but are reshaping the very logic of digital participation and economic exchange. The accelerating pace of adoption illustrates what Catalini and Gans [2] describe as a fundamental shift in the economics of information, where transaction verification and record-keeping are no longer monopolies of centralized institutions.

The genesis of this movement lies in frustration with traditional finance and its opacity. Following the 2008 global recession, trust in banks and regulators eroded, paving the way for a peer-to-peer alternative. Nakamoto's [3] white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, proposed a mechanism that used cryptographic consensus rather than institutional authority to validate transactions. This innovation established blockchain as a transparent and tamper-evident ledger, inspiring subsequent systems built on similar principles. Goundar [4] argues that this development marked the dawn of a "trust protocol," one that decentralizes confidence itself rather than simply digitizing money. In this sense, blockchain is not merely a technical architecture but a social contract encoded in mathematics, a notion that underpins every major cryptocurrency today.

The growing acceptance of cryptocurrencies reflects deeper socio-economic transitions. Baur and Dimpfl [5] note that Bitcoin's extreme volatility has not prevented its recognition as both an asset class and a hedge against institutional instability. Meanwhile, governments and corporations are experimenting with blockchain-based applications for remittances, supply-chain management, and identity verification [6]. This convergence of private innovation and public experimentation signals a turning point: digital currencies are no longer a technological curiosity but a legitimate element of financial infrastructure. As Tiwari et al. [7] emphasize, the trajectory of such innovations depends on how well societies balance openness with oversight, creativity with accountability.

The global conversation around cryptocurrencies is shaped by this tension between promise and peril. Scholars, practitioners, and policymakers are increasingly exploring cryptocurrencies as technological systems, socio-economic phenomena, and ethical experiments in decentralization. The aim is not only to describe what cryptocurrencies are but to interrogate what they mean for markets, for governance, and for the future of human collaboration. A growing body of work now seeks to bridge the divide between theory and real-world practice [8].

Cryptocurrencies continue to evolve from niche experiments into influential systems that challenge legacy institutions. Their development reveals a central insight: cryptocurrencies are not just about code or currency, they are about trust, power, and the continuous negotiation between innovation and responsibility. Understanding their trajectory requires examining historical foundations, technological implications, social impacts, and the controversies that shape them. Taken together, these dimensions underscore why cryptocurrencies are not simply a technological trend, but a profound catalyst for rethinking how value, governance, and participation function in the digital age.

2. The evolution of cryptocurrencies

The story of cryptocurrencies is one of continuous experimentation, beginning decades before Bitcoin's rise. Early digital-cash systems, such as *DigiCash* and *e-Gold* in the 1990s, sought to create electronic value transfer mechanisms, but their reliance on central authorities led to regulatory pressure and eventual collapse [9]. These initial efforts, however, planted the conceptual seeds for decentralized money, systems that could operate without banks, borders, or intermediaries. As Goundar et al. [10] note, technological revolutions often begin on the margins, dismissed as impractical until social and economic crises expose the fragility of existing models.

The turning point came in 2008 when *Satoshi Nakamoto* introduced Bitcoin, a peer-to-peer digital currency that merged cryptography, distributed computing, and game theory into a single trustless framework [3]. Bitcoin's introduction was not merely a technical breakthrough but a philosophical one, it challenged the necessity of centralized oversight in verifying financial transactions. In the years that followed, open-source communities expanded Bitcoin's architecture, and mining became both a security mechanism and an economic incentive [2, 9]. The early adoption period revealed two key insights: decentralization could scale, and trust could be programmed.

By 2015, *Ethereum* extended this foundation by introducing programmable logic through *smart contracts*, a self-executing code that enables automated, conditional transactions [11]. This innovation turned the blockchain from a payment system into a computational platform capable of supporting entire decentralized applications (DApps). As Harvey et al. [12] explain, Ethereum's flexibility gave rise to the *Decentralized Finance (DeFi)* movement, allowing borrowing, lending, and trading to occur without banks or brokers. The emergence of tokens, non-fungible assets (NFTs), and decentralized autonomous organizations (DAOs) in subsequent years demonstrated how the blockchain could underpin entirely new economic ecosystems.

Governments and regulatory institutions gradually began to recognize the transformative potential of blockchain-based digital currency systems. Lee et al. [13] reported that more than 90 central banks worldwide are exploring or piloting *Central Bank Digital Currencies (CBDCs)* as secure, regulated alternatives to cryptocurrencies.

This institutional embrace signals that blockchain is evolving from a countercultural innovation to a foundational layer of modern finance. Harvey et al. [12] describe this phase as the “convergence era,” where public institutions and decentralized systems coexist, influencing one another’s growth.

From the collapse of early digital-cash experiments to the emergence of sovereign digital currencies, the evolution of cryptocurrencies reveals a continuous pursuit of trust without centralization. As Goundar [4] emphasizes, each iteration from Bitcoin’s genesis block to Ethereum’s smart contracts, represents not only technological progress but also a philosophical redefinition of how societies exchange value, negotiate power, and envision the future of finance.

3. The transformational role of cryptocurrencies

The transformational power of cryptocurrencies lies in their ability to reconstruct the foundations of financial trust, governance, and inclusion. Traditional finance depends on centralized intermediaries such as banks, clearinghouses, and regulators to authenticate transactions. Cryptocurrencies replace these gatekeepers with code, consensus, and cryptography, effectively redefining the architecture of trust [14]. As Goundar and Anandan [1] notes, decentralization is not just a technical concept but an ideological one, shifting control from institutions to individuals. This redistribution of trust has made cryptocurrencies an essential instrument for financial autonomy in both developed and emerging economies.

Nowhere is this transformation more visible than in the realm of financial inclusion. Billions of people worldwide remain unbanked or underbanked due to limited access to traditional financial systems. The World Bank Group [15] highlights how mobile-based wallets and blockchain-enabled payment systems have bridged this gap, allowing secure participation in digital economies without dependence on physical banking infrastructure. In sub-Saharan Africa, for example, blockchain-based remittance solutions have reduced transfer costs and improved transparency [16]. These developments illustrate what Goundar and Anandan [1] calls “technological inclusion”, that is the use of innovation as a social equalizer in global development contexts.

The industrial and governmental adoption of blockchain has expanded its influence beyond payments and remittances. Corporations such as IBM, Maersk, and Visa now employ blockchain for supply-chain integrity, data verification, and cross-border settlements [17]. Simultaneously, the emergence of DAOs has introduced new governance models that embody collective decision-making without hierarchy. Li and Chen [18] argue that DAOs demonstrate how financial and organizational power can be redefined through transparent, algorithmic rules, a concept that aligns with [19] observation that distributed technologies promote accountability when designed around ethical principles.

Case studies reveal both promise and complexity. *El Salvador’s* adoption of Bitcoin as legal tender in 2021 illustrates an ambitious attempt to integrate decentralized finance into national economic policy. While the move showcased innovation, it also exposed volatility and infrastructural fragility [20]. In contrast, smaller-scale applications such as blockchain-based identity projects in Estonia and Sierra Leone demonstrate sustainable, citizen-centered innovation. These examples suggest that cryptocurrencies, when paired with good governance, can strengthen transparency and inclusivity.

In essence, the transformative role of cryptocurrencies extends far beyond speculation or technology. It signals a deeper rethinking of what constitutes money, authority, and participation in the digital age. As Goundar and Anandan [1] emphasize, the movement toward decentralized economies is less about replacing institutions and more about redefining collaboration, accountability, and trust in a hyperconnected world.

4. Challenges and controversies

While cryptocurrencies represent one of the most transformative financial innovations of the twenty-first century, they also embody a paradox; systems built on transparency often operate in markets clouded by uncertainty, volatility, and misinformation. As Bajra and Aliu [21] highlight, cryptocurrency prices fluctuate more violently than traditional assets, reflecting speculative behavior rather than intrinsic value. Such volatility undermines their use as stable mediums of exchange. Yet, this instability is characteristic of early technological paradigms, and innovation tends to precede regulation, and markets mature through cycles of experimentation and correction.

Security and fraud pose another persistent challenge. The open and pseudonymous nature of blockchain transactions have facilitated unprecedented freedom but have also created fertile ground for cyber-crime. Conti et al. [22] provide a detailed taxonomy of common vulnerabilities, from exchange hacks and ransomware payments to rug pulls and phishing attacks. The *Mt. Gox* collapse and *FTX* insolvency serve as cautionary tales of weak governance and inadequate custodial safeguards [23]. These incidents underscore the urgent need for stronger auditing, transparency, and the integration of AI-based detection systems to counter digital fraud.

Regulation and compliance remain equally complex. Global policy responses to cryptocurrencies vary widely from supportive innovation sandboxes in Singapore and Switzerland to strict prohibitions in China and India. Kandpal et al. [24] argue that the challenge for regulators lies in achieving balance: protecting investors without stifling creativity. The *European Union's 2023 Markets in Crypto-Assets (MiCA)* regulation represents one of the first comprehensive frameworks addressing these tensions by introducing consumer protection and transparency obligations. However, in many developing economies, the absence of clear legal categories for cryptocurrencies leads to fragmented oversight and inconsistent enforcement [25].

Environmental sustainability has also become a flashpoint in the debate. Proof-of-Work (PoW) blockchains, particularly Bitcoin, require immense computational power, raising concerns about carbon emissions and energy consumption. Kohli et al. [26] argue that this environmental cost could undermine the technology's social license to operate. Emerging alternatives such as Proof-of-Stake (PoS) and green-mining initiatives aim to mitigate this impact. Ethereum's 2022 transition to PoS demonstrates that sustainability and innovation can coexist when guided by responsible governance.

Ultimately, these controversies illustrate the maturing of an ecosystem learning to regulate itself. The collapse of unregulated exchanges, the tightening of compliance standards, and the global push for green innovation mark a turning point in crypto's evolution. The future of digital assets depends not on the absence of regulation but on designing ethical frameworks that foster innovation while preserving public trust.

5. Technological innovations driving cryptocurrencies

The sustainability and scalability of cryptocurrencies depend largely on the evolution of the technologies that underpin them. As Belchior et al. [27] explain, blockchain architectures continue to mature through innovations in consensus mechanisms, interoperability, and computational efficiency. The shift from Proof-of-Work (PoW) to Proof-of-Stake (PoS) represents a major milestone in addressing energy consumption and transaction latency. Ethereum's *Merge* in 2022 reduced energy usage by over 99%, demonstrating that distributed systems can evolve without compromising security. According to Goundar and Anandan [1], this transition illustrates a broader pattern within emerging technologies, where iterative refinements rather than radical replacements define progress.

Scalability has long been one of the central obstacles to mass adoption. *Layer-2* protocols such as the Lightning Network for Bitcoin and Polygon for Ethereum have dramatically increased throughput by processing transactions off-chain while maintaining main-chain integrity [28]. These solutions showcase the growing modularity of blockchain ecosystems where separate layers manage settlement, computation, and privacy independently yet cohesively. Interoperability frameworks like *Cosmos* and *Polkadot* further extend this capability, enabling assets and data to flow securely across previously isolated blockchains. Belchoir et al. [27] contend that these designs represent the “Internet of Blockchains,” in which diverse ecosystems communicate through standardized protocols, much like the early evolution of TCP/IP for the web.

Beyond consensus and scaling, the integration of Artificial Intelligence (AI) and the Internet of Things (IoT) is reshaping how cryptocurrencies interact with data and automation. Goundar [29] highlights that blockchain's immutability offers an ideal foundation for AI-based analytics and machine-learning models that require verified, tamper-resistant data streams. In IoT contexts, blockchain enables secure machine-to-machine micropayments, facilitating autonomous communication among sensors, drones, or vehicles. Goundar and Anandan [1] observe that this convergence between AI, blockchain, and cyber security not only enhances technical resilience but also opens new frontiers in digital trust and predictive intelligence.

Emerging research also anticipates a quantum-resistant era. With advances in quantum computing threatening current cryptographic standards, post-quantum algorithms are being explored to ensure blockchain longevity [30]. These include lattice-based and hash-based signature schemes that could secure distributed ledgers against future computational attacks. The preparedness of blockchain systems for quantum disruption will determine their role in next-generation digital infrastructures.

Collectively, these innovations indicate that cryptocurrencies are far from static; they are living systems evolving through a global collaboration of engineers, researchers, and communities. The progress from basic cryptographic consensus to AI-integrated, quantum-safe, interoperable ecosystems reflects not only technological ingenuity but also a sustained human pursuit to build systems that are secure, inclusive, and enduring.

6. Ethical, legal, and regulatory perspectives

The rapid ascent of cryptocurrencies has outpaced the development of consistent legal and ethical frameworks to govern them. As Bodo and De Filippi [31] explain,

financial regulation traditionally relies on centralized accountability, whereas blockchain-based systems are designed to operate without intermediaries. This structural inversion challenges existing legal paradigms around ownership, responsibility, and jurisdiction. According to Goundar [10], such disruption requires not just policy adaptation but a rethinking of how digital ethics can be codified into decentralized systems. The question is no longer whether cryptocurrencies should be regulated, but how regulation can coexist with innovation.

Around the world, responses to this dilemma vary widely. The European Union's *Markets in Crypto-Assets (MiCA)* framework, introduced in 2023, represents a significant step toward harmonized governance, providing investor protection, anti-money-laundering measures, and environmental disclosure requirements [32]. In contrast, the United States still grapples with defining whether cryptocurrencies constitute securities or commodities, leading to overlapping jurisdiction among agencies. Meanwhile, countries like Singapore and Switzerland promote regulatory "sandboxes" that foster innovation within controlled environments [33]. These divergent models highlight a global experiment in finding equilibrium between risk mitigation and technological progress.

Beyond compliance, ethical challenges define the moral boundaries of decentralization. As Sangal et al. [34] argue, blockchain's capacity for anonymity, while protecting user freedom, also enables illicit behavior and raises questions about surveillance and privacy. The rise of privacy-enhancing tools, mixers, tumblers, and zero-knowledge proofs further complicates this ethical landscape. They note that the same technologies used to preserve digital rights can also obscure criminal activity, reinforcing the need for ethical design that anticipates dual-use outcomes.

DAOs add yet another layer of complexity. With decision-making distributed across code-governed networks, legal accountability becomes diffuse. Cheng [35] observes that the absence of legal personality in DAOs creates ambiguities around liability and enforcement. Some jurisdictions have begun experimenting with DAO registration frameworks to address these concerns, blending corporate law with algorithmic governance. The broader lesson is that technology and regulation must evolve symbiotically, neither should dominate the other, for the legitimacy of digital economies depends on both innovation and integrity.

In sum, the ethical and regulatory questions surrounding cryptocurrencies are not peripheral, they are central to their sustainability. A future of responsible decentralization will depend on transparent governance models, cross-border legal cooperation, and education systems that embed ethical reasoning into technological design.

7. Future prospects and emerging trends

The evolution of cryptocurrencies now stands at a crossroads, where innovation intersects with institutional integration. As Ghosh et al. [36] suggest, the next stage of blockchain's journey will be defined by Web3, a decentralized internet architecture that reimagines ownership, identity, and participation. Unlike Web2, which centralizes data within corporate ecosystems, Web3 empowers users to control digital assets, manage identity credentials, and even participate in decentralized governance through tokenized voting. They observe that this emerging paradigm reflects a societal shift toward participatory technology, one where users are not just consumers but co-creators of the digital economy.

Central Bank Digital Currencies (CBDCs) are likely to coexist with decentralized assets, creating hybrid monetary systems that combine state oversight with blockchain efficiency. Lee et al. [13] report that more than 90 countries are developing CBDC prototypes or pilots, each exploring the balance between privacy and traceability. Tsareva and Komarov [16] note that these sovereign digital currencies could stabilize the financial ecosystem while legitimizing blockchain infrastructures. The coexistence of centralized and decentralized currencies may also produce new tensions over data sovereignty, surveillance, and monetary control.

Beyond policy evolution, technological convergence will define the next wave of crypto innovation. The fusion of blockchain, artificial intelligence (AI), and the Internet of Things (IoT) is paving the way for intelligent, self-regulating networks capable of automating compliance and optimizing resource allocation [8]. These integrations can transform finance, logistics, and governance, but they also demand resilient frameworks for privacy and accountability. As Goundar [8] has emphasized, the challenge is not merely to connect technologies but to align them ethically so that machine intelligence and distributed ledgers reinforce transparency rather than amplify bias.

Sustainability is another defining trend. Environmental scrutiny following Bitcoin's energy-intensive mining practices has led to the rise of carbon-neutral and proof-of-stake protocols. Shin and Rice [37] describe this transition as a "green renaissance" for blockchain, where technical efficiency becomes synonymous with moral legitimacy. Such progress illustrates that ethical innovation guided by global cooperation will determine the long-term credibility of digital economies.

Looking ahead, the future of cryptocurrencies will depend less on technical breakthroughs and more on collective intent. The interplay between technological ingenuity, governance maturity, and societal trust will shape whether cryptocurrencies become tools of empowerment or instruments of exclusion. The next frontier will not be measured by the sophistication of algorithms but by our capacity to build technologies that sustain equity, accountability, and human dignity.

8. Concluding reflections

Cryptocurrencies represent more than a technological breakthrough; they embody an ongoing transformation in how societies define value, trust, and participation in an increasingly digitized world. Their evolution has prompted new intersections between finance, policy, and computer science, while also surfacing unresolved questions about ethics, regulation, sustainability, and equity. The continued advancement of decentralized systems will require dialog across disciplines and institutions to ensure that innovation strengthens rather than undermines public trust.

Understanding cryptocurrencies therefore requires a holistic perspective. Blockchain should be seen not only as a technical architecture but also as a socio-economic experiment in shared governance and digital empowerment. The future of decentralized technologies will be shaped not only by cryptographic protocols or scalability breakthroughs but also by the collective choices societies make about transparency, inclusivity, and responsibility in digital economies.

As cryptocurrencies continue to influence global finance, governance models, and technological infrastructure, the coming era will be defined by how thoughtfully their potential is integrated with ethical and regulatory foresight. Innovation may drive

progress, but integrity will determine its legitimacy. This is the central challenge and promise of decentralized systems: to build technologies that not only disrupt but also uplift, connect, and sustain. The choices we make today will shape whether these systems become tools for empowerment or instruments of exclusion in the decades ahead. Ultimately, the future of cryptocurrencies will reflect not just technical ambition, but society's collective values and the human vision guiding their development.

Author details

Sam Goundar
School of Arts and Sciences University of Central Asia Naryn, Kyrgyzstan

*Address all correspondence to: sam.goundar@ucentralasia.org

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Goundar S, Anandan R. Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations. Berlin, Germany: Springer Nature; 2023
- [2] Catalini C, Gans JS. Some simple economics of the blockchain. *Communications of the ACM*. 2020;**63**(7):80-90
- [3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. Available from: <https://bitcoin.org/bitcoin.pdf>
- [4] Goundar S, editor. Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends. Singapore: World Scientific; 2020
- [5] Baur DG, Dimpfl T. The volatility of bitcoin and its role as a medium of exchange and a store of value. *Empirical Economics*. 2021;**61**(5):2663-2683
- [6] Jegerson D, Mertzanis C. Deciphering the role of cryptocurrencies in global remittances: A comprehensive literature review. *Management & Sustainability: An Arab Review*. 2025;**4**(2):268-291
- [7] Tiwari V, Goundar S, Teja KBR, Agarwal B, Harjule P. A transparent, distributed, and secure crowdfunding platform based on Blockchain. In: *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations*. Cham: Springer International Publishing; 2023. pp. 185-199
- [8] Goundar S. Introduction to the convergence of artificial intelligence with blockchains: Challenges and opportunities. In: *Convergence of Artificial Intelligence and Blockchain Technologies, The: Challenges and Opportunities*. Singapore: World Scientific Publishing; 2022
- [9] Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. New Jersey, USA: Princeton University Press; 2016
- [10] Goundar S, Tabunakawai N, Tamata J, Deb A, Nusair S. Cryptocurrencies - An assessment of global adoption trends. In: *Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends*. Singapore: World Scientific Publishing; 2021. pp. 231-248
- [11] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, 151. 2014. pp. 1-32
- [12] Harvey CR, Ramachandran A, Santoro J. *DeFi and the Future of Finance*. New Jersey, USA: John Wiley & Sons; 2021
- [13] Lee DKC, Yan L, Wang Y. A global perspective on central bank digital currency. *China Economic Journal*. 2021;**14**(1):52-66
- [14] Garriga M, Dalla Palma S, Arias M, De Renzis A, Pareschi R, Andrew Tamburri D. Blockchain and cryptocurrencies: A classification and comparison of architecture drivers. *Concurrency and Computation: Practice and Experience*. 2021;**33**(8):e5992
- [15] World Bank Group. *Regulation and Supervision of Fintech: Considerations for EMDE Policymakers*. Washington, DC, USA: World Bank; 2022. Available from: <https://openknowledge.worldbank.org/>

org/entities/publication/41a3b4d2-1c86-5783-aac4-922cab79d845

[16] Tsareva A, Komarov M. Retail central bank digital currency design choices: Guide for policymakers. *IEEE Access*. 2024;**12**:66129-66146

[17] Rajput N, Garg V, Alavardov E, Jyotsna, Varmani SG. International business and block-chain ventures. In: *Industry 4.0 and the Digital Transformation of International Business*. Singapore: Springer Nature Singapore; 2023. pp. 69-83

[18] Li S, Chen Y. Governing decentralized autonomous organizations as digital commons. *Journal of Business Venturing Insights*. 2024;**21**:e00450

[19] Pandey R, Goundar S, Fatima S, editors. *Distributed Computing to Blockchain: Architecture, Technology, and Applications*. Amsterdam, Netherlands: Elsevier; 2023

[20] Attri S, Gupta S, Singh S. Examining cryptocurrency versatility: Is it a currency or an investment asset? *Journal of Economic and Administrative Sciences*. 2025

[21] Bajra UQ, Aliu F. Deciphering the cryptocurrency conundrum: Investigating speculative characteristics and volatility. *Finance Research Letters*. 2023;**58**:104589

[22] Conti M, Gangwal A, Lal C, Ruj S. Bitcoin blockchain system: An overview of security and privacy aspects. In: *Blockchains: A Handbook on Fundamentals, Platforms and Applications*. Berlin, Germany: Springer; 2023. pp. 75-108

[23] Conlon T, Corbet S, Hu Y. The collapse of the FTX exchange: The end of cryptocurrency's age of innocence. *The British Accounting Review*. 2023:101277

[24] Kandpal V, Ozili PK, Jeyanthi PM, Ranjan D, Chandra D. Regulation of the Fintech industry. In: *Digital Finance and Metaverse in Banking: Decoding a Virtual Reality towards Financial Inclusion and Sustainable Development*. Leeds, UK: Emerald Publishing Limited; 2025. pp. 181-198

[25] Staley I, Amankwa E. Bridging Blockchain and digital asset gaps: A comparative policy analysis of regulatory practices in emerging markets. *IET Blockchain*. 2025;**5**(1):e70019

[26] Kohli V, Chakravarty S, Chamola V, Sangwan KS, Zeadally S. An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions. *Digital Communications and Networks*. 2023;**9**(1):79-89

[27] Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*. 2021;**54**(8):1-41

[28] Rebello GAF, Camilo GF, de Souza LAC, Potop-Butucaru M, de Amorim MD, Campista MEM, et al. A survey on blockchain scalability: From hardware to layer-two protocols. *IEEE Communications Surveys & Tutorials*. 2024;**26**(4):2411-2458

[29] Goundar S. Blockchain-AI integration for resilient real-time cyber security. In: *Global Congress on Emerging Technologies (GCET-2024)*. New York, USA: IEEE; 2024. pp. 342-349

[30] Revathi K, Suganthi K. Enhancing blockchain security against quantum threats through integration of post-quantum cryptographic algorithms. *Computers and Electrical Engineering*. 2025;**127**:110610

[31] Bodo B, De Filippi P. Trust in context: The impact of regulation on blockchain and DeFi. *Regulation & Governance*. 2025;**19**(3):740-760

[32] European Commission. Markets in Crypto-Assets (MiCA) Regulation. Brussels: EU Publications; 2023

[33] OECD. International Standards for Automatic Exchange of Information in Tax Matters - Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard. Paris, France: OECD; 2023. Available from: https://www.oecd.org/en/publications/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en.html

[34] Sangal S, Duggal G, Nigam A. Blockchain's double-edged sword: Thematic review of illegal activities using blockchain. *Journal of Information, Communication and Ethics in Society*. 2024;**22**(1):58-81

[35] Cheng KY. The legal structure of decentralised autonomous organisations (DAOs): Governance, legal personality and liability. *Information & Communications Technology Law*. 2025;**34**(3):262-278

[36] Ghosh A, Hassija V, Chamola V, El Saddik A. A survey on decentralized metaverse using blockchain and web 3.0 technologies, applications, and more. *IEEE Access*. 2024

[37] Shin D, Rice J. Cryptocurrency: A panacea for economic growth and sustainability? A critical review of crypto innovation. *Telematics and Informatics*. 2022;**71**:101830

Integration of AI and ML in Cryptoeconomics

*Basetty Mallikarjuna, Puspalatha Chittem Setty
and Sam Goundar*

Abstract

The integration of three different domains: artificial intelligence (AI) and machine learning (ML) and advanced deep learning (DL) algorithms with blockchain and cryptocurrency ecosystems is revolutionizing financial technologies. The “Cryptoeconomics” word born from the intersection of cryptography, economics, and decentralized computation. It has its own importance existing in AI and ML to enhance decision-making, optimize consensus mechanisms, detect fraud, and forecast market trends. This chapter provides the AI and blockchain, highlighting innovations in algorithmic trading, predictive analytics, and security management. This chapter also provides the research gaps, AI and ML applications in cryptoeconomics, technical challenges, and future prospects. And overall, this chapter gives the applications and implementation of ethical concerns, and potential research directions for establishing the intelligent and sustainable cryptoeconomic systems.

Keywords: artificial intelligence, machine learning, blockchain, cryptoeconomics, algorithmic trading, smart contracts

1. Introduction

The word “cryptoeconomics” is a new word and not existing, it derived from the convergence of AI, and blockchain technology has created a new paradigm in digital economics known as “cryptoeconomics” [1]. It is an interdisciplinary field focuses on designing economic incentives within decentralized systems. AI and ML and DL improved the efficiency and intelligence of blockchain-based enhancements, enabling AI and ML applications in cryptoeconomics, automated governance, and adaptive security mechanisms. This integration of **Figure 1** provides the potential to transform traditional financial approach to integration of AI and ML in cryptoeconomics capable of learning from market dynamics [2].

Figure 1 illustrates as cryptoeconomics studies how economic incentives, cryptographic primitives, and distributed consensus interact to produce the desirable behavior in decentralized systems [3].

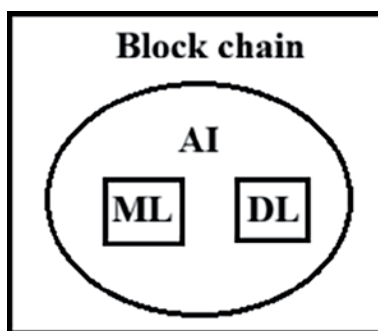


Figure 1.
Integration of AI and ML in cryptoeconomics.

1.1 Motivation

In market and risk prediction, to develop cryptoeconomics, ML models (time-series, reinforcement learning) can improve price forecasting, liquidity management, and automated market maker (AMM) parameter tuning to reduce slippage and impermanent loss with integration of AI and ML in cryptoeconomics [4]. In smarter oracles and context-aware triggers to cryptoeconomics, AI-augmented oracles can filter, aggregate, and sanity-check noisy external data before it reaches smart contracts, improving reliability and reducing costly oracle errors with integration of AI and ML in cryptoeconomics. Robust tokenomics and governance to develop cryptoeconomics, data-driven reputation systems, and ML-informed incentive curves can make DAOs and token economies more resilient to manipulation (Sybil attacks, vote buying) and better aligned with long-term goals with integration of AI and ML in cryptoeconomics [5]. To implement automated fraud detection and security to develop cryptoeconomics and Zero Knowledge Machine Frameworks (ZKML). ML helps detect abnormal transaction patterns, flash-loan attacks, and rug pulls faster than manual monitoring with integration of AI and ML in cryptoeconomics [6].

1.2 Challenges

It cryptoeconomics era on data privacy vs. transparency, Blockchains are transparent by design, but ML often needs private or sensitive features. Reconciling immutable transparency with integration of AI and ML in cryptoeconomics privacy requirements and regulation is nontrivial. Techniques like federated learning, differential privacy, and cryptographic protocols are promising but add complexity integration of AI and ML in cryptoeconomics [7]. In scalability and computation costs from On-chain computation is expensive and limited, it off-chain ML needs reliable validation and trust assumptions (oracle problem). In Explainability and accountability environment, financial decisions driven by opaque ML models create regulatory and governance issues which is accountable for a model's decision that harms users integration of AI and ML in cryptoeconomics [8]. In adversarial and strategic manipulation, ML systems can be gamed (poisoning, adversarial examples), it attackers may manipulate on-chain signals to bias models or exploit learned strategies integration of AI and ML in cryptoeconomics. Sybil attacks and identity fraud remain persistent threats. If smart contracts rely on opaque off-chain models, verifying

model correctness and data provenance becomes a challenge for users and auditors’ integration of AI and ML in cryptoeconomics [9].

1.3 Existing approaches vs. proposed approaches

There huge research work on this domain, cryptoeconomics creates an intelligent layer that can, the following **Table 1** shows the differences on existing vs. proposed approaches (i) analyze large on-chain and off-chain datasets to inform protocol design integration of AI and ML in cryptoeconomics, (ii) automate and adapt token-based incentive mechanisms integration of AI and ML in cryptoeconomics, and (iii) make smart contracts and oracles context-aware integration of AI and ML in cryptoeconomics. This combination turns static economic rules into adaptive, data-driven systems capable of responding to market dynamics, and fraud detection in real-time environment [10].

1.4 Objectives

The main objective to enhance, improved, decision-making and predictive accuracy in cryptoeconomic systems through AI and ML models capable of analyzing large-scale blockchain and market data for better forecasting, pricing, and investment strategies intelligent and sustainable cryptoeconomic systems. Integration of AI and

Existing approaches (state of the art)	Proposed approaches and research directions (Practical + Novel)
AI-augmented oracles with ML-based systems that validate, de-noise, and synthesize multi-source data before feeding smart contracts. They integrate ZKPs and MPC to maintain data confidentiality while proving correctness.	Hybrid privacy-preserving ML for cryptoeconomics—Combines federated learning, differential privacy, and MPC for secure collaborative model training. Model proofs or summaries are recorded on-chain to ensure transparency and auditability integration of AI and ML in cryptoeconomics.
On-chain and off-chain hybrid ML pipelines architecture that executes heavy ML training and inference off-chain while posting model outputs or proofs on-chain, balancing scalability and trust.	Verifiable AI oracles with ZKP-backed assertions—Oracles generate not only data outputs but also cryptographic proofs (ZKPs) verifying the model and dataset integrity used in off-chain inferences.
Reputation and Sybil-tolerant mechanisms are utilizing graph-based reputation, decay functions, and MERITRANK algorithms to counter Sybil attacks and manipulation in tokenized ecosystems.	Adaptive tokenomics via reinforcement learning (RL) with safety constraints are RL agents dynamically tune token parameters (inflation, staking rewards) under safety limits to ensure economic stability and adaptability.
Automated trading and risk analytics—Employs ML models for crypto market forecasting, algorithmic trading, and portfolio optimization to minimize volatility and trading risks.	Sybil-resistant reputation + Economic disincentives—Integrates ML-based behavioral clustering with cryptoeconomic penalties (bonding, slashing) and MERITRANK-style ranking for continuous anomaly detection and deterrence.
Tokenomics simulation and reinforcement learning (RL)—Uses RL and agent-based simulations to study market dynamics and optimize incentive structures before deployment.	Explainable ML (XAI) for financial decisions—promotes interpretable ML models for high-stakes blockchain applications like credit scoring or liquidation, ensuring transparency through on-chain metadata and governance oversight.
<i>Standardized Evaluation Benchmarks and Datasets are the development of open, privacy-preserving benchmark datasets and standardized metrics to improve reproducibility and comparison of AI-crypto models.</i>	

Table 1.
Existing vs. proposed approaches.

ML in cryptoeconomics develops intelligent and adaptive tokenomics frameworks that automatically adjust incentive mechanisms, staking rewards, and governance policies using reinforcement learning and agent-based simulation, the objectives are as follows [11]:

- To strengthen blockchain security and fraud detection by employing machine learning algorithms to identify anomalous transactions, intelligent and sustainable cryptoeconomic systems provide the Sybil attacks, and malicious network behaviors in real time [12].
- To improve oracle reliability and data integrity using AI-driven validation with intelligent and sustainable cryptoeconomic systems and Zero-Knowledge Proofs (ZKPs) for secure and verifiable off-chain data integration into smart contracts [13].
- To ensure privacy-preserving and transparent computation through hybrid federated learning and secure multi-party computation (MPC), with intelligent and sustainable cryptoeconomic systems to enabling decentralized model training without compromising user data confidentiality [14].
- To promote explainability and accountability in AI-driven financial decisions within cryptoeconomic systems by integrating explainable AI (XAI) techniques with intelligent and sustainable cryptoeconomic systems for model interpretability and regulatory compliance [15].
- To create standardized frameworks with intelligent and sustainable cryptoeconomic systems and benchmark datasets for evaluating AI- and ML-based cryptoeconomic models, ensuring reproducibility, interoperability, and fair comparison across research and industry applications [16].
- To establish trust and verifiability in AI-assisted cryptoeconomic operations by integrating cryptographic proofs and transparent governance mechanisms with intelligent and sustainable cryptoeconomic systems to validate the model outputs and decisions [17].
- To advance sustainable and scalable AI integration by optimizing computational resources with intelligent and sustainable cryptoeconomic systems and leveraging on-chain/off-chain hybrid architectures for efficiency and performance balance [18].
- To foster innovation and collaboration among researchers, developers, and policymakers toward building secure, adaptive, and intelligent decentralized economic systems with intelligent and sustainable cryptoeconomic systems for the future of digital finance [18].

1.5 Structure of the chapter

This chapter Section 2 describes the research gaps and Blockchain-based Federated Learning (BCFL) /Privacy-Preserving ML and Section 3 describes the AI and ML applications in cryptoeconomics and Section 4 describes the technical and changes and future prospects followed by Section 5 defining the conclusion.

2. Research gaps

From the surveyed literature, the following gaps are described. These are potential opportunities to evaluate the future work; Recent studies have emphasized the transformative impact of AI in blockchain ecosystems.

Nakamoto [1] introduced the concept of blockchain, forming the foundation of intelligent and sustainable cryptoeconomic systems decentralized trust. Explored AI-driven blockchain optimization for predictive modeling and fraud detection [1]. Discussed hybrid AI-blockchain systems for decentralized financial governance with intelligent and sustainable cryptoeconomic systems [2]. Proposed RL algorithm for optimizing crypto trading and resource allocation with intelligent and sustainable but not completely give the solution of cryptoeconomic systems. AI augments cryptoeconomic stability provides the improving scalability, “A Survey of ZKPs based verifiable ML,” covers work from mid-2017 to late 2024 [3]. It categorizes efforts into verifiable training, verifiable inference, and verifiable testing, analyzing trade-offs among efficiency, privacy, and applicability with intelligent and sustainable cryptoeconomic systems [4]. The survey notes that although many schemes exist for small- to medium-sized models, scaling to DNN transformer architectures remains expensive both in proving time and memory. ZKML systems with intelligent and sustainable cryptoeconomic systems allow proving correctness of inference, that the model produced the output claimed without showing weights or full data [5]. The training is harder proving that the training with the development of intelligent AI and ML productions and sustainable cryptoeconomic systems was done correctly with correct gradients, no cheating, it is often infeasible or requires restrictive settings. Huge number of commercial applications are beginning to appear, but with narrow model classes or simpler architectures with integration of AI and ML in cryptoeconomics [6]. ZKML with integration of AI and ML in cryptoeconomics is promising for cryptoeconomic systems where trust and auditability are essential. The following **Table 2** provides the overall research gaps with the integration of AI and ML in cryptoeconomics [7–10].

2.1 Blockchain-based federated learning (BCFL) and ML

There is a sizable literature exploring how Federated Learning (FL) with integration of AI and ML in cryptoeconomics can be combined with blockchain to enhance

Research gap	Description	Why it matters	How to overcome the gap
Scalability of zkML for large models	Current ZKML frameworks integration of AI and ML in cryptoeconomics work efficiently only for small- or medium-sized models; proving large neural network computations is computationally expensive.	Large cryptoeconomic systems like DeFi or blockchain governance require high-complexity models for fraud detection, oracle reliability, and risk prediction.	Develop optimized proof systems e.g., zk-SNARK optimizations, recursive proofs and hardware acceleration of GPU/FPGA-based to reduce proof generation time and cost.
Lack of standardized datasets and benchmarks	Research uses proprietary or small datasets, making it hard to compare or reproduce results.	Absence of common benchmarks slows scientific progress and prevents fair evaluation of AI-blockchain integration methods.	Create open-access, blockchain-based datasets (e.g., DeFi transaction logs, governance data) with standardized metrics for AI/ML evaluation.

Research gap	Description	Why it matters	How to overcome the gap
Limited real-world implementation and evaluation	Most studies are simulation-based or theoretical, lacking large-scale deployment under adversarial conditions.	Real-world systems exhibit unpredictable behaviors such as collusion, manipulation, or flash-loan attacks that simulations miss.	Develop pilot projects and real-world testnets with multi-agent simulations, robust auditing, and adversarial testing environments.
Trade-off between privacy and verifiability	Ensuring both model privacy (keeping data and parameters confidential) and verifiability (ensuring correctness) is difficult.	Financial applications require confidentiality (for compliance) and transparency (for trust).	Combine federated learning, differential privacy, and zk-proofs; introduce hybrid architectures that balance off-chain privacy with on-chain proofs.
Incentive misalignment among stakeholders	Data providers, miners, and verifiers often have conflicting goals; existing reward mechanisms may be gamed or lead to collusion.	Poor incentive alignment causes dishonest participation, data poisoning, or economic instability in decentralized AI systems.	Use game-theoretic models and reinforcement learning to dynamically adjust rewards and punishments for optimal cooperation.
High latency and computational cost in on-chain ML	On-chain execution of ML tasks introduces delays and high gas costs.	Real-time cryptoeconomic applications of price oracles and fraud alerts need low latency and low-cost computation.	Employ off-chain AI computation with cryptographic proof submission, for example, rollups, zkOracles, and Layer-2 blockchain scalability solutions.
Lack of explainability and transparency in AI decisions	Many AI models are black boxes, making it hard to justify predictions or actions in decentralized finance systems.	Regulatory compliance and user trust require transparency, especially for credit scoring or liquidation decisions.	Integrate Explainable AI (XAI) frameworks and on-chain logging mechanisms for auditability and accountability.
Weak robustness to adversarial and byzantine attacks	Existing models are not rigorously tested against data poisoning, Sybil attacks, or adversarial manipulation.	In decentralized settings, malicious actors can exploit vulnerabilities for financial gain.	Implement Byzantine Fault-Tolerant consensus, anomaly detection systems, and adversarial training techniques to enhance model resilience.
Lack of interoperability between AI-blockchain platforms	AI frameworks and blockchain networks often operate in silos with incompatible protocols.	Without interoperability, models cannot exchange knowledge or operate across multiple ecosystems.	Develop standardized APIs, cross-chain smart contracts, and decentralized AI middleware layers.
Limited regulatory and ethical frameworks	Integration of AI in finance and blockchain raises legal and ethical concerns of data protection, bias, accountability.	Regulatory non-compliance can result in misuse of user data or legal penalties.	Establish global governance standards and compliance protocols integrating GDPR, KYC/AML, and ethical AI design principles.

Table 2.
Research gaps and to overcome with description.

decentralization, privacy, and incentive alignment [11]. A survey on blockchain FL with data privacy systematically maps existing architectures, threat types, and security and privacy mechanisms [12]. Securing federated learning a systematic way of similarly reviews approaches that use smart contracts to aggregate model updates, reward honest participants, guard against free-riders, poisoning attacks, or unreliable clients. Blockchain FL for Industrial IoT proposes using Intel SGX. FLCoin provides the scalable blockchain-enabled FL architecture with resource constraints. These works show that combining FL and blockchain with integration of AI and ML in cryptoeconomics is viable, especially for settings where many small participants contribute to data and computation [13].

3. AI and ML applications in cryptoeconomics

AI and ML are providing the tremendous change in cryptoeconomics by enabling intelligent, data-driven decision-making across decentralized financial systems. By weaving AI and ML into the fabric of cryptoeconomics, we are seeing improvements in market predictions, risk analysis, and algorithmic trading. AI-driven blockchain improves the reliability of on-chain data feeds by filtering and verifying multi-source information before integration into smart contracts. RL algorithms and agent-based simulations are becoming more popular for fine-tuning tokenomics and governance structures, allowing for dynamic adjustments to incentives, staking rewards, and inflation rates to keep the economy stable. Federated learning and privacy-focused ML techniques enable collaborative model training without putting sensitive blockchain or user data at risk, striking a balance between transparency and confidentiality in the integration of AI and ML in cryptoeconomics (**Table 3**). XAI enhances accountability in automated financial decisions, with ZKPs and cryptographic verification ensure trustworthy AI outputs in decentralized ecosystems. These advancements create a bridge between intelligence and trust in blockchain networks, setting the stage for adaptive, secure, and transparent cryptoeconomic systems [14].

3.1 Market forecasting

The world of cryptocurrency is buzzing with the integration of AI and machine learning algorithms, like RL, which are being used to predict price swings. The historical data of social sentiment, and on-chain metrics, AI and ML models offer accurate short-term trading signals and long-term investment forecasts. In the realm of cryptoeconomics, predictive analytics and market forecasting harness AI and ML techniques to sift through historical blockchain and market data, helping to spot trends, price shifts, and volatility in the crypto markets. Time-series models, DL architectures, and graph-based approaches are employed to detect patterns in trading volumes, transaction flows, and network activity, enabling accurate short-term and long-term predictions. These valuable insights aid in algorithmic trading, portfolio optimization, and risk management, empowering investors and decentralized platforms to make well-informed choices. Plus, predictive models are increasingly being woven into smart contracts and automated systems, enabling timely actions like liquidations, dynamic staking adjustments, or rebalancing token incentives, which boosts efficiency and resilience in the fast-paced market landscape [15].

Application area.	Description/role of AI & ML	Example techniques/models
Predictive analytics and market forecasting	Analyzes historical blockchain and market data to predict price trends, volatility, and trading opportunities. Supports informed decision-making and risk management.	Time-series models, LSTM, GRU, Graph Neural Networks (GNN), ARIMA
Algorithmic and automated trading	Executes trading strategies automatically, adapting to market fluctuations in real-time. Reduces latency, human error, and enables high-frequency trading.	Reinforcement Learning (RL), Deep Q-Networks (DQN), Neural Networks, Predictive Modeling
AI-augmented oracles	Enhances reliability and trustworthiness of on-chain data feeds by filtering, validating, and synthesizing multi-source inputs for smart contracts.	ML-based data validation, ZK Proof integration, Ensemble Models
Reinforcement learning for tokenomics and governance	Simulates participants' behavior to optimize staking rewards, inflation schedules, and incentive mechanisms in decentralized ecosystems.	Multi-agent RL, agent-based modeling, policy gradient methods
Fraud detection and anomaly identification	Detects malicious transactions, Sybil attacks, flash loans, and other irregularities to enhance network security and reduce financial risk.	Anomaly detection, autoencoders, graph neural networks, outlier analysis
Privacy-preserving collaborative learning	Enables decentralized training of ML models without exposing sensitive user or blockchain data, maintaining transparency and auditability.	FL, Secure MPC
Explainable AI (XAI) for financial decisions	Provides interpretable insights for automated decisions like credit scoring, liquidation, and governance, ensuring accountability and compliance.	SHAP, LIME, rule-based models, generalized additive models (GAM)
Tokenomics simulation and RL-based economic modeling	Simulates economic dynamics of token ecosystems to test and refine incentive structures before deployment.	Reinforcement learning, agent-based simulations, Monte Carlo methods
Risk management and portfolio optimization	Optimizes portfolio allocation and risk exposure in crypto markets using predictive and adaptive AI models.	Markowitz optimization, neural networks, deep reinforcement learning
Cross-protocol and multi-chain AI integration	Ensures interoperability of AI models and ML-driven insights across multiple blockchain platforms.	Standardized APIs, middleware layers, smart contract interfacing

Table 3.
AI and ML applications in cryptoeconomics.

3.2 Automated trading

The world of cryptoeconomics is buzzing with the integration of AI and machine learning in trading bots, which use deep reinforcement learning to autonomously navigate the unpredictable waters of crypto markets. These smart algorithms are designed to fine-tune execution timing, cut down on slippage, and keep emotional biases at bay, all of which can lead to better profitability and smoother liquidity management. AI and ML algorithmic and automated trading in cryptoeconomics utilizes AI and ML models to execute trading strategies with minimal human intervention, optimizing for speed, accuracy, and profitability in highly volatile cryptocurrency markets. ML techniques, including reinforcement learning, neural networks, and predictive modeling, are applied to identify trading signals, forecast price trends, and adapt strategies in real time [16].

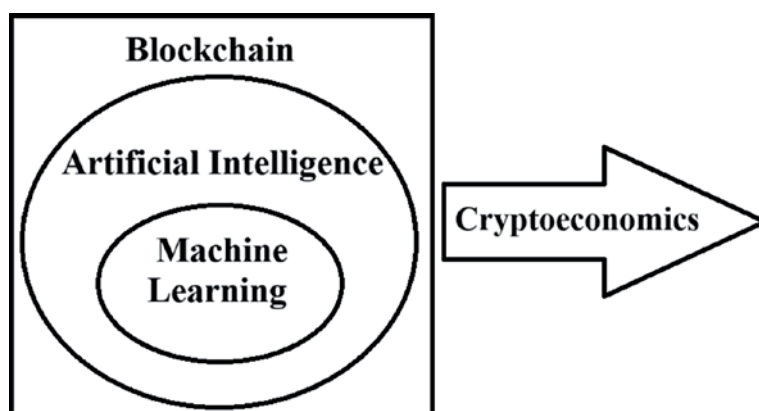


Figure 2.
The generation of cryptoeconomics from AI and ML with blockchain.

3.3 Fraud detection and security enhancement

Blockchain's ability to remain unchanged is enhanced by AI-driven anomaly detection systems that spot fraudulent patterns in transactions. AI and ML models trained on historical data detect phishing attacks, double-spending attempts [17].

3.4 Smart contract optimization

To generate the cryptoeconomics which is from NLP techniques assist in analyzing smart contract code for vulnerabilities as shown in **Figure 2**, enabling automatic verification and semantic error detection. This reduces the risks associated with logic flaws and contract exploitation with AI and ML. AI facilitates intelligent decision-making in Decentralized Autonomous Organizations (DAOs) using AI and ML-based reputation scoring and voting optimization [18].

4. Technical challenges

- **Data availability and quality:** The blockchain data is fragmented and non-structured, making it difficult to train reliable AI models.
- **Computational complexity:** The AI algorithms require significant processing power, which conflicts with blockchain's resource constraints.
- **Transparency vs. privacy:** The balancing AI model interpretability with blockchain's anonymity remains unresolved.
- **Security and trust:** The malicious AI and ML models could manipulate consensus or alter on-chain incentives.
- **Interoperability issues:** The integrating heterogeneous blockchain networks and AI frameworks presents standardization challenges.

5. Future prospects

The next generation of cryptoeconomic systems will incorporate autonomous AI and ML capable of self-learning and governance within decentralized markets and health care applications. Emerging paradigms such as FL, and quantum computing, and integration of AI and ML in cryptoeconomics protocols are expected to enhance scalability and trust. Integration with Web3 and Metaverse economies will further expand AI's influence, enabling intelligent asset management as shown in **Tables 2 and 4**.

Implementation methods for future	Description	Tools used for future prospects
AI and ML augmented oracles	Integrates AI and ML models to validate, de-noise, and aggregate off-chain data before delivering it on-chain. Ensures reliability and correctness of smart contract inputs.	Ensemble models, neural networks, ZK-proofs, MPC
On-chain and off-chain hybrid pipelines	Heavy ML computations are performed off-chain, that only results or proofs are posted on-chain to balance scalability, trust, and cost.	Federated learning, off-chain model training, proof aggregation
Federated learning and privacy-preserving ML	Supports auditability and privacy.	FL and MPC
Reinforcement learning and agent-based simulation	Models participant behavior and dynamically optimizes tokenomics, staking rewards, and incentive mechanisms.	Multi-agent RL, policy gradient, Q-learning, Monte Carlo simulation
Graph-based reputation and Sybil-tolerant mechanisms	Computes trust and reputation scores to mitigate Sybil attacks and malicious behavior in decentralized communities.	MeritRank, graph neural networks (GNN), decay functions
Automated trading and risk analytics	Uses AI/ML models to automate trading strategies, optimize portfolios, and forecast volatility.	LSTM, GRU, deep Q-networks (DQN), autoencoders
Explainable AI (XAI) and auditable models	Provides interpretable predictions for high-stakes decisions, linking AI outputs to on-chain metadata and governance processes.	SHAP, LIME, rule-based models, GAM
Simulation and scenario testing	Tests economic and market scenarios to evaluate the impact of RL policies or incentive designs before deployment.	Agent-based models, reinforcement learning, Monte Carlo simulation
Standardized evaluation and benchmarking	Ensures reproducible comparisons of models and systems using shared datasets and metrics for tokenomics and fraud detection.	Synthetic blockchain datasets, metrics frameworks, benchmarking tools
Cross-chain/multi-protocol integration	Ensures AI and ML models and predictions work across multiple blockchains and protocols for interoperability and composability.	Standard APIs, Smart Contract Middleware, Oracles

Table 4.
Implementation methods of AI and ML in cryptoeconomics.

6. Conclusion

The integration of AI and ML in cryptoeconomics represents a major step toward creating intelligent, autonomous, and secure decentralized systems, and this chapter also provides the research gaps, AI and ML applications in cryptoeconomics,

technical challenges, and future prospects. As we dive deeper into the integration of AI and machine learning in the world of cryptoeconomics, it is becoming increasingly clear that teamwork among data scientists, economists, and blockchain developers is essential. Together, they will tackle the ethical, computational, and regulatory hurdles are faced. The evolution of AI and ML blockchain solutions will redefine the future of digital finance, cryptocurrency, ensuring efficiency, transparency, and adaptive economic ecosystems.

Author details

Basetty Mallikarjuna^{1*}, Pusalatha Chittem Setty² and Sam Goundar³

1 Department of Information Technology, Institute of Aeronautical Engineering, Hyderabad, India

2 Department of MBA, Institute of Aeronautical Engineering, Hyderabad, India

3 School of Arts and Sciences, University of Central Asia, Kyrgyzstan

*Address all correspondence to: basettymalli@gmail.com

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Vol. 4. No. 2. Bitcoin; 2008. p. 15. Available from: <https://bitcoin.org/bitcoin.pdf>
- [2] Zuo Y. Exploring the synergy: AI enhancing blockchain, blockchain empowering AI, and their convergence across IoT applications and beyond. *IEEE Internet of Things Journal*. 2024. DOI: 10.1109/JIOT.2024.3507746
- [3] Singh M, Srivastava K, Vittala KP, Tyagi AK. Modern banking with blockchain technology: The impact of distributed ledger technology on revolutionizing global financial systems. In: *Establishing AI-Specific Cloud Computing Infrastructure*. IGI Global Scientific Publishing; 2025. pp. 331-358. DOI: 10.4018/979-8-3693-9694-0.ch016
- [4] Fatima S, Arshad MJ. A comprehensive review of blockchain and machine learning integration for peer-to-peer energy trading in smart grids. *IEEE Access*. 2025. DOI: 10.1109/ACCESS.2025.3572174
- [5] Vyas AK, Khatri N, Jha SK, editors. *6G Communication Network: Architecture, Security and Applications*. CRC Press; 2024. Available from: https://www.google.co.in/books/edition/6G_Communication_Network/izEmEQAAQBAJ?hl=en&gbpv=1&dq=Khatri+N,+Jha+SK,+editors.+6G+Communication+network:+architecture,+security+and+applications.+CRC+Press%3B+2024+&pg=PP1&printsec=frontcover
- [6] Chhetri B, Gopali S, Olapojoye R, Dehbashi S, Namin AS. A survey on blockchain-based federated learning and data privacy. In: *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE; 2023. pp. 1311-1318. DOI: 10.1109/COMPSAC57700.2023.00199
- [7] Mallikarjuna B, Reddy TC. A policy and secure based protocol in information systems using blockchain. *International Journal of Blockchains and Cryptocurrencies*. 2024;5(4):274-293. DOI: 10.1504/IJBC.2024.143984
- [8] Moudoud H, Cherkaoui S, Khoukhi L. Towards a secure and reliable federated learning using blockchain. In: *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE; 2021. pp. 01-06. DOI: 10.1109/GLOBECOM46510.2021.9685388
- [9] Mallikarjuna B, Pushpalatha C. Intricate dynamics between cryptography, blockchain technology, and the internet of things (IoT). *International Journal of Blockchains and Cryptocurrencies*. 2024;5(4):314-330. DOI: 10.1504/IJBC.2024.143983
- [10] Sameera KM, Nicolazzo S, Arazzi M, Nocera A, Rafidha Rehiman KA, Vinod P, et al. Privacy-preserving in blockchain-based federated learning systems. *Computer Communications*. 2024;222:38-67. DOI: 10.1016/j.comcom.2024.04.024
- [11] Mallikarjuna B, Kiranmayee D, Saritha V, Krishna PV. Development of efficient e-health records using IoT and blockchain technology. In: *ICC 2021-IEEE International Conference on Communications*. IEEE; 2021. pp. 1-7. DOI: 10.1109/ICC42927.2021.9500390
- [12] Wu B, Seneviratne O. Blockchain-based framework for scalable and incentivized federated learning. In: *Companion Proceedings of the ACM on*

Web Conference 2025. 2025. pp. 1761-1767. DOI: 10.1145/3701716.371764

[13] Mallikarjuna B, Sathish K, Gitanjali J, Krishna PV. An efficient vote casting system with Aadhar verification through blockchain. *International Journal of System of Systems Engineering*. 2021;**11**(3-4):237-256. DOI: 10.1504/IJSSE.2021.121439

[14] Xing Z, Zhang Z, Zhang Z, Li Z, Li M, Liu J, et al. Zero-knowledge proof-based verifiable decentralized machine learning in communication network: A comprehensive survey. *IEEE Communications Surveys & Tutorials*. 2025. DOI: 10.1109/COMST.2025.3561657

[15] Mallikarjuna B. An improved hybrid (HHO-FFO) algorithm for healthcare and secure data transmission. *International Journal of Services Technology and Management*. 2024;**29**(2-4):274-295. DOI: 10.1504/IJSTM.2024.145234

[16] Nasrulin B, Ishmaev G, Pouwelse J. Meritrunk: Sybil tolerant reputation for merit-based tokenomics. In: 2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE; 2022. pp. 95-102. DOI: 10.1109/BRAINS55737.2022.9908685

[17] Kalapaaking AP, Khalil I, Rahman MS, Atiquzzaman M, Yi X, Almashor M. Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things. *IEEE Transactions on Industrial Informatics*. 2022;**19**(2):1703-1714. DOI: 10.1109/TII.2022.3170348

[18] Mallikarjuna B, Shrivastava G, Sharma M. Blockchain technology: A DNN token-based approach in healthcare and COVID-19 to generate extracted data. *Expert Systems*. 2022;**39**(3):e12778. DOI: 10.1111/exsy.12778

Determinants of Fintech Adoption: A Systematic Review Integrating Trust, Security, and User Perceptions within Technology Acceptance Frameworks

*Nikolaos Papanikolaou, Paraskevi Boufounou
and Nikolaos Eriotis*

Abstract

The rapid evolution of financial technology (fintech), including cryptocurrencies and decentralized finance (DeFi), has transformed how consumers and businesses engage with financial services. This chapter examines the drivers of fintech adoption by extending established technology acceptance models, such as technology acceptance models (TAM), unified theory of acceptance and use of technology (UTAUT), and theory of planned behavior (TPB). A systematic review of 80 articles (2017–2023) identifies key factors influencing adoption, including perceived usefulness, ease of use, social influence, and facilitating conditions. Emerging factors, such as financial literacy, hedonic motivation, and trust, are especially important during crises, such as the COVID-19 pandemic. However, gaps remain in understanding how evolving perceptions of security and trust impact sustained adoption, particularly in decentralized environments, such as blockchain networks and crypto assets, where algorithmic transparency replaces institutional intermediaries. This chapter proposes integrating trust, security, and user perceptions into existing models to create a cohesive framework applicable across fintech services. The findings provide actionable insights for researchers and industry stakeholders to enhance user acceptance and guide future innovation.

Keywords: fintech adoption, technology acceptance models (TAM), trust, security, user perceptions, behavioral intention

1. Introduction

The COVID-19 pandemic accelerated global fintech adoption, driving both consumers and institutions toward digital banking and contactless payments [1–3]. Despite this growth, adoption remains uneven across demographics and regions,

influenced by disparities in technological infrastructure, regulatory environments, and user perceptions [4, 5]. Recent studies highlight that understanding fintech adoption requires integrating traditional technology acceptance models with emerging factors, such as financial literacy, government support, and crisis-driven behavioral shifts [6, 7]. However, the growing body of research remains fragmented, with inconsistent frameworks complicating cross-contextual comparisons [8]. Fintech adoption has been shown to positively impact financial development by enhancing access to financial services, particularly in emerging markets, where it supports financial-sector growth [9]. Yet, a cohesive framework explicitly comparing these theories across contexts is lacking. This chapter addresses this gap by systematically reviewing fintech adoption literature, focusing on trust, security, and user perceptions within technology acceptance models.

The research is guided by the following questions:

1. What are the primary determinants influencing fintech adoption, and how do trust, security, and user perceptions interact within technology acceptance models to shape adoption behaviors?
2. How effectively do traditional technology acceptance models (TAM, UTAUT) capture the influence of trust, security, and user perceptions on fintech adoption behaviors?
3. Which emerging factors significantly influence fintech adoption, and how can they be integrated with trust, security, and user perceptions to enhance technology acceptance models?

2. Methodology

2.1 Database selection

The selection of databases for this study was guided by well-established academic practices to ensure comprehensive coverage of relevant literature. Scopus was chosen for its high-quality indexing of peer-reviewed journals and its integration with other scholarly databases, while Google Scholar was included for its ability to capture a broader spectrum of publications, including gray literature.

2.2 Search strategy

The search strategy was developed based on established practices for systematic reviews and refined through iterative testing [10]. In Scopus, the search was conducted using the TITLE-ABS-KEY field, which searches within article titles, abstracts, and keywords. This approach ensures a focus on the most relevant publications. In Google Scholar, the keyword-search functionality was utilized to capture a broader range of literature, including gray literature. Search terms included those related to fintech adoption, technology acceptance models, and behavioral intention. Publications focusing solely on specific fintech applications (e.g., cryptocurrencies, blockchain-based systems) were excluded to ensure findings are generalizable across fintech services. The specific search strings employed in each database are detailed in **Table 1**.

Database	Search terms
SCOPUS	TITLE-ABS-KEY (fintech AND adoption) AND PUBYEAR >2016 AND PUBYEAR <2024 AND (LIMIT-TO (SUBJAREA, "BUSI") OR LIMIT-TO (SUBJAREA, "COMP")) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp")) AND (LIMIT-TO (LANGUAGE, "English")) AND (LIMIT-TO (SRCTYPE, "j") OR LIMIT-TO (SRCTYPE, "p"))
Google scholar	Fintech AND adoption, "acceptance of technology", «behavioral intention»

Source: Authors.

Table 1.
Databases and search scope.

2.3 Inclusion and exclusion criteria

The following inclusion and exclusion criteria were applied to select relevant studies for this review:

- Year restrictions: 2017–2023
- Language requirement: English
- Publication source: Journals and conference proceedings
- Research area Computer Science, and Business and Management
- Excluded: Studies focused exclusively on specific fintech applications

2.4 The PRISMA framework

The PRISMA 2020 Flow Diagram [11] serves as a standardized visual tool in systematic reviews and meta-analyses for illustrating study-selection processes. The database search yielded 324 articles from Scopus and 544 from Google Scholar. Following the removal of 80 duplicate records, 788 records were screened based on their titles and abstracts. This screening process resulted in the exclusion of 632 records due to irrelevance to the research question and the scope of the study. The remaining 156 reports were sought, retrieved, and assessed for eligibility. Of these, 40 were excluded due to overlapping content with other studies, and 36 did not meet the predefined inclusion criteria. This process resulted in a final set of 80 studies that were included in the systematic review.

3. Theoretical background

Fintech adoption research relies on established technology acceptance frameworks, though their application requires adaptation to address the sector’s unique challenges. Below is a synthesis of key theories and their relevance to fintech adoption.

3.1 Foundational theories

3.1.1 Theory of reasoned action (TRA)

Proposed by Ajzen and Fishbein [12] TRA indicates that behavioral intentions are shaped by personal attitudes and the perceived social norms (subjective norms). As the foundation for later models, TRA provides a crucial historical context for understanding the evolution of technology acceptance theories. It sets the stage for understanding the subsequent models [12].

3.1.2 Theory of planned behavior (TPB)

Developed by Ajzen [13], the TPB framework illustrates the essential nature of attitudes, social norms, and perceived control in determining one's intentions. TPB has been used to explore how users' attitudes toward fintech and their perceptions of social norms influence their adoption decisions [13]. It is particularly useful in understanding the social context of fintech adoption.

3.2 Core technology acceptance models

3.2.1 Technology acceptance model (TAM)

TAM, developed by Davis [14] suggests that the perception of a technology's perceived usefulness (PU) and its perceived ease of use (PEOU) are essential in influencing its adoption. Within the fintech sector, PU denotes the user's conviction that fintech utilization will enhance their financial outcomes, whereas PEOU refers to the user's belief that engaging with fintech will require minimal effort. These two factors are central to understanding technology adoption from a user perspective.

3.2.2 Extended technology acceptance model (TAM2)

Developed by Venkatesh and Davis [15] TAM2 extends TAM [14] by incorporating additional constructs, such as subjective norms, image, job relevance, output quality, and result demonstrability. TAM2 has been used to better capture social influences and cognitive instrumental processes in technology adoption [15]. This extension allows for a more nuanced understanding of the factors influencing technology adoption.

3.2.3 Unified theory of acceptance and use of technology (UTAUT)

UTAUT, developed by Venkatesh et al. [16] extends TAM [14] by integrating additional factors, including performance expectancy, effort expectancy, social influence, and facilitating conditions. UTAUT has been widely applied in fintech studies, particularly in emerging markets, where social influence and facilitating conditions play a significant role in adoption [16]. Its application in emerging markets is particularly relevant due to the strong influence of social and environmental factors.

3.2.4 Extended unified theory of acceptance and use of technology (UTAUT2)

With UTAUT2, Venkatesh et al. [17] extend the original UTAUT [16] by adding hedonic motivation, price value, and habit as additional determinants to better

explain consumer behavior in voluntary contexts. UTAUT2 [17] is particularly relevant for fintech adoption studies examining consumer-oriented financial technologies. This framework is particularly valuable for understanding voluntary technology adoption in consumer contexts.

4. Key constructs in fintech adoption theories

To better understand the determinants of fintech adoption, we categorize the key constructs into two groups: Traditional TAM [14] and UTAUT [16] constructs (including perceived usefulness, ease of use, performance expectancy, effort expectancy, social influence, and facilitating conditions), and emerging factors (such as trust, security, and government support, personal innovativeness, financial literacy, and hedonic motivation). This categorization facilitates a more structured analysis of the factors influencing fintech adoption.

4.1 Traditional constructs

The literature identifies several key determinants of fintech adoption, which can be grouped into traditional and emerging determinants.

- *Perceived usefulness (PU)*: Users are more likely to adopt fintech if they believe it will improve their financial performance [14]. Empirical evidence supports this, with studies highlighting its consistent positive impact on adoption. This belief is a fundamental driver of technology adoption [6, 18].
- *Perceived ease of use (PEOU)*: Users demonstrate a tendency to accept financial technology when they find it to be user-friendly [14]. Studies demonstrate that ease of use predominantly shows a positive influence on adoption [19, 20].
- *Performance expectancy*: Indicates the level of belief that employing a system will lead to better job outcomes [16]. Studies underscore its strong correlation with adoption. The perception that a technology will improve job performance is a strong predictor of adoption [21, 22].
- *Effort expectancy*: The level of convenience and usability that people feel when using a specific information system [16]. While generally enhancing adoption, studies note context-dependent variations [23, 24]. The perception of convenience and usability is a key factor influencing adoption, but can vary depending on the context.
- *Social influence*: The influence of peers and social networks affects fintech adoption [16]. Many Studies emphasize peer and societal impact [22, 25].
- *Facilitating conditions*: The degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system [16]. Studies in literature demonstrate their pivotal role [7, 26]. A supportive infrastructure is crucial for successful technology adoption.

Table 2 provides a summary key determinants of fintech adoption and their impact.

Determinant	Impact	Key supporting studies
Perceived usefulness	Strong (+)	[6, 18, 27]
Perceived ease of use	Moderate (+)	[18, 20, 21]
Social influence	Contextual (+/–)	[23, 25, 28]
Performance expectancy	Strong (+)	[22, 25, 29]
Effort expectancy	Moderate (+)	[23–25]
Facilitating conditions	Strong (+)	[23, 26, 29]

Source: Authors.

Table 2.

Key determinants of fintech adoption and their impact.

4.2 Emerging determinants

- *Trust*: Trust refers to loyalty to the services or reputation of a firm [30]. Studies highlight its positive influence on adoption behavior. Trust in the service provider is crucial for adoption [18, 31].
- *Perceived benefit*: An individual's belief that specific positive outcomes will result from a specific behavior [32]. Economic benefits and convenience are significant drivers, as noted in the literature [33, 34]. Individuals are more likely to adopt fintech when they perceive notable benefits.
- *Perceived risk*: Perceived risk is defined as people's belief about potential negative consequences when trading online [35]. It can have both positive and negative effects, depending on the context, with operational risks being a concern for small and medium-sized enterprises (SMEs) [36, 37]. Perceived risk can have complex effects on technology adoption, depending on the context and the user.
- *Government support*: Government support includes the regulatory and legislative framework established by the government for the development of financial technology [38]. Its impact can be both positive and negative, depending on user perceptions, as indicated by the same authors [38]. Government support can influence technology adoption, but the impact is dependent on user perceptions of the regulatory environment.
- *Personal innovativeness*: Individuals who are more open to experimenting with new technologies are more likely to adopt fintech services [39]. A willingness to experiment with new technologies is a strong predictor of adoption.
- *Security and privacy*: Security and privacy prerequisites were quantitatively emphasized as critical for technology adoption, while their role in building trust was highlighted [40, 41]. Barriers to adoption can arise when these concerns emerge.
- *Hedonic motivation*: Enjoyment and satisfaction derived from technology use (hedonic motivation) influences adoption behaviors according to research [28].

Determinant	Impact	Key supporting studies
Trust	Strong (+)	[18, 23, 31]
Perceived benefit	Moderate (+)	[21, 33, 34]
Perceived risk	Contextual (+/–)	[33, 36, 37]
Government support	Contextual (+/–)	[6, 38, 44]
Personal innovativeness	Strong (+)	[21, 28, 38]
Security and privacy	Strong (+)	[40, 41]
Hedonic motivation	Contextual (+/–)	[22, 28, 29]
Financial literacy	Moderate (+)	[38, 43]

Source: Authors.

Table 3.
Emerging determinants of fintech adoption identified in the literature and their impact.

- *Financial literacy*: Understanding personal finance information (“financial literacy”) enables better planning and positively impacts fintech adoption through informed decision-making [42, 43].

Table 3 demonstrates the emerging determinants of fintech adoption, as they appear in the literature.

Emerging determinants help address research gaps: Trust and perceived risk directly shape adoption behaviors (Research Question 1). Financial literacy and personal innovativeness enhance traditional acceptance models by explaining user assessments of fintech utility and ease (Research Question 2). Government support, hedonic motivation, and perceived benefits—combined with trust and security—provide a holistic understanding of acceptance (Research Question 3), as government mitigates trust barriers, hedonic motivation drives nonutilitarian adoption, and perceived benefits amplify usefulness. These constructs collectively complement traditional frameworks.

5. Results and discussion

5.1 Research question 1: Synthesizing determinants of adoption

The review synthesizes evidence addressing what drives fintech adoption and how trust/security interact within acceptance frameworks.

5.1.1 TAM-related factors

Perceived Usefulness (PU) remains a cornerstone of the technology acceptance model (TAM) [14], with empirical studies affirming its pivotal role across diverse contexts. Its significance is evident among tech-savvy users prioritizing transactional efficiency in Malaysia and in India, where cost reduction drives adoption [29, 45]. However, exceptions exist where trust surpasses PU in high-risk contexts. Noted exceptions where trust surpasses PU in high-risk contexts, underscoring its contextual dependency [27]. Simplified interfaces were found to enhance PEOU-driven

adoption among rural populations in Palestine, while preliminary studies in Malaysia identified competitive advantage as a key PEOU amplifier [46, 47].

Perceived Ease of Use (PEOU) is critical for non-tech users in Indonesia through simplified interfaces, but less influential in advanced economies like Germany, where advanced features take precedence [44, 48]. This dichotomy highlights PEOU's diminishing relevance in digitally mature markets but reinforces its necessity in bridging adoption gaps among underserved populations. PEOU showed stronger effects among financially literate users in Malaysia, yet proved insignificant in South Korea despite cultural proximity to high-adoption regions [49, 50]. The impact of PEOU is also mediated by trust [27].

5.1.2 UTAUT-related factors

While TAM [14] emphasizes perceived usefulness and ease of use, UTAUT [16] extends this framework with social influence and facilitating conditions, offering broader applicability in emerging markets. Age significantly moderated performance expectancy in Pakistan [51], while system quality showed no effect on adoption in nonfinancial institutions [52].

Performance Expectancy is particularly notable in professional contexts [16]. For instance, streamlining small business operations in Saudi Arabia [24] observed its impact in Saudi Arabia. However, weaker effects occurred in Ghana due to infrastructural gaps, and COVID-19 accelerated finance app downloads globally [48, 53].

Effort Expectancy aligns with PEOU but extends to cognitive load reduction [16]. Effort Expectancy (reflecting ease of use and reduced cognitive load) significantly drives FinTech adoption in Malaysia by minimizing transactional complexity [49]. Conversely, in South Korea, Effort Expectancy becomes less relevant, as speed supersedes simplicity [37]. These disparities underscore their context-dependent relevance, particularly in cash-to-digital transitions.

Social Influence emerges as a robust predictor in collective cultures [16]. It drives rural adoption in Vietnam through community endorsements and tribal networks in Saudi Arabia, and did not affect attitudes in the Gulf Cooperation Council (GCC) countries [54–56].

Facilitating Conditions are critical for bridging adoption barriers [16]. They thrive under Bangladesh's government-backed infrastructure [7], but falter under Ghana's fragmented policies [57]. This determinant's efficacy hinges on regulatory coherence and public-private collaboration, particularly in emerging economies, with financial literacy enhancing conditions in Indonesia [58].

5.1.3 Trust-related factors

Trust, defined as confidence in fintech providers' reliability and integrity, mediates traditional adoption factors [30]. Research in India pointed out that trust is a vital component that influences user decisions, while also considering institutional credibility against perceived risks [59]. Moreover, trust fully mitigates hesitancy in Indonesia [60]. During COVID-19 in Jordan, it mediated perceived risks but was insignificant in Islamic Fintech adoption in Indonesia [61, 62]. These insights position trust as both a catalyst and vulnerability in adoption ecosystems.

Security perceptions, integral to trust, directly influence long-term fintech engagement [35]. Stringent data laws drive adoption in Germany, while security perceptions prioritize encryption in Bangladesh [63, 64]. Technical factors (system

quality, situational normality) and social factors (herding, subjective norm) built trust for continuance in China [65], though security risk was insignificant in Malaysia [36]. Consequently, these findings necessitate adaptive security frameworks calibrated to region-specific risk profiles.

5.1.4 Emerging determinants

Financial literacy exhibits significant contextual variability: In Indonesia, it shows minimal influence on adoption due to intuitive platform designs [38], while in Malaysia, educated users' investment activities correlate strongly with fintech adoption [43]. Meta-analytic reviews confirm its role as a supplementary factor in markets with user-centric platforms, though it significantly shapes attitudes when combined with trust in Bangladesh [66, 67].

Government Support, through policies and infrastructure, accelerates adoption in regulated environments [6], with high innovation and economic development driving country-level adoption [68]. While effective in India's rural penetration, top-down approaches neglect grassroots needs in Ghana [57] and traditional infrastructure moderates household consumption impacts in China [69].

Personal Innovativeness, or openness to new technologies, drives adoption among early adopters despite risks [5], though infrastructural gaps offset effects in Bangladesh [7]. Post-COVID, it boosted loyalty in Malaysia, while perceived risks dominated benefit assessments in similar contexts [70, 71].

Hedonic Motivation retains users in South Korea's gamified platforms [37], but it is irrelevant in utilitarian-driven India [72]. In Indonesia, economic benefits and convenience showed stronger effects than enjoyment, while brand trust, mediated through attitudes, significantly influenced adoption [73, 74]. Consumer-attitude studies in India highlighted low cost and time-saving as paramount drivers [75].

Overall, these findings confirm that emerging adoption determinants—financial literacy, government support, personal innovativeness, and hedonic motivation—vary significantly across contexts instead of operating universally or adhering to fixed hierarchies.

5.1.5 Demographic factors in fintech adoption

Demographic factors, such as age, gender, income, and education, shape fintech adoption variably across contexts. Younger generations prioritize perceived usefulness and trust in India and exhibit higher adaptability to facilitating conditions in Jordan [1, 21]. In Poland, income and gender gaps persist, while in Bangladesh, age significantly moderates effort expectancy and social influence [76, 77]. Studies emphasized the role of trust and social influence in shaping attitudes toward fintech in Nigeria, especially among educated urban populations [18]. In Nigeria, studies emphasize trust and social influence as key drivers of fintech adoption among educated urban populations, aligning with Palestine's findings, where Millennials prioritized trust and Gen-Z emphasized ease of use [18, 46].

Contradictions in findings emerge across regions: In Indonesia, financial literacy showed minimal influence on adoption, challenging assumptions about education as a key driver [38]. Meanwhile, income is irrelevant in Germany—contrasting with developing economies—where age and education significantly moderated perceived usefulness [48]. Gender differences also varied, with no effect observed in Bangladesh [7], whereas males are more inclined to adopt fintech in Malaysia [78]. Trust and

responsiveness mediated adoption intentions in India, while Islamic financial technology adoption followed distinct behavioral patterns [79, 80].

In summary, demographics are context-dependent: Younger, tech-proficient, higher-income users drive adoption in advanced markets, whereas accessibility and usability prevail in developing regions (**Figure 1**).

5.1.6 Trends in fintech adoption across countries

Fintech adoption varies widely across regions, shaped by differences in socio-economic conditions, regulatory environments, and technological infrastructure. In advanced economies like Germany and the Netherlands, high adoption rates are driven by strong digital infrastructure, widespread trust in technology, and perceived benefits [48, 81]. In contrast, emerging markets, such as Indonesia and Nigeria, have made progress through government-led initiatives, including financial literacy programs and the expansion of mobile technology to address challenges like limited access to traditional banking services [18, 38]. Pakistan significantly advanced financial inclusion through government-led policies in the last decade, with fintech innovations serving as a key driver for extending service coverage [82]. Meanwhile, in emerging markets, such as Indonesia, technostress hinders Gen-Z adoption [83], while perceived risk, ease of use, and usefulness significantly boosted adoption attitudes in Jakarta [84]. In Hungary, COVID-19 risk emerged as a predominant determinant of mobile payment adoption [85]. Comparative analysis of China and Korea identified price value as the primary driver in China, contrasting with credibility in Korea, while systematic reviews highlight firm-user communication as critical for adoption alignment [86, 87].

Regional differences highlight the diverse factors influencing fintech adoption. In Sub-Saharan Africa, for instance, practical considerations, such as ease of use and established habits, drive adoption among specific user groups, such as port workers in Ghana [57]. Meanwhile, East Asian countries, like China and South Korea, lead in adoption by seamlessly integrating fintech into e-commerce platforms and

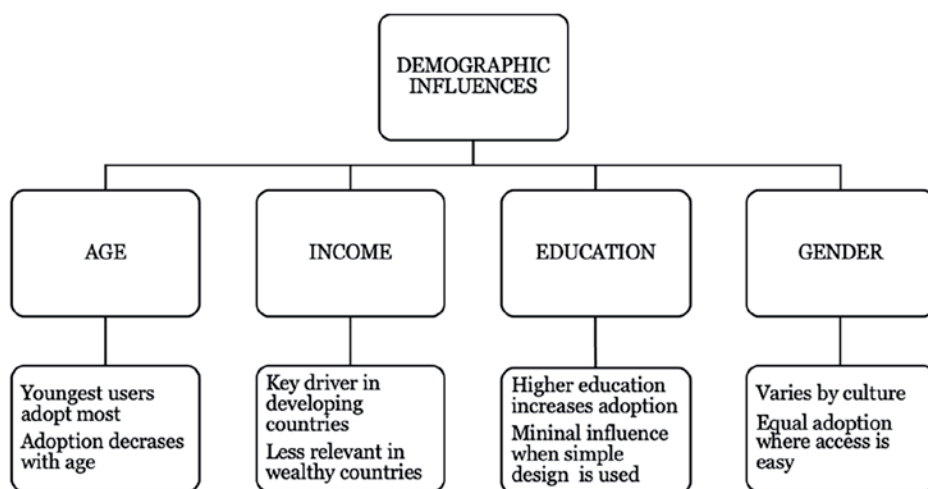


Figure 1.
Demographic patterns in fintech adoption concerning age, income, education, and gender. Source: Authors.

broader digital ecosystems [37]. Challenges persist in regions such as Pakistan and Bangladesh, where fragmented regulations and low financial literacy hinder progress despite rising mobile penetration [26, 82].

Most studies agree that regulatory clarity, government support, and cultural acceptance are critical drivers of fintech adoption. Emerging economies prioritize accessibility for underserved populations, while advanced economies focus on innovation and technological refinement, underscoring the need for context-specific strategies to address distinct regional challenges and opportunities (**Figure 2**).

5.1.7 Cryptocurrency adoption: Trust, security, and decentralized frameworks

The rise of cryptocurrencies introduces unique determinants of adoption that extend beyond traditional technology acceptance frameworks. Unlike centralized financial technologies, cryptocurrencies operate in decentralized ecosystems where trust shifts from institutional intermediaries, such as banks, to blockchain protocols, and cryptographic security mechanisms.

Empirical studies emphasize that perceived security—such as resistance to hacking, fraud, and unauthorized access in wallets and exchanges—is critical for adoption [88]. For instance, trust in decentralized exchanges (DEXs) hinges on transparent smart contract audits by third parties, as vulnerabilities in code can lead to irreversible financial losses [89].

Regulatory ambiguity remains a significant barrier, with users fearing legal repercussions due to inconsistent global frameworks [90]. Security breaches in centralized exchanges (CEXs) further underscore the need for robust cybersecurity measures,

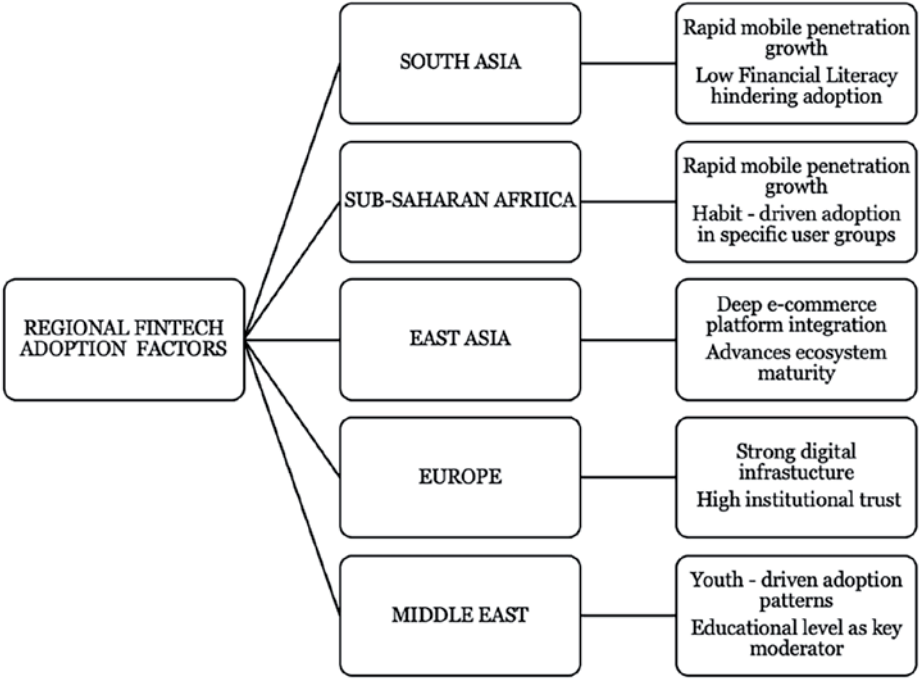


Figure 2.
Regional fintech adoption factors. Source: Authors.

driving users toward noncustodial wallets despite usability challenges (e.g., complex private key management) and risks of human error [91].

Trust in cryptocurrencies is also tied to technological transparency. Blockchain's immutable ledger fosters trust through algorithmic consensus, yet DeFi platforms face unique risks like oracle manipulation or flash loan attacks, which exploit decentralized governance gaps [92].

These findings underscore the need to redefine trust in decentralized contexts. Unlike traditional models where trust is institutionally anchored, cryptocurrency adoption requires frameworks that prioritize algorithmic transparency, regulatory clarity, and user education on security practices.

5.1.8 Synthesizing the findings of primary determinants of adoption

This synthesis integrates evidence from Sections 5.1.1–5.1.7 to address RQ1. Synthesizing the findings derived from the reviewed literature, the primary determinants influencing the adoption of fintech are intricate and interrelated. Perceived usefulness (PU) and perceived ease of use (PEOU) consistently surface as fundamental catalysts [14]. PU emerges as the strongest catalyst in distinct socioeconomic settings [93]. Further analysis reveals that trust operates three interdependent dimensions: Institutional, technological, and interpersonal trust distinctly shape risk governance and continuance intention [94]. Nonetheless, its impact is significantly mediated by perceptions of confidence and safety [95]. This aligns with findings that trust mitigates perceived risk, as evidenced in Malaysia and India, while users balance fintech benefits against privacy concerns [45, 96].

Notably, risk perceptions dominate adoption barriers in culturally distinct contexts like Pakistan [97]. Further reinforcing these dynamics, TPB [13] studies in Spain verify that attitudes, control beliefs, and social norms—combined with trust-risk assessments—jointly guide adoption decisions within context-sensitive frameworks [98].

In conclusion, while PU and PEOU establish initial acceptance, trust and security perceptions ultimately dictate adoption. Addressing these concerns is critical for designing effective fintech strategies across diverse contexts.

These complex interrelationships are visually synthesized in **Figure 3**, which conceptualizes adoption as requiring three interconnected domains: (1) Traditional factors (PU, PEOU, social influence, facilitating conditions) form essential inputs; (2) Trust and security mediate these inputs; and (3) Emerging factors (financial literacy, government support, etc.) serve as dual enhancers that simultaneously strengthen traditional factors and build trust.

5.2 Research question 2: Critical evaluation of traditional models

This section critically evaluates the capacity of TAM and UTAUT frameworks to model trust and security dynamics in fintech adoption contexts.

5.2.1 Dominant theoretical networks related to technology acceptance indexed in the literature

The review of fintech adoption literature shows that the technology acceptance model (TAM) [14] and Unified Theory of Acceptance and Use of Technology (UTAUT) [16] dominate the field. TAM primarily emphasizes perceived usefulness and ease of use [14], while UTAUT extends this foundation by incorporating

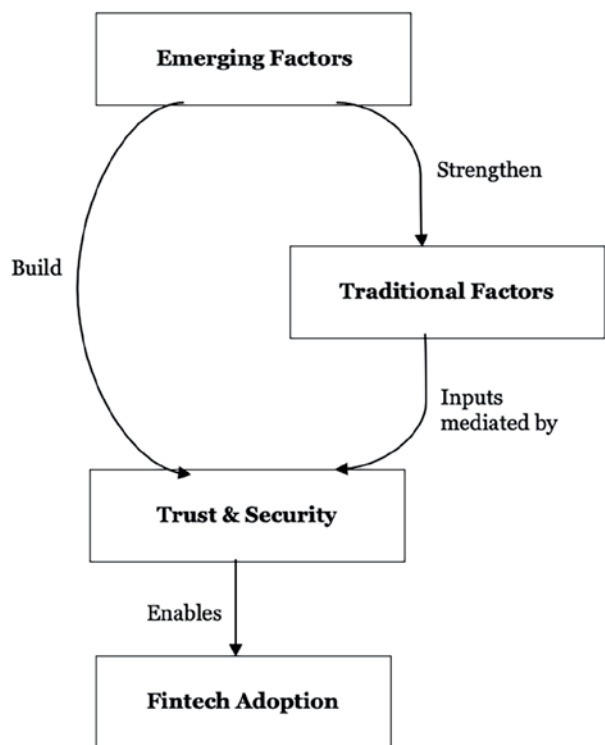


Figure 3.
Interrelationships among traditional factors, trust-security, and emerging factors in fintech adoption. Source: Authors.

social influence, facilitating conditions, and demographic moderators [16], enhancing its applicability in diverse contexts—particularly emerging markets. Though less prevalent, complementary theories like the Theory of Reasoned Action (TRA) [12] and the theory of planned behavior (TPB) [13] contribute valuable insights on attitudinal and normative influences. Worth highlighting, extended models (e.g., like TAM2 [15], UTAUT2 [17]) address complex drivers but remain less prevalent in the literature, suggesting underexplored opportunities. Despite their theoretical dominance, TAM and UTAUT suffer from significant constraints: They oversimplify human behavior and completely overlook trust and security (see Section 5.2.2) [14, 16].

Table 4 describes the frequency of theories used in fintech adoption based on the literature review.

5.2.2 Limitations in capturing trust and security dynamics

While TAM [14] and UTAUT [16] provide foundational insights, their simplified view of human behavior requires extensions to fully account for trust and security dynamics. Research demonstrates that trust and perceived ease of use significantly shape adoption attitudes in extended frameworks, though perceived usefulness lacks consistent influence [14, 27].

Similarly, trust's critical role in adoption decisions is emphasized, with perceived risk and ease of use showing negligible effects [99]. Contrasting perspectives

Theory	Unique citations	Variables	Key studies
TAM	35	44%	[20, 21, 27]
UTAUT	23	29%	[7, 24, 26]
TRA	6	8%	[33, 34, 96]
Other Theories ¹	16	19%	[1, 23, 29]
Total	80	100%	

Source: Authors.¹Includes studies applying TPB, UTAUT2, TAM2, and unclassified frameworks.

Table 4.

Dominant theories related to technology acceptance are indexed in the literature.

highlight model refinement needs: Trust links to perceived usefulness in some studies, while others associate it with transparency [19, 48]. Crucially, TAM/UTAUT inadequately addresses trust and security as mediators of risk and adoption intent [14, 16].

For instance, in Indonesia, trust dominates traditional UTAUT variables like effort expectancy, while UTAUT extensions incorporating trust reaffirm the influence of performance expectancy, effort expectancy, and social influence on FinTech Market Aggregator adoption [60]. Thus, while valuable for utility/usability assessment, these models' inherent oversimplification of behavior means their predictive power remains limited without explicit trust-security integration [14, 16].

5.3 Research question 3: Integrating emerging factors into acceptance frameworks

Building on determinants identified in Section 5.1.4, this section examines how emerging factors integrate with trust/security to enhance technology acceptance models, addressing RQ3. These factors serve as valuable complements to traditional models by addressing contextual dynamics.

Financial Literacy emerges as a significant driver in developing economies, linked to informed decision-making and higher adoption rates in Jordan and Malaysia [21, 43]. Contradictorily, it was identified as the least influential variable in Indonesia, suggesting cultural or contextual disparities [38]. Government Support proves pivotal, fostering trust and reducing perceived risks in India and China [6, 44]. In contrast, facilitating conditions proved insignificant in Ghana, indicating that top-down interventions must be adapted locally to be effective [57].

Hedonic motivation exhibits mixed outcomes: Insignificant in India and Ghana [23, 56, 72], but proved critical for sustaining user engagement in South Korea [37]. Personal Innovativeness consistently functions as a key determinant in Pakistan and Malaysia, aligning with findings from China, where technological adeptness increases trust and adoption [5, 45, 99]. However, in Bangladesh, personal innovativeness exhibited no significant effect, attributed to infrastructural barriers that limit user experimentation [7].

While core constructs (PU, PEOU, trust) remain consistent drivers, regional and demographic disparities underscore the need for adaptive frameworks. Financial literacy and government support dominate in emerging markets but fade in mature ecosystems, whereas personal innovativeness varies with user risk tolerance. Integrating these factors with trust and security into context-sensitive models is critical for global fintech adoption.

6. Conclusion

In conclusion, this study synthesizes key drivers of fintech adoption, demonstrating the enduring relevance of established acceptance frameworks while underscoring the critical need to integrate trust, security dynamics, and user perceptions with traditional models to fully explain behavioral patterns. While TAM [14] and UTAUT [16] provide foundational utility, their limitations in capturing decentralized ecosystems (e.g., cryptocurrencies) and crisis-induced behavioral shifts motivate adaptive refinements. Crucially, trust mediates risk perceptions in high-stakes contexts, while government support and financial literacy emerge as pivotal adoption bridges in emerging economies.

Moving forward, research should prioritize developing hybrid models incorporating decentralized trust mechanisms, such as blockchain; cross-regional validations of frameworks accounting for heterogeneity; and temporal analyses of crisis-driven adoption. For practitioners, advancing financial inclusion requires user-centric security design and collaborative policymaking. Addressing these gaps will enable technology-acceptance models to better reflect fintech’s evolving landscape.

Conflict of interest

The authors declare no conflict of interest.

Notes

Impact definitions (Tables 3 and 4):

- Strong (+): Supported by >70% of studies.
- Moderate (+): Supported by 50–70% of studies.
- Contextual (+/–): Impact varies by region/culture.

Abbreviations for the appendix table

Theory frameworks

TAM	technology acceptance model
UTAUT	unified theory of acceptance and use of technology
TPB	theory of planned behavior
TRA	theory of reasoned action
TTM	trust theoretic model
ServPerf	service performance
WebQual	web site quality measure
PRT	perceived risk theory

Methodology abbreviations

SEM	structural equation modeling
PLS	partial least squares
EFA	exploratory factor analysis
CFA	confirmatory factor analysis
PCA	principal component analysis
TCA	thematic content analysis
MASEM	meta-analysis using structural equation modeling
AHP	analytic hierarchy process
FAHP	fuzzy analytic hierarchy process
TOPSIS	technique for order of preference by similarity to ideal solution
SLR	systematic literature review

Other

Self-developed	Studies without established theoretical frameworks proposed context-specific models.
----------------	--

Appendix

(See **Table A1**).

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[1]	Aggarwal et al.	Examining the factors influencing fintech adoption behavior of Gen Y in India	Cogent Economics and Finance	2023	TPB	SEM-PLS
[2]	Rahim et al.	Measurement and structural modeling on factors of Islamic fintech adoption among Millennials in Malaysia	Journal of Islamic Marketing	2023	UTAUT	SEM
[4]	Kansal and Saha	The intention of fintech adoption in TAM perspective: A SEM approach	Journal of Statistics and Management Systems	2023	TAM	SEM
[5]	Shaikh and Amin	Consumers' innovativeness and acceptance toward use of financial technology in Pakistan: Extension of the UTAUT model	Information Discovery and Delivery	2023	Extended UTAUT	SEM
[6]	Das and Das	Adoption of fintech services amidst the COVID-19 pandemic: empirical evidence from Assam	Managerial Finance	2023	Extended TAM	Empirical research
[7]	Sultana et al.	Gravitating toward fintech: A study on undergraduates using the extended UTAUT model	Heliyon	2023	ExtendedUTAUT	SEM
[10]	Firmansyah et al.	Factors affecting fintech adoption: A systematic literature review	Fintech,	2022	TAM-Related Determinants, UTAUT -Related Determinants	SLR
[18]	Akinwale and Kyari	Factors influencing attitudes and intention to adopt financial technology services among the end-users in Lagos State, Nigeria	Journal of Science, Technology, Innovation and Development	2022	Extended TAM	SEM
[19]	Meyliana and Fernando	The influence of perceived risk and trust on the adoption of fintech services in Indonesia	CommIT (Communication and Information Technology) Journal	2019	Extended TAM	SEM
[20]	Singh et al.	What drives fintech adoption? A multi-method evaluation using an adapted technology acceptance model	Management Decision	2020	TAM, TAM 2, UTAUT, ServPerf and WebQual 4.0	SEM and multigroup analysis
[21]	Alkhwaldi et al.	Toward an understanding of fintech users' adoption: Intention and e-loyalty post-COVID-19 from a developing country perspective	Sustainability	2022	TAM and UTAUT	SEM-PLS

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[22]	Khan et al.	Determinants of behavioral intentions to use Islamic financial technology: An empirical assessment	Risks	2022	UTAUT	SEM-PLS
[23]	Amnas et al.	Understanding the determinants of fintech adoption: Integrating UTAUT2 with the trust theoretic model	Journal of Risk and Financial Management	2023	UTAUT2 TTM	PLS
[24]	Bajunaied et al.	Behavioral intention to adopt fintech services: An extension of the unified theory of acceptance and use of technology	Journal of Open Innovation: Technology, Market, and Complexity	2023	Extended UTAUT	SEM-PLS
[25]	Yohanes et al.	The Unified Theory of Acceptance and Use of Technology (UTAUT) model perspective to enhance user acceptance of fintech application	International Conference on Information Management and Technology (ICIMTech)	2020	Extended UTAUT	PLS
[26]	Hassan et al.	Drivers influencing the adoption intention toward mobile fintech services: A study on the emerging Bangladesh market	Information	2022	Extended UTAUT	SEM-PLS
[31]	Fernando et al.	Development and validation of instruments adoption of fintech services in Indonesia (Perspective of trust and risk)	International conference on sustainable information engineering and technology (SIET)	2018	Extended TAM	SEM-PLS
[33]	Ali et al.	How perceived risk, benefit, and trust determine user fintech adoption: A new dimension for Islamic finance	Foresight	2021	TPR	SEM - PLS
[34]	Gerlach and Lutz	Evidence on usage behavior and future adoption intention of Fintechs and digital finance solutions	The International Journal of Business and Finance Research	2019	TRA, UTAUT2	Empirical analysis
[36]	Keong et al.	Perceived risk factors affect intention to use FinTech	Journal of Accounting and Finance in Emerging Economies	2020	TRA, PRT	SEM-PLS
[37]	Ryu	What makes users willing or hesitant to use fintech?: The moderating effect of user type	Industrial Management and Data Systems	2018	Not available (self-developed)	PLS

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[38]	Setiawan et al.	User innovativeness and fintech adoption in Indonesia	Journal of Open Innovation: Technology, Market, and Complexity	2021	TAM	SEM - PLS
[41]	Bouteraa et al.	Understanding consumers' barriers to using fintech services in the United Arab Emirates: Mixed-Methods research approach	Sustainability	2023	Extended UTAUT	TCA, SEM-PLS
[28]	Almashhadani et al.	Exploring the determinants of fintech adoption and intention to use in Jordan: The impact of COVID-19	Cogent Social Sciences	2023	TAM, UTAUT	SEM
[43]	Taufiq et al.	Does financial literacy or digital literacy determine a consumer's use of fintech?	International Conference on Business and Technology (pp. 289–298). Cham: Springer International	2022	Extended TAM	SEM
[45]	Samarasekara et al.	Unlocking the key drivers of fintech adoption: The mediating role of trust among Malaysians	Migration Letters	2023	TAM	SEM
[29]	Jangir et al.	The moderating effect of perceived risk on users' continuance intention for fintech services	Journal of Risk and Financial Management	2022	UTAUT2	SEM-PLS
[27]	Shahzad et al.	COVID-19's impact on fintech adoption: Behavioral intention to use the financial portal	Journal of Risk and Financial Management	2022	Extended TAM	PLS
[46]	Daqar et al.	Fintech in the eyes of Millennials and Generation Z (the financial behavior and fintech perception)	Banks and Bank Systems	2020	Modified TAM	Descriptive Research
[47]	Huei et al.	Preliminary study on consumer attitude toward fintech products and services in Malaysia	International Journal of Engineering and Technology	2018	Extended TAM	SEM
[44]	Nangin et al.	The effects of perceived ease of use, security, and promotion on trust and its implications on fintech adoption	Journal of Consumer Sciences	2020	Not available (self-developed)	SEM-PLS

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[48]	Jünger and Mietzner	Banking goes digital: The adoption of fintech services by German households	Finance Research Letters	2020	TAM	Principal Component Analysis
[49]	Jin et al.	Factors affecting the consumer acceptance of fintech products and services in Malaysia	International Journal of Asian Social Science	2019	TAM	Literature review
[50]	Joo	Understanding acceptance of fintech service in Korea: Focused on decomposed TPB into TAM	Journal of Digital Convergence	2017	TAM, TPB	PLS
[51]	Ashraf et al.	Factors affecting the adoption of fintech in Pakistan based on the Unified Theory of Acceptance and Use of Technology Model: An empirical study on financial inclusion in Pakistan	Journal of Financial Technologies (Fintech), Inclusion and Sustainability	2022	UTAUT	SEM-PLS
[52]	Tohang et al.	Financial Technology 3.0 adoption in financial and nonfinancial institutions from the Modified UTAUT perspective	Conference on International Issues in Business and Economics Research (CIIBER 2019)	2021	Modified UTAUT	PLS
[53]	Fu and Mishra	Fintech in the time of COVID–19: Technological adoption during crises	Journal of Financial Intermediation	2022	Not available (self-developed)	Preliminary analysis
[54]	Linh and Tuyen	Factors affecting the intention to use fintech services in Vietnam	Economics, Management, and Business	2020	Modified TAM	Panel data regression
[55]	Alamoodi and Selamat	Determinants of fintech products and aervices adoption in Kingdom of Saudi Arabia (KSA)	Journal of International Business, Economics and Entrepreneurship	2021	Extended TAM	Reliability Analysis
[56]	Shehata et al.	Factors affecting customers' adoption of fintech in the Gulf Cooperation Council countries	Asian Economic and Financial Review	2023	TAM, UTAUT	SEM-PLS
[57]	Antwi-Boampong et al.	Factors affecting port users' behavioral intentions to adopt financial technology (fintech) in ports in Sub-Saharan Africa: A case of ports in Ghana	Fintech	2022	UTAUT2	PCA, CFA, SEM

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[58]	Pertiwi and Purwanto	Analysis of adopting Millennial Generation financial technology (fintech) Services	International Journal of Business Management and Economic Review	2021	Not available (self-developed)	SEM-PLS
[59]	Nayak et al.	Data security and trust affect the users of fintech?	International Journal of Management	2021	Extended TAM	EFA
[60]	Kurniasari et al.	Determinant factors of fintech adoption in organizations using the UTAUT theory approach	Journal of Business and Management Review	2023	Extended UTAUT	SEM
[61]	Al Nawayseh MK	Fintech in COVID-19 and beyond: What factors are affecting customers' choice of fintech applications?	Journal of Open Innovation: Technology, Market, and Complexity	2020	Modified UTAUT	SEM
[62]	Widiatmo	Technology acceptance model analysis of adoption intention to use Indonesian Islamic fintech Apps Amid the COVID-19 pandemic	TIJARI International Journal of Islamic Economics, Business and Entrepreneurship, 1(3), 80–107	2021	Extended TAM	SEM-PLS
[63]	Stewart and Jürjens	Data security and consumer trust in fintech innovation in Germany	Information and Computer Security,	2018	Extended TAM	CFA, SEM
[64]	Yan et al.	Factors influencing the adoption intention of using mobile financial service during the COVID-19 pandemic: The role of fintech	Environmental Science and Pollution Research volume	2021	Extended UTAUT	SEM
[65]	Wang	What determines customers' continuance intention of fintech? Evidence from YuEbao	Industrial Management and Data Systems	2019	Not available (self-developed)	SEM-PLS
[36]	Tang et al.	Perceived risk factors affect intention to use fintech	Journal of Accounting and Finance in Emerging Economies	2020	TRA	SEM
[66]	Feng et al.	Determinants of technology acceptance: Two model-based meta-analytic reviews	Journalism and Mass Communication Quarterly	2021	Extended TAM	MASEM
[67]	Ayoungman et al.	User attitude and intentions toward fintech in Bangladesh	International Journal of Asian Business and Information Management	2021	TAM and TPB	PLS

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[68]	Huarng and Yu	Causal complexity analysis for fintech adoption at the country level	Journal of Business Research	2022	Not available (self-developed)	Fuzzy set/Qualitative Comparative Analysis
[69]	Yang and Zhang	Fintech adoption and financial inclusion: Evidence from household consumption in China	Journal of Banking and Finance,	2022	Not available (self-developed)	Heterogeneity analysis
[70]	Le	Examining factors that boost intention and loyalty to use fintech post-COVID-19 lockdown as a new normal behavior	Heliyon,	2021	TRA and TAM	SEM-PLS
[71]	Jain and Raman	A partial least squares approach to digital finance adoption	Journal of Financial Services Marketing	2022	Not available (self-developed)	SEM-PLS
[72]	Sakhare et al.	What drives fintech adoption? A study on perception, adoption, and constraints of fintech services	European Economic Letters	2023	Not available (self-developed)	EFA, CFA
[73]	Haqqi and Suzianti	Exploring risk and benefit factors affecting user adoption intention of fintech in Indonesia	Proceedings of the 3rd Asia Pacific Conference on Research in Industrial and Systems Engineering	2020	Not available (self-developed)	SEM-PLS
[74]	Sa'diyah	Analysis of factors affecting adoption of financial technology application	Sentralisasi	2021	TAM	PLS
[75]	Lachhwani and Jain	A study on consumer attitude toward fintech services	Skips Anveshan	2021	Not available (self-developed)	Descriptive Research
[76]	Swacha-Lech and Solarz	Determinants of the adoption of innovative fintech services by Millennials	E and M Ekonomie a Management	2021	Not available (self-developed)	Logistic regression
[77]	Khatun and Tamanna	Factors affecting the adoption of fintech: A study based on the financial institutions in Bangladesh	Copernican Journal of Finance and Accounting	2020	Modified UTAUT	SEM with the Generalized Least Squares method
[78]	Tun-Pin et al.	An adoption of fintech services in Malaysia	South East Asia Journal of Contemporary Business	2019	TAM, UTAUT	Regression Analysis

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[79]	Singh et al.	Exploring trust and responsiveness as antecedents for intention to use fintech services	International Journal of Economics and Business Research	2021	Extended TAM	ESM-EFA
[80]	Darmansyah et al.	Factors determining behavioral intentions to use Islamic financial technology: Three competing models	Journal of Islamic Marketing	2020	TAM	SEM-PLS
[81]	Hasan and al.	Evaluating drivers of fintech adoption in the Netherlands	Global Business Review	2021	TAM and VAM	Correlation analysis and frequency analysis
[82]	Noreen et al.	Role of government policies in fintech adoption and financial inclusion: A study in Pakistan	Universal Journal of Accounting and Finance	2022	Not available (self-developed)	Literature review
[83]	Nurjaman et al.	Assessing the adoption of fintech acceptance among Indonesian Gen-Z using the UTAUT model and SEM analysis	International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS)	2023	UTAUT	SEM
[84]	Natsir et al.	The implementation of the technology acceptance model in analyzing attitudes toward the adoption of fintech	International Journal of Application on Economics and Business	2023	Extended TAM	SEM-PLS
[85]	Daragmeh et al.	FinTech payments in the era of COVID-19: Factors influencing behavioral intentions of “Generation X” in Hungary to use mobile payment	Behavioral and Experimental Finance	2021	Extended TAM 2	SEM
[86]	Mu and Lee	An application of fuzzy AHP and TOPSIS methodology for ranking the factors influencing fintech adoption intention: A comparative study of China and Korea	Journal of Service Research and Studies	2017	UTAUT2	FAHP
[87]	Utami et al.	Adoption of fintech products: A systematic literature review	Journal of Creative Communications	2021	Not available (self-developed)	SLR

Nr.	Author/s	Title	Source	Year	Theory examined	Methodology used
[93]	Fernando	Analysis of the influence of consumer behavior using fintech services with SEM and TOPSIS	International conference on information management and technology (ICIMTech)	2019	TAM	SEM
[94]	Xie et al.	Understanding fintech platform adoption: Impacts of perceived value and perceived risk	Journal of Theoretical and Applied Electronic Commerce	2021	Extended UTAUT	SEM
[95]	Xia et al.	Trust in fintech: Risk, governance, and continuance intention	Journal of Computer Information Systems	2022	Not available (self-developed)	SEM-PLS
[96]	Gupta et al.	Determinants of continuous intention to use fintech services: the moderating role of COVID-19	Journal of Financial Services Marketing	2023	TAM, TRA	EFA, SEM
[97]	Saleem	Fintech revolution, perceived risks, and fintech adoption: Evidence from the financial industry of Pakistan	International Journal of Multidisciplinary and Current Educational Research	2021	Not available (self-developed)	Multi-method quantitative analysis
[98]	Irimia-Diéguez	Predicting fintech innovation adoption: the mediator role of social norms and attitudes	Finance Innovation	2023	TPB, TRA	SEM-PLS
[99]	Hu et al.	Adoption intention of fintech services for bank users: An empirical examination with an extended technology acceptance model	Symmetry	2021	Extended TAM	SEM

Table A1.

Author details

Nikolaos Papanikolaou¹, Paraskevi Boufounou^{1*} and Nikolaos Eriotis²

1 Department of Economics, National and Kapodistrian, University of Athens, Greece

2 Department of Business Administration, National and Kapodistrian, University of Athens, Greece

*Address all correspondence to: pboufounou@econ.uoa.gr

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Aggarwal M, Nayak KM, Bhatt V. Examining the factors influencing fintech adoption behaviour of gen Y in India. *Cogent Economics and Finance*. 2023;**11**:2197699. DOI: 10.1080/23322039.2023.2197699
- [2] Rahim NF, Bakri MH, Fianto BA, Zainal N, Al Shami H, SA. Measurement and structural modelling on factors of Islamic fintech adoption among millennials in Malaysia. *Journal of Islamic Marketing*. 2023;**14**:1463-1487. DOI: 10.1108/JIMA-09-2020-0279
- [3] Boufounou P, Eriotis N, Gekas K, Kounadeas T. The COVID-19 Pandemic, the Digital Transformation, and the Banking System: Empirical Evidence in Greece. London: IntechOpen; 2024. DOI: 10.5772/intechopen.1004205
- [4] Kansal A, Saha S. The intention of fintech adoption in TAM perspective: A SEM approach. *Journal of Statistics & Management Systems*. 2023;**26**:505-514. DOI: 10.47974/JSMS-1043
- [5] Shaikh IM, Amin H. Consumers' innovativeness and acceptance towards use of financial technology in Pakistan: Extension of the UTAUT model. *Information Discovery and Delivery*. 2024;**52**(1):114-122. DOI: 10.1108/IDD-08-2022-0080
- [6] Das A, Das D. Adoption of fintech services amidst COVID-19 pandemic: Empirical evidence from Assam. *Managerial Finance*. 2023;**49**:1075-1093. DOI: 10.1108/MF-08-2022-0379
- [7] Sultana N, Chowdhury RS, Haque A. Gravitating towards fintech: A study on undergraduates using extended UTAUT model. *Heliyon*. 2023;**9**:e20731. DOI: 10.1016/j.heliyon.2023.e20731
- [8] Liu Q, Chan KC, Chimhundu R. Fintech research: Systematic mapping, classification, and future directions. *Financial Innovation*. 2024;**10**:24. DOI: 10.1186/s40854-023-00524-z
- [9] Muganyi T, Yan L, Yin Y, Sun H, Gong X, Taghizadeh-Hesary F. Fintech, regtech, and financial development: Evidence from China. *Financial Innovation*. 2022;**8**:1-20. DOI: 10.1186/s40854-021-00313-6
- [10] Firmansyah EA, Masri M, Anshari M, Besar MHA. Factors affecting fintech adoption: A systematic literature review. *Fintech*. 2022;**2**:21-33. DOI: 10.3390/fintech2010002
- [11] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*. 2021;**372**:n71. DOI: 10.1136/bmj.n71
- [12] Ajzen I, Fishbein M. A Bayesian analysis of attribution processes. *Psychological Bulletin*. 1975;**82**:261-267. DOI: 10.1037/h0076477
- [13] Ajzen I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. 1991;**50**:179-211. DOI: 10.1016/0749-5978(91)90020-T
- [14] Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*. 1989;**13**:319-340. DOI: 10.2307/249008
- [15] Venkatesh V, Davis FD. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*. 2000;**46**:186-204. DOI: 10.1287/mnsc.46.2.186.11926

- [16] Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: Toward a unified view. *MIS Quarterly*. 2003;27:425-478. DOI: 10.2307/30036540
- [17] Venkatesh V, Thong JYL, Xu X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*. 2012;36:157-178. DOI: 10.2307/41410412
- [18] Akinwale YO, Kyari AK. Factors influencing attitudes and intention to adopt financial technology services among the end-users in Lagos state, Nigeria. *African Journal of Science, Technology, Innovation and Development*. 2022;14:272-279. DOI: 10.1080/20421338.2020.1835177
- [19] Meyliana M, Fernando E. The influence of perceived risk and trust in adoption of fintech services in Indonesia. *CommIT (Communication and Information Technology) Journal*. 2019;13:31-37. DOI: 10.21512/commit.v13i1.5708
- [20] Singh S, Sahni MM, Kovid RK. What drives fintech adoption? A multi-method evaluation using an adapted technology acceptance model. *Management Decision*. 2020;58:1675-1697. DOI: 10.1108/MD-09-2019-1318
- [21] Alkhwaldi AF, Alharasis EE, Shehadeh M, Abu-AlSondos IA, Oudat MS, Bani Atta AA. Towards an understanding of fintech users' adoption: Intention and e-loyalty post-COVID-19 from a developing country perspective. *Sustainability*. 2022;14:12616. DOI: 10.3390/su141912616
- [22] Khan MS, Rabbani MR, Hawaldar IT, Bashar A. Determinants of behavioral intentions to use Islamic financial technology: An empirical assessment. *Risks*. 2022;10:114. DOI: 10.3390/risks10060114
- [23] Amnas MB, Selvam M, Raja M, Santhoshkumar S, Parayitam S. Understanding the determinants of fintech adoption: Integrating UTAUT2 with trust theoretic model. *Journal of Risk and Financial Management*. 2023;16:505. DOI: 10.3390/jrfm16120505
- [24] Bajunaied K, Hussin N, Kamarudin S. Behavioral intention to adopt fintech services: An extension of unified theory of acceptance and use of technology. *Journal of Open Innovation: Technology, Market, and Complexity*. 2023;9:100010. DOI: 10.1016/j.joitmc.2023.100010
- [25] Yohanes K, Junius K, Saputra Y, Sari R, Lisanti Y, Luhukay D. Unified theory of acceptance and use of technology (UTAUT) model perspective to enhance user acceptance of fintech application. In: *Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech)*; 19-20 August 2020; Jakarta, Indonesia. New York: IEEE; 2020. pp. 643-648. DOI: 10.1109/ICIMTech50083.2020.9211250
- [26] Hassan MS, Islam MA, Sobhani FA, Nasir H, Mahmud I, Zahra FT. Drivers influencing the adoption intention towards mobile fintech services: A study on the emerging Bangladesh market. *Information*. 2022;13:349. DOI: 10.3390/info13070349
- [27] Shahzad A, Zahrullail N, Akbar A, Mohelska H, Hussain A. COVID-19's impact on fintech adoption: Behavioral intention to use the financial portal. *Journal of Risk and Financial Management*. 2022;15:428. DOI: 10.3390/jrfm15100428
- [28] Almashhadani IS, Abuhashesh M, Bany Mohammad A, Masa'deh RE,

- Al-Khasawneh M. Exploring the determinants of fintech adoption and intention to use in Jordan: The impact of COVID-19. *Cogent Social Science*. 2023;**9**:2256536. DOI: 10.1080/23311886.2023.2256536
- [29] Jangir K, Sharma V, Taneja S, Rupeika-Apoga R. The moderating effect of perceived risk on users' continuance intention for fintech services. *Journal of Risk and Financial Management*. 2022;**16**:21. DOI: 10.6007/IJARBSS/v12-i4/13035
- [30] Lewis JD, Weigert A. Trust as a social reality. *Social Forces*. 1985;**63**:967-985. DOI: 10.1093/sf/63.4.967
- [31] Fernando E, Surjandy S, Widjaja M, Touriano D. Development and validation of instruments adoption fintech services in Indonesia (perspective of trust and risk). In: *Proceedings of the 2018 International Conference on Sustainable Information Engineering and Technology (SIET)*; 10-12 November 2018; Malang, Indonesia. New York: IEEE; 2018. pp. 283-287. DOI: 10.1109/SIET.2018.8693192
- [32] Chandon P, Wansink B, Laurent G. A benefit congruency framework of sales promotion effectiveness. *Journal of Marketing*. 2000;**64**:65-81. DOI: 10.1509/jmkg.64.4.65.18071
- [33] Ali M, Raza SA, Khamis B, Puah CH, Amin H. How perceived risk, benefit and trust determine user fintech adoption: A new dimension for Islamic finance. *Foresight*. 2021;**23**:403-420. DOI: 10.1108/FS-09-2020-0095
- [34] Gerlach JM, Lutz JK. Evidence on usage behavior and future adoption intention of fintechs and digital finance solutions. *International Journal of Business Management and Finance Research*. 2019;**13**:83-105. DOI: 10.2139/ssrn.3489024
- [35] Kim DJ, Ferrin DL, Rao HR. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*. 2008;**44**:544-564. DOI: 10.1016/j.dss.2007.07.001
- [36] Keong OC, Leong TK, Bio CJ. Perceived risk factors affect intention to use fintech. *Journal of Accounting and Finance in Emerging Economies*. 2020;**6**:453-463. DOI: 10.26710/jafee.v6i2.1101
- [37] Ryu HS. What makes users willing or hesitant to use fintech?: The moderating effect of user type. *Industrial Management & Data Systems*. 2018;**118**:541-569. DOI: 10.1108/IMDS-07-2017-0325
- [38] Setiawan B, Nugraha DP, Irawan A, Nathan RJ, Zoltan Z. User innovativeness and fintech adoption in Indonesia. *Journal of Open Innovation: Technology, Market, and Complexity*. 2021;**7**:188. DOI: 10.3390/joitmc7030188
- [39] Lu J, Yao JE, Yu CS. Personal innovativeness, social influences and adoption of wireless internet services via mobile technology. *The Journal of Strategic Information Systems*. 2005;**14**:245-268. DOI: 10.1016/j.jsis.2005.07.003
- [40] Yoon J, Vonortas NS, Han S. Do-it-yourself laboratories and attitude toward use: The effects of self-efficacy and the perception of security and privacy. *Technological Forecasting and Social Change*. 2020;**159**:120192. DOI: 10.1016/j.techfore.2020.120192
- [41] Bouteraa M, Chekima B, Lajuni N, Anwar A. Understanding consumers' barriers to using fintech services in the United Arab Emirates: Mixed-methods research approach. *Sustainability*. 2023;**15**:2931. DOI: 10.3390/su15042931

- [42] Hoffmann A, Otteby K. Personal finance blogs: Helpful tool for consumers with low financial literacy or preaching to the choir? *International Journal of Consumer Studies*. 2018;**42**:241-254. DOI: 10.1111/ijcs.12412
- [43] Taufiq M, Chung TF, Chrisniyanti A. Does financial literacy or digital literacy determine a consumer use of fintech? In: *Proceedings of the International Conference on Business and Technology*; 2022; Istanbul, Turkey. Cham: Springer; 2022. pp. 289-298. DOI: 10.1007/978-3-031-26953-0_28
- [44] Nangin MA, Barus IRG, Wahyoedi S. The effects of perceived ease of use, security, and promotion on trust and its implications on fintech adoption. *Journal of Consumer Sciences*. 2020;**5**:124-138. DOI: 10.29244/jcs.5.2.124-138
- [45] Samarasekara L, Tanaraj K, Rajespari K, Sundarasan S, Rajagopalan U. Unlocking the key drivers of fintech adoption: The mediating role of trust among Malaysians. *Migration Letters*. 2023;**20**:505-521. DOI: 10.47059/ml.v20i3.2934
- [46] Daqar MAMA, Arqawi S, Karsh SA. Fintech in the eyes of millennials and generation Z (the financial behavior and Fintech perception). *Banks and Bank Systems*. 2020;**15**(3):20-28. DOI: 10.21511/bbs.15(3).2020.03
- [47] Huei CT, Cheng LS, Seong LC, Khin AA, Bin RLL. Preliminary study on consumer attitude towards fintech products and services in Malaysia. *International Journal of Engineering and Technology*. 2018;**7**(2):166-169. DOI: 10.14419/ijet.v7i2.29.13310
- [48] Jünger M, Mietzner M. Banking goes digital: The adoption of fintech services by German households. *Finance Research Letters*. 2020;**34**:101260. DOI: 10.1016/j.frl.2019.08.008
- [49] Jin CC, Seong LC, Khin AA. Factors affecting the consumer acceptance towards fintech products and services in Malaysia. *International Journal of Asian Social Science*. 2019;**9**(1):59-65. DOI: 10.18488/journal.1.2019.91.59.65
- [50] Joo J. Understanding acceptance of Fintech Service in Korea: Focused on decomposed TPB into TAM. *Journal of Digital Convergence*. 2017;**15**(4):171-179. DOI: 10.14400/JDC.2017.15.4.171
- [51] Ashraf M, Hafeez R, Sajid AN. Factors affecting the adoption of fintech in Pakistan based on the unified theory of acceptance and use of technology model: An empirical study on financial inclusion in Pakistan. *Journal of Financial Technologies (Fintech), Inclusion and Sustainability*. 2022;**1**(1):9-26. DOI: 10.52461/jftis.v1i1.1793
- [52] Tohang V, Lo E, Anggraeni A. Financial technology 3.0 adoption in financial and non-financial institutions from modified Utaut perspective. In: *Proceedings of the Conference on International Issues in Business and Economics Research (CIIBER 2019)*; January 2021. Dordrecht, The Netherlands: Atlantis Press; 2021. pp. 1-6. DOI: 10.2991/aebmr.k.210121.001
- [53] Fu J, Mishra M. Fintech in the time of COVID-19: Technological adoption during crises. *Journal of Financial Intermediation*. 2022;**50**:100945. DOI: 10.1016/j.jfi.2021.100945
- [54] Linh NHN, Tuyen DQ. Factors affecting the intention to use fintech services in Vietnam. *Economies*. 2020;**10**:57. DOI: 10.3390/economies10030057
- [55] Alamoodi MAA, Selamat Z. Determinants of fintech products and services adoption in Kingdom of Saudi Arabia (KSA). *The Journal of*

International Business, Economics and Entrepreneurship. 2021;**6**:1-8. DOI: 10.24191/jibe.v6i2.16637

[56] Shehata SM, Abdeljawad AM, Mazouz LA, Aldossary LYK, Alsaeed MY, Sayed MN. Factors affecting customers' adoption of fintech in the gulf cooperation council countries. *Asian Economic and Financial Review*. 2023;**13**(7):463-477. DOI: 10.55493/5002.v13i7.4800

[57] Antwi-Boampong A, Boison DK, Doumbia MO, Boakye AN, Osei-Fosua L, Owiredo SK. Factors affecting port users' behavioral intentions to adopt financial technology (fintech) in ports in sub-Saharan Africa: A case of ports in Ghana. *Fintech*. 2022;**1**:362-375. DOI: 10.3390/fintech1040027

[58] Pertiwi TK, Purwanto E. Analysis of adopting millennial generation financial technology (Fintech) services. *International Journal of Business Management and Economic Review*. 2021;**4**(3):36-47. DOI: 10.35409/IJBMER.2021.3257

[59] Nayak K, Singh P, Dave P. Does data security and trust affect the users of fintech? *International Journal of Management*. 2021;**12**:1-12. DOI: 10.34218/IJM.12.1.2021.016

[60] Kurniasari F, Utomo P, Jimmy SY. Determinant factors of fintech adoption in organization using UTAUT theory approach. *Journal of Business and Management Review*. 2023;**4**:092-103. DOI: 10.47153/jbmr42.6032023

[61] Al Nawayseh MK. Fintech in COVID-19 and beyond: What factors are affecting customers' choice of fintech applications? *Journal of open innovation: Technology, Market, and Complexity*. 2020;**6**(4):153. DOI: 10.3390/joitmc6040153

[62] Widiatmo G. Technology acceptance model analysis of adoption intention to use Indonesian Islamic Fintech apps amid the COVID-19 pandemic. *TIJARI International Journal of Islamic Economics, Business and Entrepreneurship*. 2021;**1**(3):80-107

[63] Stewart H, Jürjens J. Data security and consumer trust in fintech innovation in Germany. *Information and Computer Security*. 2018;**26**:109-128. DOI: 10.1108/ICS-06-2017-0039

[64] Yan C, Siddik AB, Akter N, Dong Q. Factors influencing the adoption intention of using mobile financial service during the COVID-19 pandemic: The role of fintech. *Environmental Science and Pollution Research*. 2021;**30**:61271-61289. DOI: 10.1007/s11356-021-17437-y

[65] Wang Z, Zhengzhi Gordon GU, Hou F, Li B, Zhou W. What determines customers' continuance intention of Fintech? Evidence from YuEbao. *Industrial Management & Data Systems*. 2019;**119**(8):1625-1637. DOI: 10.1108/imds-01-2019-0011

[66] Feng GC, Su X, Lin Z, He Y, Luo N, Zhang Y. Determinants of technology acceptance: Two model-based meta-analytic reviews. *Journalism and Mass Communication Quarterly*. 2021;**98**(1):83-104. DOI: 10.1177/1077699020952400

[67] Ayoungman FZ, Chowdhury NH, Hussain N, Tanchangya P. User attitude and intentions towards fintech in Bangladesh. *International Journal of Asian Business and Information Management (IJABIM)*. 2021;**12**(3):1-19. DOI: 10.4018/ijabim.20210701.0a30

[68] Huarng KH, Yu THK. Causal complexity analysis for fintech adoption at the country level. *Journal of*

- Business Research. 2022;**153**:228-234. DOI: 10.1016/j.jbusres.2022.08.030
- [69] Yang T, Zhang X. FinTech adoption and financial inclusion: Evidence from household consumption in China. *Journal of Banking & Finance*. 2022;**145**:106668. DOI: 10.1016/j.jbankfin.2022.106668
- [70] Le MT. Examining factors that boost intention and loyalty to use Fintech post-COVID-19 lockdown as a new normal behavior. *Heliyon*. 2021;**7**(8):e07821. DOI: 10.1016/j.heliyon.2021.e07821
- [71] Jain N, Raman TV. A partial least squares approach to digital finance adoption. *Journal of Financial Services Marketing*. 2022;**27**:1-14. DOI: 10.1057/s41264-021-00127-8
- [72] Sakhare CA, Somani NN, Patel BL, Khorgade SN, Parchake S. What drives fintech adoption? A study on perception, adoption, and constraints of fintech services. *European Economic Letters*. 2023;**13**:1216-1230. DOI: 10.59652/eel.v13i3.418
- [73] Haqqi FR, Suzianti A. Exploring risk and benefit factors affecting user adoption intention of fintech in Indonesia. In: *Proceedings of the 3rd Asia Pacific Conference on Research in Industrial and Systems Engineering*; June 2020. New York, NY, USA: ACM; 2020. pp. 13-18. DOI: 10.1145/3400934.3400939
- [74] Sa'diyah C. Analysis of factors affecting adoption of financial technology application. *Sentralisasi*. 2021;**10**(1):57-70. DOI: 10.33506/sl.v10i1.1208
- [75] Lachhwani H, Jain R. A study on consumer attitude towards Fintech services. *Skips Anveshan*. 2021;**2**(1):1-8. DOI: 10.53031/skips.2.1.2021.03
- [76] Swacha-Lech M, Solarz M. Determinants of the adoption of innovative fintech services by millennials. *The Journal E&M Economics and Management*. 2021;**24**:1-18. DOI: 10.15240/tul/001/2021-3-009
- [77] Khatun N, Tamanna M. Factors affecting the adoption of Fintech: A study based on the financial institutions in Bangladesh. *Copernican Journal of Finance and Accounting*. 2020;**9**(4):51-75. DOI: 10.12775/cjfa.2020.021
- [78] Tun-Pin C, Keng-Soon WC, Yen-San Y, Pui-Yee C, Hong-Leong JT, Shwu-Shing N. An adoption of fintech service in Malaysia. *South East Asian Journal of Contemporary Business*. 2019;**18**:134-147
- [79] Singh S, Sahni MM, Kovid RK. Exploring trust and responsiveness as antecedents for intention to use FinTech services. *International Journal of Economics and Business Research*. 2021;**21**(2):254-268. DOI: 10.1504/IJEBr.2021.113152
- [80] Darmansyah FBA, Hendratmi A, Aziz PF. Factors determining behavioral intentions to use Islamic financial technology: Three competing models. *Journal of Islamic Marketing*. 2020;**12**(6):1140-1156. DOI: 10.1108/JIMA-12-2019-0252
- [81] Hasan R, Ashfaq M, Shao L. Evaluating drivers of Fintech adoption in the Netherlands. *Global Business Review*. 2021;**24**(4):1-15. DOI: 10.1177/09721509211027402
- [82] Noreen M, Mia MS, Ghazali Z, Ahmed F. Role of government policies to fintech adoption and financial inclusion: A study in Pakistan. *Universal Journal of Accounting and Finance*. 2022;**10**:37-46. DOI: 10.13189/ujaf.2022.100105
- [83] Nurjaman J, Saputra M, Puspitasari W, Bazen J. Assessing the

- adoption of Fintech acceptance among Indonesian gen-Z using UTAUT model and SEM analysis. In: Proceedings of the 2023 International Conference on Advancement in Data Science, E-Learning and Information System (ICADEIS); August 2023. Piscataway, NJ, USA: IEEE; 2023. pp. 1-6. DOI: 10.1109/ICADEIS58666.2023.10271081
- [84] Natsir K, Arifin AZ, Darmawan H. The implementation of technology acceptance model in analyzing attitudes toward the adoption of fintech. *International Journal of Application on Economics and Business*. 2023;1(2):386-400. DOI: 10.24912/ijaeb.v1i2.386-400
- [85] Daragmeh A, Lentner C, Sági J. FinTech payments in the era of COVID-19: Factors influencing behavioral intentions of "generation X" in Hungary to use mobile payment. *Journal of Behavioral and Experimental Finance*. 2021;32:100574. DOI: 10.1016/j.jbef.2021.100574
- [86] Mu HL, Lee YC. An application of fuzzy AHP and TOPSIS methodology for ranking the factors influencing FinTech adoption intention: A comparative study of China and Korea. *Journal of Service Research and Studies*. 2017;7(4):51-68. DOI: 10.18807/jsrs.2017.7.4.051
- [87] Utami AF, Ekaputra IA, Japutra A. Adoption of FinTech products: A systematic literature review. *Journal of Creative Communications*. 2021;16(3):233-248. DOI: 10.1177/09732586211032092
- [88] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work Blockchains. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. October 2016, Vienna, Austria. 2016. pp. 3-16. DOI: 10.1145/2976749.2978341
- [89] Chen Y, Bellavitis C. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*. 2020;13:e00151. DOI: 10.1016/j.jbvi.2019.e00151
- [90] Zetzsche DA, Buckley RP, Arner DW, Barberis JN. From FinTech to TechFin: The regulatory challenges of data-driven finance. *NYU Journal of Law and Business*. 2020;17(2):393-446. DOI: 10.2139/ssrn.2959925
- [91] Krombholz K, Judmayer A, Gusenbauer M, Weippl E. The other side of the coin: User experiences with bitcoin security and privacy. In: Grossklags J, Preneel B, editors. *Financial Cryptography and Data Security*. FC 2016. Lecture Notes in Computer Science. Vol. 9603. Berlin, Heidelberg: Springer; 2017. pp. 555-580. DOI: 10.1007/978-3-662-54970-4_33
- [92] Qin K, Zhou L, Gervais a. quantifying blockchain extractable value: How dark is the forest? In: *2022 IEEE Symposium on Security and Privacy (SP)*. Piscataway, NJ, USA: IEEE; 2022. pp. 198-214. DOI: 10.1109/SP46214.2022.9833734
- [93] Fernando E. Analysis of the influence of consumer behavior using FinTech services with SEM and TOPSIS. 2019 *International Conference on Information Management and Technology (ICIMTech)*. 2019;1:93-97. DOI: 10.1109/ICIMTech.2019.8843843
- [94] Xie J, Ye L, Huang W, Ye M. Understanding fintech platform adoption: Impacts of perceived value and perceived risk. *Journal of Theoretical and Applied Electronic Commerce Research*. 2021;16:1893-1911. DOI: 10.3390/jtaer16050106
- [95] Xia H, Lu D, Lin B, Nord JH, Zhang JZ. Trust in Fintech: Risk,

governance, and continuance intention.
The Journal of Computer Information
Systems. 2023;**63**(3):648-662.
DOI: 10.1080/08874417.2022.2093295

[96] Gupta K, Wajid A, Gaur D.
Determinants of continuous intention
to use fintech services: The moderating
role of COVID-19. Journal of Financial
Services Marketing. 2023;**28**(3):567-583.
DOI: 10.1057/s41264-023-00221-z

[97] Saleem A. Fintech revolution,
perceived risks and Fintech
adoption: Evidence from financial
industry of Pakistan. International
Journal of Multidisciplinary and
Current Educational Research.
2021;**3**(1):191-205

[98] Irimia-Diéguez A, Velicia-Martín F,
Aguayo-Camacho M. Predicting FinTech
innovation adoption: The mediator role
of social norms and attitudes. Financial
Innovation. 2023;**9**(1):36. DOI: 10.1186/
s40854-022-00434-6

[99] Hu Z, Ding S, Li S, Chen L, Yang S.
Adoption intention of fintech services
for bank users: An empirical examination
with an extended technology acceptance
model. Symmetry. 2019;**11**:340.
DOI: 10.3390/sym11030340

Chapter 4

Regulating the Future: Global Infrastructure, Compliance, and the Role of Digital Currencies

Andrea Romaoli Garcia

Abstract

This paper explores the intersection of cryptocurrency regulation and Global Infrastructure Initiative (GII), analyzing how emerging regulatory frameworks and transnational cooperation are reshaping the future of ethical digital finance. It examines the evolution of regulatory responses to decentralized technology, including priority topics such as anti-money laundering (AML), know-your-customer (KYC) compliance, and jurisdictional fragmentation. Drawing on connections to GII, the chapter underlines the appeal for interoperable standards, digital sovereignty, and ethical governance in order to facilitate robust financial infrastructures in emerging and developing economies. Focusing particularly on how international PPPs, multi-lateral institutions, and regulatory sandboxes can merge innovation with security, the chapter issues a new paradigm of regulation under the Sixth Dimension of Human Rights and the Principle of Sovereignty of Life. This paradigm embraces cross-border collaboration, technology neutrality, and human rights protection in the digital economy. The discussion also takes into consideration the environment of Central Bank Digital Currencies (CBDCs), digital identity systems, and the ethical basis of algorithmic decision-making in global financial infrastructure design.

Keywords: cryptocurrency regulation and digital sovereignty, Global Infrastructure Initiative, financial inclusion, supranational coordination, ethical fintech and digital economy

1. Introduction

Nowadays, one of the biggest concerns that causes severe consequences for financial institutions relates to organized crime acting through cybersecurity and money laundering. On the one hand, it can lead to economic instability, corruption, and erosion of public trust in institutions from a societal perspective. On the other hand, financial institutions can be impacted by reputational damage, robust fines, and even criminal charges. A moral decline can be raised as a general result when financial crime is unchecked because it would encourage more people to engage in similar activities, leading to a societal breakdown.

Those are consequences from criminal organizations using change of value to perform crimes, or related to cybercrime when they use technological resources to perform these crimes. It means that dollars, euros, yen, reals, any other coin, and also cryptocurrency can be used by organized crime as instruments to perform crimes. While coins are designed to deliver value to society and increase human dignity, organized organizations will also use them regardless of the species of coin.

The emergence of cryptocurrencies brought complexity in global finance and stressed conventional regulatory regimes and raising existential concerns about the nature of monetary sovereignty, compliance, and systemic stability. On one hand, decentralized technologies facilitate new modes of value transmission beyond the control of established financial intermediaries; on the other hand, they also expose fundamental regulatory blind spots, particularly in the areas of anti-money laundering (AML), know-your-customer (KYC) practices, and cross-border enforcement. These disruptions go beyond physical territories as well, and they point to the imperative of an internationally coordinated task force to ensure that digital finance innovation proceeds by ensuring legal, ethical, or economic safeguards.

The disruption led to the sensitive demand for strong, inclusive, and interoperable digital financial infrastructure due to current regulatory approaches remaining largely reactive and jurisdictionally fragmented, frustrating the development of consistent policies that could underpin both innovation and systemic stability. In these conditions, the definition of a shared global infrastructure capable of mapping new financial technologies onto shared principles of governance has become an urgent priority. This is particularly applicable in a world where digital finance is ever more intersecting with development goals, cybersecurity concerns, and evolving concepts of digital sovereignty.

This chapter approaches the Global Infrastructure Initiative (GII) as a crucial framework for examining the intersection of digital currency regulation and transnational financial infrastructure. Also considering the critical engagement with the role of public-private partnerships, multilateral institutions, and regulatory sandboxes, it is expected that the discussion may be able to identify pathways toward a regulatory paradigm that embraces cross-border coherence, technological neutrality, and fundamental rights protections. In doing so, this chapter contributes to advocating for regulatory designs that are anticipatory rather than reactive and that align with the ethical and operational demands of a digitized global economy.

The Global Infrastructure Initiative (GII) is a community of senior leaders focused on promoting sustainable, inclusive, and future-ready infrastructure in which the United Nations (UN) plays a significant role. The GII acts primarily through the UN Sustainable Development Goals (SDG) and different strategic initiatives aimed at bridging the global infrastructure gap and scaling innovation, facilitating relationships, and mobilizing change to advance infrastructure as a catalyst for growth.

Furthermore, senior leaders and UN leaders emphasize that financial institutions and financial instruments are crucial to promote financing for development that will increase infrastructure investment to achieve the SDG.

Thus, while there is no assertive crypto regulation with the power to build a strong and direct relationship with the Global Infrastructure Initiative, it cannot be denied that synergy is a realistic possibility. The purpose and relevance of exploring the connection are in the shared goal of encouraging innovation to meet global infrastructure needs within a more effective and inclusive path toward development of infrastructure and a better citizenship relationship. However, filling the gaps in risk, regulation, and basic philosophy will require a joint effort by policymakers, banks, and the

technological sector for building a regulatory infrastructure with the potential to support both the physical world's solid foundations and the digital infrastructure of the new financial frontier.

The notion of connecting the Global Infrastructure Initiative (GII) with the turbulent world of cryptocurrency regulation presents an interesting and complex frontier in the creation of innovative sources of infrastructure financing, in which underlying blockchain technology alongside cryptocurrencies remains in the initial stage as a help to bridge the multi-trillion-dollar global infrastructure gap.

The critical point lies in significant discrepancies in their core philosophies and operational realities that prevent a seamless integration.

This chapter aims to discuss crucial issues and opportunities in blockchain and cryptocurrency integration in the financing of the Global Infrastructure Initiative (GII).

2. The evolving landscape of cryptocurrency regulation

As cryptocurrencies transition from the edge of financial creativity toward the heart of global financial systems, different regulatory responses have come up by jurisdiction and reflect a broad array of philosophical, political, and economic agendas. What has been noted is that while some countries have embraced digital asset innovation, others have responded with tough restrictions and even prohibitions. This has resulted in a mosaic of regulations that reflects both the geopolitical agendas and technological ambitions of the twenty-first century.

These are policy gaps identified:

Lack of universal legal definitions, such as the Decentralized Autonomous Organization (DAO), stablecoin, and tokenized assets.

Absence of a binding international convention or regulatory treaty.

Minimal ethical and sustainability integration in existing frameworks.

Inconsistent treatment of cross-border crypto activity, such as taxation and consumer protection.

Regarding the international scenario, despite there being multilateral efforts and forums seeking to solve this regulatory mosaic that aim to coordinate regulatory approaches and address cross-border risks, at present, no single binding international convention or global council has authority over the regulation of cryptocurrencies.

In this regard, in 2023, the International Organization of Securities Commissions (IOSCO), which acts in the securities regulations and guidance, including crypto-asset markets, released a comprehensive policy recommendation framework for crypto-asset service providers. However, there are non-binding guidelines, and enforcement depends on domestic regulators.

Also, the Bank for International Settlements (BIS), which leads the Innovation Hub and the Basel Committee on Bank Supervision on policy frameworks for Central Bank Digital Currencies (CBDCs), seeks to establish financial stability and banking exposure to crypto with less focus on retail or decentralized finance (DeFi).

In 2023, the G20 and Financial Stability Board (FSB) emerged as a strong leader in crypto regulation by endorsing the FSB's recommendations to create a global regulatory baseline that is in progress by 2025 (the year that this book is published) and is still non-binding with no enforcement mechanism.

Some specialized UN bodies are discussing ethical frameworks and sustainable development considerations, and the United Nations Office on Drugs and Crime (UNODC) and the United Nations Interregional Crime and Justice Research

Institute (UNICRI) are focused on the use of crypto in crime and digital justice frameworks and are discussing ethical frameworks and sustainable development considerations. However, UNODC and UNICRI are not yet a coordinated financial regulation authority.

Given the current fragmented scenario, it would make sense to fill all gaps through harmonization or at least to align global crypto regulation. I would suggest establishing a UN-led International Convention on Digital Assets that could follow the same model adopted by the United Nations Commission on International Trade Law (UNCITRAL) by creating baseline legal definitions, such as digital asset and stablecoin, as well as harmonizing principles of consumer protection, compliance, and jurisdiction.

With global consensus, establishing a UN-led International Convention on Digital Assets would define the UN's inclusive representation and legitimacy with a function to serve as a soft-law governance forum and to develop a "Global Crypto Taxonomy Classification System" with working groups. Also, as proposed solution, to accelerate adoption, would be created a "Multilateral Crypto Governance Body" as a council that could follow similar model adopted by the Intergovernmental Panel on Climate Change (IPCC) or Internet Governance Forum (IGF) with benefits for tokenization assets, cross-border taxation and privacy and security through a strong community of experts and interested beneficiaries: Governments, private sector, academia, civil society and technologists.

This proposition would prevent regulatory arbitrage by ensuring that what is recognized as a security in one jurisdiction is recognized consistently such as already happens with Carbon Credits.

This model that I suggest here would be covered with trust, integrity and accountability if embed Ethical and Sustainable Principles that combines the Sixth Dimension of Human Rights with blockchain protocols which the Principle of Sovereignty of Life would be a foundation to establish a binding regulation within national regulatory actions as a solid wall to protect all form of life in the planet of the use of cryptocurrency to perpetrate crimes even using authorized or registered titles. The Sixth Dimension of Human Rights through the Principle of Sovereignty of Life will align regulation with human rights, ethics, and sustainability that will appeal to both governments and public-interest stakeholders.

2.1 Major regulatory approaches

Regarding current regulatory validation, in 2025, a new Markets in Crypto-Assets (MICA) regulation came into force to provide resources to develop digital markets throughout the 27-nation bloc. After that, the European Union (EU) was hit by concerns about the potential to undermine MICA's goals regarding the speed with which licenses are being granted by member states [1].

In the same line, the United States has adopted a fragmented, sector-based regulatory model alongside the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Financial Crimes Enforcement Network (FinCEN), expecting to bring more integrity and transparency to digital asset markets that resulted in legal uncertainty to the ecosystem.

China accelerates its pilot testing of CBDC began in 2021, and it is expected to expand digital yuan globally and create a Shanghai operations center, given that the People's Bank of China (PBOC), led by Governor Pan Gongsheng, called for a multi-polar global currency system and financial regulators have been collaborating with the pledge to establish a stable yuan [2].

Conversely, in September 2021, El Salvador became the first country in the world to adopt Bitcoin as a legal tender to increase financial inclusion, remittance effectiveness, and private investments using emerging technologies. The global community acted, however, with macroeconomic stability issues within the international financial institutions, consumer protection concerns, and compliance with global AML standards. Thus, in retaliation, the International Monetary Fund (IMF) insisted, as a condition of approving, the implementation of a new \$1.4 billion aid program given by El Salvador. In brief, in January 2025, El Salvador changed its mind, and it ended: legal tender status was abandoned.

Canada recognizes cryptocurrency through platforms as money services businesses (MSBs) with a tough regulatory framework to prevent money laundering and financing terrorism under the laws: Proceeds of Crime (money laundering), Terrorist Financing Act (PCMLTFA) and a sandbox on blockchain infrastructure (FINTRAC). The FINTRAC is Canada's financial intelligence unit (FIU) that plans a variety of new and changing obligations for businesses against money laundering and anti-terrorist financing, with tough sanctions by the end of 2025 [3].

The presented regulatory approach demonstrates that even though it has a fragmented regulatory scenario that provokes uncertainty in the digital identity integration with cryptocurrencies, the development is gradual and fragile, converging toward a safety for interoperability, common definitions, and market operation.

Enforcing cryptocurrency regulation poses unique challenges and cross-border collaboration, yet it remains struggling against heavy penalties resulting from the lack of adequate tax classification and increasing risk from the lack of certainty in the market operation with cryptocurrency.

In this sense, into my book-chapter published in 2019, I discussed about risk coming from jurisdictional uncertainty and patchwork in the cryptocurrency regulatory framework as much as I proposed an end-to-end legal foundation to form a proper scheme of taxation in digital markets with cryptocurrency that would avoid this patchwork also I detailed about impossibility of harness legal framework that is applied to traditional financial institutions only with changes or additions to address complex topics on crypto-assets and its conflicts with securities, commodities, institutional jurisdictions and conducts toward decentralized finance (DeFi).

2.2 Fragmentation vs. convergence: The global regulatory patchwork

The presented regulatory approach demonstrates that even though it has a fragmented regulatory scenario that provokes uncertainty in the digital identity integration with cryptocurrencies, the development is gradual and fragile, converging toward a safety for interoperability, common definitions and market operation.

Geopolitics affects the enforcement of cryptocurrency regulation due to some jurisdictions having a strong presence of criminal activities that force authorities to keep eagle eyes on financial transactions in order to avoid feeding terrorism through laundering money. The future will show a balance between cybersecurity, reliable algorithms, and digital sovereignty over blockchain anonymity. This future depends on a peaceful world as a perfect ecosystem to promote diplomacy among global leaders that should seek true solutions that will separate trustful citizens and criminals without bringing poverty to citizens.

The current diplomacy solves cybersecurity risks by imposing tough rules on trustful citizens, which is one of the causes of poverty. It is a lazy diplomacy that

makes profitable work non-affordable due to high costs with taxation that is imposed as a solution to establish national security.

In this sense, into my book-chapter published in 2019, I discussed about risk coming from jurisdictional uncertainty and patchwork in the cryptocurrency regulatory framework as much as I proposed an end-to-end legal foundation to form a proper scheme of taxation in digital markets with cryptocurrency that would avoid this patchwork also I detailed about impossibility of harness legal framework that is applied to traditional financial institutions only with changes or additions to address complex topics on crypto-assets and its conflicts with securities, commodities, institutional jurisdictions and conducts toward decentralized finance (DeFi) [4].

In sum, the conclusion in that book revolves around gray zones and just affirms that it remains up to the present, given the lazy activity of regulatory bodies. In fact, in digital finance, using cryptocurrency is complex and harnessing the existing legal framework causes a “Juridical Frankenstein,” that is to say, a clumsy creature tripping that scares us.

3. Ethics, compliance, and digital trust in a borderless economy

As global financial systems increasingly integrate decentralized technologies, the sense extracted from existing fragmentation and the necessity of convergence that forms a current global regulatory patchwork brings confirmation of compliance and fosters digital trust that has become a critical priority that remains fraught with legal, technical, and ethical complexity. Legitimacy, enforceability, and inclusion imply values circulation as a match for geography issues at a paradox for a borderless digital economy in which demands for transparency coexist with risks of exceeding limits, and it is expected that compliance frameworks may strengthen market integrity but also deepen global inequalities.

Thus, it is a question that would arise from this paradox:

Why do compliance frameworks in cryptocurrency strengthen and deepen global inequalities?

While compliance frameworks for cryptocurrency are often introduced with the aim of consumer protection, financial stability, and combating illicit activities, there are strong arguments and emerging concerns that they could inadvertently strengthen and deepen global inequalities.

Among reasons, is the increased barriers to entry and financial exclusion caused by know-your-customer (KYC) and anti-money laundering (AML) that prevents financial crime and financing terrorism but can be significant hurdles for individuals in developing countries or marginalized communities due to many people in these regions may lack official identification documents, proof of address, or access to traditional banking services that are often required for KYC/AML compliance. As a consequence, these individuals will be excluded from participating in regulated crypto markets and their financial inclusion opportunities.

Alongside KYC and AML barriers are joined technological and infrastructural gaps, whose advanced devices and digital literacy may not be available for every person, and adding to network coverage with slow speeds and less access to technology will increase the digital divide.

Also, implementing and maintaining compliance measures can be expensive for smaller crypto businesses as well as repress innovation, resulting in a centralization and concentration of wealth and power because it favors larger, well-funded

cryptocurrency companies and institutional investors who have resources to hire legal teams, develop sophisticated compliance systems, and success complex regulations.

3.1 Risks of overregulation and financial exclusion for GII in the cryptocurrency terrain

Regulatory arbitrage can arise from inconsistent regulatory environments globally, where crypto international operations can be relocated to jurisdictions with less rigorous rules as a solution to avoid stricter oversight. The paradox is expanded because those without such options are left where they will be limited and more heavily regulated choices.

As an example of this ecosystem, the Global North nations are predominantly leading discussions and shaping international crypto regulations, while the Global South nations are developing nations that can be placed at a disadvantage insofar as being in limited representation in policy-making.

In this perspective, this instability of regulation assumes particular significance when framed within the context of the Global Infrastructure Initiative (GII). As a regime that seeks to catalyze cross-border collaboration and long-term infrastructure investment, the GII can be an essential facilitator of inclusive digitalization. Yet when decisions regarding financial and technological infrastructure are made in a manner that fails to adequately take into account divergences in regulatory power and access, the result may be a bifunctional digital economy. Those nations in the Global South, with minimal institutional capacity to build adaptive regulatory systems or to negotiate on equal terms in multilateral negotiations, may be locked out of the cycles of financial innovation fueled by blockchain and cryptocurrency systems. This regulatory gap, if not bridged, can make the promise of digital inclusion into a tool of additional exclusion.

As supposed, the overregulation of virtual currencies in the infrastructure frameworks promoted by the GII can, by default, debase one of its very fundamental goals: economic development through stable, open systems rendering economic benefits available to offer human security. In case of a thorough imposition of regulatory guidelines modeled primarily on Global North priorities, such as strict mechanisms of identity authentication, without localization to diverse national contexts, the GII would be perpetuating system barriers rather than eliminating them. For instance, strict AML/KYC conditions linked to infrastructure financing or fintech evolution can disproportionately weigh on the unregistered, disqualifying millions in Latin America's informal economies, Sub-Saharan Africa, or Southeast Asia.

In this regard, decentralized financial technologies and cryptocurrency have the possibility to both be a challenge and an opportunity for the GII. In case of suitable integration into global infrastructure schemes, and with regulatory climates proportional to, interoperable with, and reactive to local contexts, these technologies would enable financial autonomy, invite trust through decentralized identity platforms, and enable cross-border economic interaction. But if these innovations are met with blanket bans or plastered institutions, they risk becoming just another fault line in the geography of global development. An open GII to digital finance could also be open to pluralism of regulation, so that financial infrastructure is not only linked internationally, but also ethically and justly governed.

Although cryptocurrency and blockchain are often mentioned in the context of infrastructure, it is stressed that they are not directly integrated into the GII framework since the G7-led initiative adopted traditional infrastructure development

through established financial mechanisms in reason of transparency and efficiency, showing that public and private investments within the cryptocurrency ecosystem are not ready or adequate for massive adoption.

However, an important path has been trilled through BRICS nations: Brazil, Russia, India, China, and South Africa to develop a blockchain for crypto-payments to facilitate international transactions using digital versions of national currencies, although adoption will yet depend on a robust and supportive innovation ecosystem, a factor directly measured by the GII [5].

3.2 Concerns on digital identity frameworks into decentralized compliance systems

The fragmentation of democratic nations would benefit authoritarian interests due to geopolitics having relevant consequences for the decision-making process in the data governance models. In general, norms and national sovereignty are not obstacles to trade and transferring data, but this landscape is changing once the *Sixth Dimension of Human Rights* considers data as political and meaningful instruments to states as a matter of security, accountability, and transparency for reaching inclusive and equal societies [6].

It remains an evolutive scenario as much as it could lead to the development of robust digital identity standards whose goal is to define how individuals and entities would be authenticated and authorized in the digital scope, also seeking to ensure security, privacy, and ethical and trustworthy interactions. These frameworks are essential to achieving data sovereignty and citizen empowerment.

Moreover, only with an alliance of democratic states would there be a constructive impact for digital governance in law and the judiciary system for prioritizing privacy, security, and ethics in digital governance without creating islands of national rules that would not cooperate with international field demands.

In order to harness technological benefits as well as strengthen democratic and ethical digital governance, democratic governments should examine its multilateral institutions and their capacity in building consensus as well as to support each other to build a consensus capable to achieve *Principle of Sovereignty of Life* toward to materialize human-centric values such as inclusive societies, participative engagement, transparency and innovation through harmony with people into fairly and equally policies and practices.

This necessitates the collaborative development of interoperable digital identity frameworks that prioritize individual control and privacy, rather than top-down, nationally siloed systems.

The question that remains in the Sixth Dimension of Human Rights regarding digital sovereignty and life's sovereignty is: *Would vulnerable people and companies be disadvantaged by national ambitions to impose rules as international standards, especially when these rules dictate centralized and exclusionary digital identity mechanisms?*

This question fits the social and ethical concerns because there is a trendiness on building USA-EU blocks in terms of managing technology and digital economy that could become a conflicting and discriminatory rules as well as it would not solve conflicts of regulation notably when technology converge societal establishing new challenges related to security versus protection of life by considering “to live” and “human security” as sovereignty right of all citizens.

It brings us a new question: *Which would be the most important right to sovereignty: the right to sovereignty to protect interests of rulers or the right to sovereignty to protect the lives of citizens?*

From a macro-perspective, all war events across the world in 2024–2025 show that the leader's interests are more in sovereignty than citizens' lives as sovereignty rights. This would be observed in the armed conflict between Israel and Hamas-led Palestinian militant groups that has been taking place chiefly in the Gaza Strip since 7 October 2023, where among the hostages were babies, and leaders from all countries were discussing war strategies while hostages were waiting for rescue.

Antagonistically, the scope that was sought by the leaders is different from those scopes intended by the Principle of Sovereignty, *which aims to protect territorial integrity as a second goal, while protecting life dignity and security is a primary goal because territorial integrity is an instrument to materialize life dignity and security. The Principle of Sovereignty surpasses physical geography in order to achieve the Principle of Sovereignty of Life in a Sixth Dimension of Human Rights approach, where the responsibility to protect comes as an estate's duty toward control over territory, in order to allow a state to manage its resources for the benefit of its population.*

Obviously, this conceptual paper does not intend to exhaust this discussion, but it intends to put a spotlight on current gray zones that are an obstacle to an adequate approach in order to eliminate discrepancies and fill gaps in the regulatory field. Crucially, these gaps often arise from outdated approaches to digital identity and compliance. Our vision proposes leveraging cryptocurrency grounded in principles of privacy, portability, and user agency, to embed more options for societal converging economic and employment into tangible UN Sustainable Development Goals.

In this sense, this will force us to create principles that give protection to all forms of life through a sustainable, strong, and healthy planet, together with machines and technology.

A truly powerful vision unites the cryptocurrency under principles of privacy, portability, and user agency in accordance with the *Principle of Sovereignty*, *Principle*

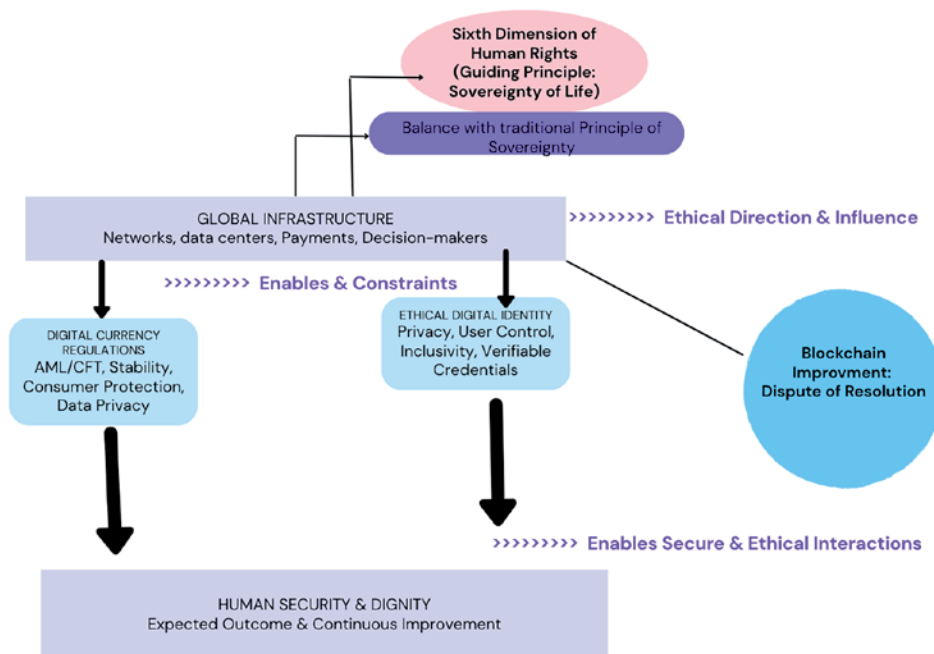


Figure 1.
 Global Regulation and Ethical Standards—Infrastructure and Cryptocurrency.

of *Sovereignty of Life*, and *democratic rights* because it adds a new scope to digital governance that sees cryptocurrency not merely as a digital asset, but more as a foundation technology that bears privacy, portability, and user agency. Thus, when it is combined with novel digital identity frameworks will deliver a powerful mechanism in which users will be allowed to keep more control over their own information and how it will be used for checks.

Also, it creates a philosophy to reshape democratic regimes that provide access to more opportunities through an economic activity free of censorship. In this sense, it is expected that individuals with open access to their transactions and assets without intermediaries or centralized and private digital currencies will live in a more level and robust world, shifting power dynamics and enhancing individual freedoms in deep ways (**Figure 1**).

Case study—India's Aadhaar project

India's Aadhaar project, with over 1.3 billion people using it in India, represents one of the world's sophisticated and largest biometric ID systems, where 99.9% of adult Indian residents possess Aadhaar IDs (2023).

Overview

By 2010, 40% of India's population did not have a birth certificate, and 60% did not have access to bank accounts.

The Aadhaar project was launched in 2012 as an initiative to benefit government programs and welfare assistance, which the UIDAI provides each Indian resident with a unique identification number, and to eliminate duplicate, fake, or stolen IDs (irrespective of age and gender).

Each Indian resident provides the Aadhaar system with basic demographic information such as name, date of birth, age, address, and gender. Also collected biometric information in person with fingerprints, two eyeball scans, and facial photographs.

After UIDAI makes checks, the concluded applications are encrypted.

Achievements

The system reduced duplicate enrollments in social welfare programs and opened more economic opportunities to Indian residents.

Concerns

The Aadhaar system allows private and public entities to access individual data stored in the Aadhaar files, such as telecom companies, banks, schools, and hospitals. Thus, it is easier to link up the behavior of Aadhaar users with communications, finance, education, health, and everything else.

Also, the system showed security concerns. One newspaper in the city of Jalandhar reported that for 500 rupees, a reporter accessed the Aadhaar database through an anonymous seller on WhatsApp.

Also, a government official posted his Aadhaar number on Twitter, challenging hackers to "do any harm." Hackers back with his cell numbers, address, and date of birth. They also claimed to have deposited a single symbolic rupee in the official's bank account, according to the Times of India.

Clearly, the system has issues with security and privacy.

These events opened international discussions around the following questions.

- Who is the owner of the data collected from Indian residents by the Aadhaar system? Government or user?
- Would the Aadhaar system have violated privacy, considering the simple fact that someone who was born and exists would have an obligation to provide a full digital profile?
- Would the Aadhaar system be secure from hacking?
- Would public or private entities be abusive in collecting a full digital profile?

Key-challenges

India's government must find a balance between recording full digital profiles of people with democracy, the benefits of Aadhaar, as well as its limits on privacy and security.

Source

<https://www.forbes.com/sites/tylerroush/2023/11/02/what-is-aadhaar-indias-id-system-sam-altman-is-reportedly-modeling-his-eye-scanning-crypto-project-worldcoin-after/>

<https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized>

The current implementation of anti-money laundering (AML) and know-your-customer (KYC) policies, while aimed at stopping illicit finance, has the unintended effect of being a significant cause of economic censorship. This mechanism involves high costs with compliance that unbalances small businesses and individuals' budget management.

In consequence, these tough criteria tend to expel legitimate players, not because of criminality, but because they have socioeconomic drawbacks or are missing filling bureaucratic requirements of documentation. Obviously, this exclusion is particularly harmful in the case of debtors because it is a censor on users seeking to communicate with policies that open financial tools needed to manage and repay their debt, locking them in a cycle of marginalization.

Regarding Aadhaar case, at the heart of the legal challenge was the concern that the 12 digit unique identity number related to linked to individuals biometric and demographic data would bring forefront critical questions surrounding data privacy and sovereignty and it could lead to pervasive surveillance and infringe upon the fundamental right to privacy as recognized by the Indian Supreme Court in *Puttaswamy v. Union of India* (2017).

The Court upheld the constitutional validity of Aadhaar in 2018 but imposed restrictions to safeguard against data misuse, emphasizing that the data collection must respect individual autonomy and ensure that the sovereignty of citizens over their personal information is not compromised by the state's technological reach.

This case highlights the tension between national governance objectives and the ethical imperative of protecting individuals' rights.

This regime, coincidentally, is also less efficient against sophisticated criminal groups, who often will be able to find means of circumventing such hurdles anyway, and prejudice the neediest thereby. Blockchain tech and cryptocurrencies offer the hope of a solution in terms of cheaper, more accessible money conduits for the unbanked and underbanked. The existing AML/KYC regime is therefore in need of intensive re-examination. Its unintended consequence of keeping wide groups of the public out of economic participation violates fundamental human rights and moral standards of online regulation, turning what should be a safeguard into an impediment to inclusion and opportunity.

4. Global Infrastructure Initiative into perspective of digital assets

The growing population raises the need to expand the infrastructure, requiring urgent government funding to open opportunities, promote economic growth, and improvements in the livelihoods of people. Climate change, geopolitical issues, and national interests versus international interests are issues that push countries' investments to build smart infrastructure that supports inclusive and sustainable growth.

To understand how infrastructure is deployed on a global scale Global Infrastructure Initiative (GII) is necessary to have an overview of the Transnational Infrastructure Projects (TIP) [7].

Regarding definition, the Transnational Infrastructure Projects are large-scale development initiatives that encompass multiple countries working through regional collaboration in order to design a strategic project in order to enhance connectivity, trade, transportation, sustainability, economic integration/growth across borders, and strengthen diplomatic ties and political relations.

In brief, The Transnational Infrastructure Projects are multidisciplinary approach that aims to support the Sustainable Development Goals within various

goals, particularly those related to infrastructure, such as “Industry, Innovation and Infrastructure” (Goal 9); “Sustainable Cities; Communities” (Goal 11) and “Climate Action” (Goal 13), and through an infrastructure development at smart, sustainable, inclusive and resilient initiative by covering:

- *Social impact*: it seeks to enhance living conditions, promote economic growth, and ensure access to basic services.
- *Strategic planning*: through a collaborative and strategic planning that embraces environmental, social, and economic aspects for the benefit population.
- *Global partnerships*: Transnational Infrastructure Projects aims to create partnerships with governments, the private sector, civil society, and international organizations to mobilize resources and expertise for infrastructure development.

Considering high costs to deploy infrastructure, it is beyond what governments could fund on their own; once they were to spend *4.5% of GDP*, that means *\$1.5 trillion annually*. At that point, by joint efforts, this mission can be fostered. In terms of global advancement, countries are working through Transnational Infrastructure Projects due to their expanding capacities and gathering stakeholders, local communities, international organizations, and the private sector [8].

While TIP regards specific cross-border projects among multiple countries, GII are broader initiatives toward improving infrastructure on a global scale. Its origins rely on the G20, particularly following the 2014 Brisbane Summit, where leaders recognized the critical need for increased and improved infrastructure investment worldwide.

On one hand, TIP considers regional needs that require international cooperation to expand capacity on human and financial resources for transportation, energy systems, water management, etc. On the other hand, GII includes policy frameworks and funding strategic planning, as well as relating to different transnational projects working through collaborative strategies among countries, international organizations, and the private sector to maximize infrastructure development worldwide.

In short, GII goes beyond TIP due to a global infrastructure that responds to a wider set of green, resilient, inclusive development through partnerships by global elder leaders.

The core aims of the GII are multifaceted:

- *Mobilization of private capital*: One core aim is to mobilize more private sector capital into infrastructure projects, as public funding cannot meet global needs alone. This has been the consistent view of the infrastructure trends observed.
- *Strengthening project preparation*: The GII will improve the bankability and quality of infrastructure projects by promoting best practices in planning, design, and feasibility studies.
- *Knowledge sharing and capacity building*: It will share knowledge and build capacity at the country level to develop and execute high-quality infrastructure.
- *Policy and regulatory reform*: The initiative urges governments to establish reforms that create a more attractive and more predictable investment environment for infrastructure.

- *Promoting sustainable infrastructure*: Increasingly, the GII claims attention to the development of infrastructure that is environmentally sustainable, socially responsible, and economically sound in the long term.

4.1 Blockchain, tokenization, and cryptocurrency for infrastructure transparency, anti-corruption, and public procurement tracking

Blockchain technology has huge potential to revolutionize the infrastructure sector by combating corruption, lack of transparency, and inefficient public procurement processes. Blockchain's immutable, decentralized, and open ledger system gives it unique strengths: greater transparency, anti-corruption, efficient public procurement monitoring, and supply chain integrity.

Transparency will be enhanced by each deal and decision recorded to a blockchain, being rich in details such as tagging available to all authorized players. In infrastructure projects, this can mean an open book of fund sources, contracts awarded, material purchases, and project milestones and making it difficult to conceal irregularities.

Also, blockchain ensures compliance with the AML, Due Diligence, and KYC for anti-corruption because blockchain transactions are irrevocable, and it confers barriers against corruption and erasing data entered that contributes to reducing channels for bribes, kickbacks, and fake claims throughout the life cycle of the project. In addition, automatic payments performed by smart contracts as self-executing contracts encoded on the blockchain will result in verifiable delivery completion, minimizing human intervention and corruption further.

In this manner, a reduction in conflicts that would require mediation or legal intervention. The audits could enjoy an increase in efficiency as records of public procurement can be traced back, which ensures secure data related to the capacity of blockchain generates an audit trail for the entire procurement process: from initial release on the tender toward bid submission, assessment, and awarding of contracts. It will result in an unquestionable record for all participants involved, as well as reducing events surrounding conflict resolutions, or at least, settling disputes more easily by providing unequivocal, verifiable proof.

Public-private partnerships (PPPs) are a significant means of funding and delivering large-scale infrastructure projects such as GII, combining the public sector's need for infrastructure with the private sector's efficiency and funds. Tokenization of infrastructure assets is an efficient digital asset innovation with the potential to reveal new sources of funding and management of PPPs [9].

The PPP model helps to diffuse risk, access private sector expertise, and often produces projects ahead of schedule. However, PPPs might be complicated, illiquid investments, and access to capital can become a problem, particularly for individual investors.

In this regard, tokenization appears among solutions as it involves representing real-world assets, such as a share in an infrastructure project's revenue stream or equity, as digital tokens on a blockchain. These tokens are fractionalized, meaning an asset can be divided into many smaller, tradable units.

It results in enhanced liquidity and enhanced capacity for fundraising. Tokenization transforms illiquid infrastructure investments into liquid tradable digital tokens. Investors can buy and sell fractional ownership of projects in secondary markets, bringing these opportunities to more investors, including retail investors, who might have otherwise been excluded because they might not have been able to

satisfy high entry barriers. By lowering the minimum level of investment and injecting more liquidity, tokenization can potentially increase the investor base for PPPs a great deal. This can attract more private capital, potentially reducing reliance on conventional debt and offering more flexible funding terms.

In addition, the smaller costs of documentation promote democratization of investment as tokenization enables smaller investors to participate in large-scale infrastructure projects, fostering greater public engagement and potential shared benefits from these critical assets.

There is also wider access to funds globally as digital tokens are freely tradable across borders, and infrastructure projects can get access to a global pool of funds more effectively, without geographical limitations typically associated with traditional investment tools.

Therefore, in a conceptual manner, the alignment of PPPs and tokenization is a potential path to more efficient, open, and accessible investment in GII, obliterating the perennial funding gap and catalyzing sustainable development.

Besides, the use of cryptocurrency in the framework of blockchain systems brings about a traceable, efficient, and programmable system of value transfer. Stable cryptocurrencies or tokenized national currencies can be used to make payments, thereby enabling real-time settlement as well as preventing delays or leakages associated with traditional financial systems. It also leads to transparency for every unit of value transferred through the procurement and project delivery phases.

Also, tokenized infrastructure assets can be programmed to pay dividends or returns in cryptocurrency, ensuring efficient, borderless, and near-instant payments to investors. This is yet another attraction for foreign investors and adds to the financial inclusiveness of PPP programs. In nations with limited banking facilities or capital controls, cryptocurrency can also ensure smooth participation in infrastructure financing.

In this manner, cryptocurrency wallets can be linked directly to tokenized infrastructure platforms, allowing micro-investors from around the world to contribute using digital currencies. This lowers participation barriers, bypasses traditional intermediaries, and fosters greater global engagement in infrastructure development.

The risk of criminal activities are managed because compliance requirements are also addressed, at consideration that sophisticated cryptocurrency environments are able to encode robust identity validation to allow KY, AML and Due Diligence aligned with forensic features to ensure that every cryptocurrency transaction in infrastructure environments satisfies worldwide regulatory standards, and also complemented by blockchain analytics and chain-tracing resources to establish integrity and auditability of funds.

Global Infrastructure Initiative (GII) has demonstrated great efforts in the deployment of transport, clean energy, health, sanitation, clean water, education, housing, safe food, and economic gains to all countries at vulnerabilities to deliver a dignified and safe life to people. Among these efforts, GII has designed PPP models through DeFi to accelerate development.

For instance, *MCB Ventures Holding joined forces with CHN Xinkong Investment Development Co., a subsidiary of China Energy, to deploy a DeFi fund (a blockchain-based system) for the green energy and carbon sector globally (October 2023)*. This partnership marks an important stride toward clean power. The pioneering project is a pilot solar PV farm in Kinshasa, Democratic Republic of Congo, with an initial capacity of 500 MW and a distributed infrastructure network of 5.4 GW. CHN Energy is responsible for investment and management by providing substantial investment

capital (up to \$7 billion) to RWA projects. MCB is responsible for the construction of the Decentralized Physical Infrastructure Networks (DePIN) and technical iPPA models. DePIN relates to networks that leverage blockchain technology and cryptocurrency to build and maintain physical infrastructure in a decentralized design [10].

This model of DeFi into PPP represents a unified DAO focused on democratizing the responsibilities of real-world assets. *This project will leverage cutting-edge IoT and chipset technology to ensure comprehensive traceability governance*, aiming to maximize financial returns through strategic location and innovative EPC implementation.

When cryptocurrencies are combined with blockchain, smart contracts, and tokenization, they serve not only as a model of exchange but as programmable, transparent, and auditable tools with the potential to enhance GII finance mechanisms, governance, and execution. Thus, it makes sense to expect profound innovations in how infrastructure is built, monitored, and financed in the digital age.

5. Expression of AI algorithm in financial mechanism with cryptocurrency

Currently, artificial intelligence (AI) has changed the mechanism dynamics of traditional financial systems with algorithm oversight, and is also making decision-making autonomous in fraud detection, risk analysis, and compliance reporting, which also allows banks to use AI for real-time tracking transactions with KYC policies and preventing systemic risks.

However, the transparency of AI decisions and the data concentration give rise to ethical concerns of bias, discrimination, and unrestrained surveillance, all in an environment of regulation too often poorly timed after advances in technology.

In 2019, Apple was investigated by US regulators as a sexist program when its AI-driven credit card system, managed by Goldman Sachs, offered significantly lower credit limits to women compared to men with the same financial profiles. This investigation exposed the risk of gender bias in AI systems [11].

Conversely, cryptocurrency environments introduce decentralized finance (DeFi) platforms that employ AI in a more distributed mechanism. Algorithmic trading bots and smart contracts operate independently of traditional intermediaries, so clients can access financial services by receiving an independent code. While this reduces friction and makes access available to everyone, it also increases the possibility of market manipulation, organized crime attacks, and regulatory ambiguity since such systems often lie beyond traditional compliance frameworks.

Use of AI on DeFi poses a threat to traditional compliance, particularly where machine-learning-driven algorithms interact with pseudonymous transactions. In banks, where regulatory mandates and hierarchical control are the top priority, decentralized community-governed AI-enabled crypto platforms rely on open-source auditing and community governance, so enforcement of shared standards is harder but potentially more reactive.

Traditional financial institutions are supported by developed legal frameworks and institutional governance that are capable of enforcing responsibility on AI systems. However, community consensus-based cryptocurrency networks that are fueled by autonomous algorithms defy central control, with issues of the application of global standards reconciling compliance with innovation. The outcome is regulatory divergence, whereby traditional systems are held to tight oversight while DeFi is a sandbox of free experimentation.

Thus, the marriage of AI and cryptocurrency presents a tough complexity related to the possibility of open, transparent finance participation or the danger of rogue automation. Finding balance demands reassessing governance models and creating interoperable standards respecting individual autonomy and systemic integrity.

5.1 Ethical deployment of tech in emerging markets and vulnerable communities under the sixth dimension of human rights and the principle of sovereignty of life

Vulnerable populations and emerging economies are guinea pigs for experimental or unregulated technology, including AI-based financial systems. The *Sixth Dimension of Human Rights*, which extends Rousseau's call for liberty to ecological and technological justice, repositions governance under the *Principle of Sovereignty of Life*. This principle insulates the dignity of all life forms and mandates that only ethically defensible, sustainable, and equitable technologies are utilized, especially where people are under systemic injustice.

Thus, it is expected that deployment will follow ethical standards of AI in financial systems as much as it must go beyond risk management, and must also provide digital dignity. Crypto-finance algorithms must be auditable, design-inclusive, and capable of functioning without increasing digital divides. In the Sixth Dimension, both public and private sector stakeholders are subject to legal and ethical duty to make the forces of AI and cryptocurrency serve to empower and not exploit, preserving life in its human, social, and ecological extent as secured and prioritized over profit or data harvesting.

Ethical standards arising from the Sixth Dimension of Human Rights serve as an immediate antidote to the slow speed of regulatory adoption. By embedding the *Principle of Sovereignty of Life* into AI technologies and blockchain technologies, the stakeholders are able to use a sound foundation to advocate for pre-empt harm, establish trust, and catalyze policy harmonization between jurisdictions. Ethics here is neither a brake nor a limitation but a strategic winner and the gift that is positioning ethical tech on a trajectory to becoming the legitimacy and scalability standard in the digital economy.

6. Conclusions

This chapter highlights the complex landscape of cryptocurrency regulation within the broader framework of the Global Infrastructure Initiative (GII), requiring immediate, collective, and multilateral approaches transcending nation-state boundaries.

While current proposals such as the EU's MICA regulation and the United States' sectoral models have encouraged standardization, substantive divergences and regulatory gaps persist, too frequently arrested by jurisdictional uncertainties. Notably, flagship projects like the MCB Ventures Holding cooperation with CHN Xinkong Investment Development Co., a subsidiary of China Energy, demonstrate how DeFi, DePIN, IoT, cryptocurrency, and blockchain technologies can be integrated within the GII under PPP models.

These projects demonstrate the potential of decentralized physical infrastructure networks in promoting sustainable energy development, financial inclusion, and open governance in accordance with ethical values.

The proposed establishment of a UN-governed International Convention on Digital Assets and a Multilateral Crypto Governance Body aims to foster interoperability, ethical regulation, and digital sovereignty to ensure that cryptocurrency innovations serve the cause of the values of human rights, sustainability, and social inclusion. Emphasizing the need for regulation under the Sixth Dimension of Human Rights and the Principle of Sovereignty of Life, this chapter favors a paradigm shift to align technological development with ethical governance to build strong, inclusive, and human-centered financial infrastructures that are able to meet the challenges and opportunities of the digital economy.

Acknowledgements

To my beloved son and daughter-in-law. I know it was not easy living with my frazzled side in the final months of this writing project. *Pedro Henrique*, you have supported me in every possible way. *Taymara Leonardi*, a big thank you for every motivational word and cup of tea.

I love you both and all the joys you have brought to my life.

Acronyms and abbreviations

AI	artificial intelligence
AML	anti-money laundering
BIS	Bank for International Settlements
BRICS	Brazil, Russia, India, China, and South Africa
CBDCs	Central Bank Digital Currencies
CFTC	Commodity Futures Trading Commission
DAO	Decentralized Autonomous Organization
DEFI	decentralized finance
DePIN	Decentralized Physical Infrastructure Networks
EU	European Union
FinCEN	Financial Crimes Enforcement Network
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	financial intelligence unit of Canada
FSB	Financial Stability Board
GDP	gross domestic product
GII	Global Infrastructure Initiative
G7	Group of Seven
G20	Group of Twenty
IGF	Internet Governance Forum
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IPCC	Intergovernmental Panel on Climate Change
KYC	know-your-customer
MICA	Markets in Crypto-Assets
PBOC	People's Bank of China
PCMLTFA	Terrorist Financing Act
PPP	public-private partnership
SDG	Sustainable Development Goals

SEC	Securities and Exchange Commission
TIP	Transnational Infrastructure Projects
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crime

Author details

Andrea Romaoli Garcia^{1,2,3,4,5,6,7}

1 Internet Society, New York, USA

2 International Telecommunication Union (ITU-UN), Geneva, Switzerland

3 International Electrotechnical Commission (IEC), Geneva, Switzerland

4 Standard Council of Canada, Ottawa, Canada

5 Foundation for International Blockchain and Real Estate Expertise (FIBREE—ECOSOC/UN), The Netherlands

6 Foundation for International Blockchain and Real Estate Expertise (FIBREE—ECOSOC/UN), Malta

7 UNODC, Vienna, New York, USA

*Address all correspondence to: andrea.garcia@fibree.org

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Howcroft E, O'Donnell J. Exclusive: Crypto giants set for EU green light amid growing regulatory rift, sources say. Reuters. 2025. Available from: <https://www.reuters.com/sustainability/boards-policy-regulation/crypto-giants-set-eu-green-light-amid-growing-regulatory-rift-sources-say-2025-06-13/> [Accessed: June 19, 2025]
- [2] Tang Z, Zhang Y. China talks up digital yuan in push for a multi-polar currency system. Reuters. 2025. Available from: <https://www.reuters.com/markets/currencies/chinas-central-bank-says-promote-digital-yuan-multi-polar-currency-system-2025-06-18/> [Accessed: June 19, 2025]
- [3] Canada Gov. Financial Consumer Agency of Canada. Crypto Assets. Available from: <https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html> [Accessed: June 19, 2025]
- [4] Garcia AR, Garcia PHR. Cryptocurrencies: The communication inside blockchain technology and the cross-border tax law. *International Journal of Blockchains and Cryptocurrencies (IJBC)*. 2019. ISSN: 2516-6425. eISSN: 2516-6433. Available from: [https://www.inderscienceonline.com/doi/10.1504/IJBC.2019.101850;1\(1\):22-41](https://www.inderscienceonline.com/doi/10.1504/IJBC.2019.101850;1(1):22-41) [Accessed: June 22, 2025]
- [5] Krishnakumar A. What is BRICS Pay and why does it matter? *Cointelegraph*. 2024. Available from: <https://cointelegraph.com/explained/what-is-brics-pay-and-why-does-it-matter> [Accessed: June 22, 2025]
- [6] EU Atlantic Council. Report: Digital Sovereignty in Practice—The EU's Push to Shape the New Global Economy. 2022. Available from: <https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-in-practice-the-eus-push-to-shape-the-new-global-economy/> [Accessed: June 22, 2025]
- [7] McKinsey. Report. Global Infrastructure Initiative: Accelerating Progress on Future-Ready Infrastructure. 2024. Available from: <https://www.mckinsey.com/~media/mckinsey/business%20functions/operations/our%20insights/gii/voices/voi%20accelerating%20progress%20on%20future%20ready%20infrastructure/accelerating-progress-on-future-ready-infrastructure.pdf> [Accessed: June 22, 2025]
- [8] World Bank Group. Infrastructure. 2024. Available from: <https://www.worldbank.org/en/topic/infrastructure/overview#2> [Accessed: June 22, 2025]
- [9] PPIAF. Global Infrastructure Hub Report. Managing PPP Contracts After Financial Close: Practical Guidance for Governments Managing PPP Contracts, Informed by Real-Life Project Data. Sydney, Australia: Global Infrastructure Hub Ltd (GI Hub); 2018. ISBN: 978-0-6480762-1-6. Available from: https://content.gihub.org/live/media/1465/updated_full-document_art3_web.pdf [Accessed: June 22, 2025]
- [10] MCB Ventures DAO. MCB Ventures Holdings and China Energy Unite for a Green Power Revolution. 2023. Available from: <https://www.mcbdao.com/mcb-ventures-holdings-and-china-energy-unite-for-a-green-energy-revolution> [Accessed: June 22, 2025]
- [11] Kelion L. Apple's 'sexist' credit card investigated by US regulator. *BBC*. 2019. Available from: <https://www.bbc.com/news/business-50365609> [Accessed: June 22, 2025]

Perspective Chapter: Central Bank Digital Currency and Financial Crime Regulations

Charles Chan

Abstract

This paper provides a comprehensive global analysis of how Central Bank Digital Currencies (CBDCs) influence financial crime, focusing on areas such as money laundering, terrorist financing, fraud, and tax evasion. As countries roll out CBDCs—both retail and wholesale—their technical designs and regulatory frameworks significantly impact their potential to either mitigate or exacerbate financial crime. The paper explores how features like traceability, programmability, privacy levels, and identity verification tiers shape financial integrity outcomes. Case studies from China, Nigeria, the EU, and The Bahamas illustrate diverse approaches to balancing transparency and user privacy. Retail CBDCs, if well-regulated, can limit illicit cash use and enhance monitoring, while wholesale CBDCs reinforce institutional compliance but introduce systemic risks. Risks of cybercrime, identity fraud, and abuse of programmability are discussed, alongside mitigation strategies. The essay also highlights how CBDCs may reduce tax evasion by digitizing transactions and improving auditability. Cross-border interoperability and international regulatory coordination emerge as critical factors for global AML/CFT success. The paper concludes that while CBDCs are not a panacea, they present an unprecedented opportunity to embed financial crime safeguards into the digital infrastructure of money. However, the success of CBDCs in this regard depends on thoughtful design, public trust, robust legal frameworks, and continuous international collaboration.

Keywords: central bank digital currency (CBDC), financial crime, anti-money laundering (AML), counter-terrorist financing (CFT), fraud, tax evasion, cybercrime

1. Introduction

Central Bank Digital Currencies (CBDCs) are digital forms of a nation's sovereign currency, issued and regulated by central banks. As countries pilot or launch CBDCs, questions arise about how they might reshape the landscape of financial crime. Key financial crime areas – anti-money laundering (AML), countering the financing of terrorism (CFT), fraud, and tax evasion – could be mitigated by CBDCs' enhanced transparency or potentially exacerbated by new digital vulnerabilities. This report provides a comprehensive analysis of these issues for both retail and wholesale

CBDCs, examining technical design choices (such as programmability, privacy levels, traceability, and interoperability) and their regulatory implications. A global perspective is included, with examples from leading CBDC initiatives – China’s e-CNY (digital yuan), Nigeria’s eNaira, the prospective Digital Euro, The Bahamas’ Sand Dollar, and others – to illustrate how different designs impact financial crime risks. The aim is to highlight how CBDCs, if carefully designed and governed, can bolster financial integrity while addressing privacy and security concerns [1].

2. Methodology

This chapter employs a qualitative, conceptual approach grounded in thematic analysis. It draws on publicly available policy documents, central bank discussion papers, international standards (e.g., FATF, BIS, and IMF), and academic literature to explore the impact of Central Bank Digital Currencies (CBDCs) on financial crime. A comparative lens is applied through selected case studies—including China’s e-CNY, Nigeria’s eNaira, the EU’s Digital Euro, The Bahamas’ Sand Dollar, and Sweden’s e-krona—to examine how different jurisdictions design and regulate CBDCs in relation to anti-money laundering (AML), counter-terrorist financing (CFT), proliferation financing (PF), fraud, and tax evasion. These cases were chosen for their geographic diversity, varying policy objectives, and maturity in CBDC implementation or piloting.

2.1 CBDCs: Retail vs. wholesale and crime implications

Retail CBDCs are intended for broad public use (individuals and businesses) as digital cash, while wholesale CBDCs are restricted to financial institutions for inter-bank settlement. This distinction matters for financial crime: retail CBDCs introduce a new digital cash-like instrument that could either reduce illicit cash usage or create novel channels for abuse, whereas wholesale CBDCs largely operate within existing bank networks under known compliance regimes.

By offering a digital alternative to physical cash, retail CBDCs can make transactions more traceable and transparent to authorities. In principle, this should enhance AML/CFT monitoring and deter crimes like tax evasion (since fewer transactions go “off the books”). For example, China’s e-CNY is explicitly designed to improve traceability for law enforcement while still allowing some user privacy for small transactions [2]. However, retail CBDCs also raise concerns about surveillance and data misuse if every consumer payment is monitored. Striking the right balance between user privacy and financial integrity is a core challenge. Additionally, new cybercrime risks emerge – criminals may target CBDC wallets or exploit users unfamiliar with the technology in phishing and fraud schemes.

Since wholesale CBDCs are used among regulated banks and payment providers, they inherit the robust AML/CFT controls already in place at those institutions. Transactions in a wholesale CBDC would be recorded on a ledger accessible to the central bank and participating institutions, making illicit transfers difficult to conceal. In cross-border wholesale CBDC projects, there is potential to streamline compliance – for instance, shared platforms could embed sanctions screening and transaction monitoring by design. That said, wholesale CBDCs still require coordination between jurisdictions on regulatory standards. They also concentrate operational risk: any compromise of a wholesale CBDC platform (though unlikely with proper

security) could have systemic effects [1]. Overall, wholesale CBDCs are expected to reinforce existing financial crime controls rather than radically change them, given their limited access and high oversight.

Both types of CBDCs must be designed with financial crime prevention in mind. The Financial Action Task Force (FATF) affirms that CBDCs are subject to the same international AML/CFT standards as other forms of fiat money, even though their risk profile may differ due to digitization [3]. Importantly, regulators note that specific money laundering or terrorist financing risks could be higher or lower with CBDCs depending on design choices – continuous risk assessment and adaptation of regulations will be needed as CBDCs roll out.

2.2 Design features of CBDCs and regulatory implications

2.2.1 Privacy vs. traceability

One of the thorniest design issues is how to balance user privacy with traceability for law enforcement. Physical cash offers anonymity, which criminals exploit, but also provides privacy for law-abiding citizens. CBDC designs range from fully traceable (where every transaction is linked to an identity) to partially anonymous models for small payments.

China's digital yuan (e-CNY) illustrates an approach termed “controllable anonymity.” It provides a degree of anonymity for small-value transactions, akin to cash, but ensures larger or suspicious transactions are traceable by authorities [2]. In practice, users can make low-value payments without revealing personal data, but as transaction amounts grow, the system requires identity verification. This tiered model aims to satisfy the public's desire for some privacy while equipping regulators to detect illicit activity. According to the People's Bank of China (PBoC), this approach is intended to curb money laundering and even petty tax evasion by making large flows visible if needed [2]. Essentially, users remain anonymous to other users and merchants, but the central bank can “peel back” anonymity when law enforcement investigations demand it. The trade-off is clear: controllable anonymity can improve the overall integrity of the financial system, but it concentrates a lot of power (and data) in the hands of the central authority, raising civil liberty concerns.

At one extreme, a CBDC could be fully traceable – every transaction linked to a verified identity and visible to authorities. This would maximize the ability to track illicit money flows. The Bahamas' Sand Dollar, for instance, requires user identification for anything beyond the smallest transactions, and it maintains a “fully auditable non-anonymous transaction trail” by design [4]. Such transparency helps ensure that money cannot easily disappear into untraceable channels, thereby strengthening AML efforts. However, a fully traceable system effectively eliminates cash-like privacy; every purchase or transfer could be monitored. In democratic societies, there is strong pressure to incorporate privacy safeguards. The European Central Bank (ECB) has emphasized that the Digital Euro will prioritize data protection and privacy – in fact, the ECB reports that the offline version of the digital euro is being designed to be “cash-like” in privacy, meaning those transactions would not be routinely visible to intermediaries or authorities [5, 6]. As described by the EU Commission, small offline peer-to-peer payments in digital euro would work without disclosing transaction details, just as physical cash transactions are private [7]. To prevent abuse of this privacy, however, the amount that can be stored or spent offline will be capped. In summary, most CBDC projects seek a compromise: some level of anonymity for

low-risk, low-value use, combined with robust identification and traceability for large or suspicious transactions. Policymakers acknowledge that protecting user data and countering crime are both important public interests, and not mutually exclusive goals, if balanced with the right legal frameworks [8].

Traceability is only useful if the right authorities can access the data when needed. Legal frameworks for CBDCs often delineate who can see transaction information and under what circumstances. For example, many retail CBDC designs are “two-tier” (or hybrid) – the central bank runs the core ledger, but private intermediaries (banks or regulated payment providers) handle customer-facing services and maintain KYC (Know-Your-Customer) information. In such models, the central bank might see transaction amounts and wallet IDs, but only intermediaries know the identity of the user, unless regulators request it. This mirrors the status quo in traditional digital payments, and can leverage existing AML/CFT data-sharing rules. Jurisdictions will likely extend current practices (e.g. suspicious activity reports, information-sharing with Financial Intelligence Units) to CBDC systems [9]. The legal consensus is that CBDC implementations must “draw an appropriate balance” between user privacy rights and the needs of AML/CFT enforcement, possibly by building on the rules already used in conventional banking [9]. In any case, maintaining strong cybersecurity and access control is critical – sensitive personal and financial data from CBDC transactions must be protected from breaches, or else both privacy and investigative effectiveness could be compromised.

2.2.2 Programmability and smart contracts

CBDCs can be designed with programmability features – the ability to embed rules or conditions that execute automatically with transactions (similar to smart contracts in cryptocurrencies). This opens both promising use-cases and potential risks for financial crime:

Programmability could allow certain compliance rules to be automated. For instance, a CBDC could theoretically be coded to only be spent at certain merchants (useful for government benefits payments or restricted-purpose vouchers), or to require additional authorization for very large transfers. Such features could prevent some illicit transactions by design – for example, preventing CBDC from being sent to blacklisted addresses or abroad without proper clearance. Some have even suggested that “smart money” could be programmed to flag or freeze itself if it passes through a suspicious pattern of transactions. In practice, most central banks are cautious about overly restrictive rules at the base layer of the currency, but they are exploring conditional payments. The Digital Euro proposals include conditional payments (a form of programmability where a payment only executes if certain conditions are met) which could, for example, enable automated escrow or tax payments on transactions. If implemented carefully, these features could reduce fraud (by eliminating manual processing gaps) and improve tax compliance (e.g., sales tax could be deducted and sent to the treasury at the moment of purchase).

On the flip side, a programmable CBDC could be exploited by criminals. Security experts warn that if CBDCs enable smart contracts or similar scripts, malicious actors could deploy buggy or rogue contracts to facilitate fraud or money laundering. A CBDC that supports complex transactions might be leveraged to obfuscate illicit flows – for example, chaining a series of automated transfers through many wallets to hide the origin of funds. This is analogous to how criminals today use layering techniques and mixers in the cryptocurrency world to launder money. The RAND Corporation’s

research on CBDC design notes that while programmability offers innovative financial services, it also introduces new vectors for crime that will require advanced analytical tools and expertise to tackle [10]. Law enforcement agencies might need to monitor and analyze smart contract code just as they trace transactions, developing the capability to audit code execution to understand whether it facilitated illegal activity. In essence, adding programmability turns money into a sort of software, which means financial crime fighting also needs to adopt some approaches from software security (code audits, vulnerability management, etc.). Central banks like the ECB have indicated that initial versions of retail CBDCs will likely have limited programmability (focusing on basic payment functionality) exactly to avoid unintended consequences and keep the system robust and simple – more complex programmability might be layered via banking apps on top of the CBDC, where it can be more easily managed and regulated.

An oft-cited benefit of a digital currency fully controlled by a central authority is the ability to react swiftly to crime – for example, stolen funds could be frozen or even reverted to the victim. In theory, if a fraudster scams someone and takes CBDC, the central bank (or an authorized intermediary) might have the technical means to flag those specific tokens or wallet balances and render them unusable, or credit back the victim. This is far harder with cash (irreversible loss) and somewhat hard with cryptocurrencies without the private keys. However, implementing this in a CBDC raises legal and trust issues. It essentially requires the central bank to have a backdoor to alter ledger entries, which if abused (or hacked) could undermine confidence in the currency's immutability. Some jurisdictions may empower courts or central banks to intervene in extraordinary cases (similar to how banks can sometimes reverse fraudulent wire transfers), but this would likely be done with strict legal oversight. Participants in a U.S. Federal Reserve study suggested that enabling swift recovery of funds in a CBDC might be desirable, but the bigger challenges are legal, requiring new frameworks for when and how authorities could step in to reverse transactions [10]. If implemented, it could significantly reduce losses from fraud, but it must be balanced against the need for a stable, tamper-resistant currency.

2.2.3 Interoperability and cross-border challenges

Interoperability refers to how a CBDC interacts with other payment systems and other countries' currencies. It has big implications for financial crime because criminals often move money across borders to hide its origin.

A CBDC must integrate with the existing financial system – bank accounts, payment apps, etc. Most designs achieve this by allowing conversions between CBDC and bank deposits or cash seamlessly. From an AML perspective, integration means consistent oversight: the same AML/CFT checks that banks apply to deposit transfers should also apply when someone converts large amounts of CBDC to traditional money or vice versa. Central banks are generally planning CBDCs as complements to, not replacements for, private bank money [4], so interoperability within the domestic system is high. This also implies that financial institutions remain crucial gatekeepers for AML/CFT. For example, Nigeria's eNaira is integrated into the banking system with a tiered wallet model – users can load or unload eNaira through their bank or mobile money accounts, and each tier has strict limits unless full KYC is provided [11]. This interlinking ensures that existing AML infrastructure (like Nigeria's bank verification number system and transaction monitoring) extends into the CBDC realm. Similarly, The Bahamas' Sand Dollar is distributed through Authorized

Financial Institutions (AFIs) like banks and fintechs, which must undergo rigorous security assessments and comply with AML rules before they can issue wallets. The Sand Dollar is also restricted to domestic use only (it cannot be legally transferred outside the country), which helps limit illicit outflows and simplify oversight [4].

One touted benefit of CBDCs is more efficient cross-border payments. Projects like mBridge (a multi-CBDC platform by BIS and several central banks) are experimenting with using wholesale CBDCs to streamline international transfers [12]. If successful, these could reduce reliance on correspondent banks and make it easier to trace funds across jurisdictions. However, a major challenge is aligning regulatory frameworks. Each country has its own AML/CFT rules and thresholds; when CBDCs interoperate, whose rules apply to a cross-border transaction? International bodies recognize this issue. The FATF has highlighted the need for data-sharing and collaborative analytics across borders to fight money laundering in an interconnected CBDC world [8]. One example is the use of the “travel rule” (which requires that identifying information travel with transfers above a certain amount) – this would need to apply to CBDC transactions that cross borders just as it does for bank wires or crypto exchanges. The EU’s approach for the digital euro anticipates such challenges: the proposed law would set rules for use outside the euro area and likely impose conditions to prevent the digital euro from being used to bypass other countries’ laws [7]. In summary, interoperability without cooperation could open cracks for criminals – e.g., if one CBDC has weaker ID requirements, it might become a conduit to launder money into another jurisdiction. Thus, countries moving forward with CBDCs are actively engaging in forums (BIS, IMF, G20) to harmonize standards. A positive aspect is that CBDCs being new allows authorities to bake in compliance requirements from the ground up in a coordinated way, perhaps even more consistently than the patchwork of correspondent banking today.

An interesting development in cross-border financial crime prevention is the use of privacy-preserving technology to share data. Project Aurora by the BIS Innovation Hub demonstrated how multiple institutions across jurisdictions could run joint money laundering detection on transaction data without exposing personal details. By using privacy-enhancing technologies (PETs) and machine learning, Aurora’s proof-of-concept could detect complex laundering patterns that single institutions would miss, all while keeping individual customer data encrypted or anonymized during analysis. Such collaborative analytics are particularly relevant if CBDCs increase data availability – central banks and commercial banks could pool relevant transaction information to spot cross-border illicit networks, something that today’s siloed AML systems struggle with [8]. The takeaway is that interoperability paired with collaboration can actually strengthen crime fighting: CBDCs could create a more connected financial surveillance (with appropriate legal safeguards) that makes it harder for criminals to exploit jurisdictional gaps. But this will require strong governance, data protection, and political will to share intelligence.

2.2.4 Implications for AML/CFT (anti-money laundering and counter-terrorist financing)

CBDCs stand to significantly influence AML/CFT efforts globally. By design, a CBDC can either be a boon for financial transparency or, if mis-designed, a loophole that criminals exploit. Here we evaluate how CBDCs could help detect and deter money laundering and terrorist financing, as well as what new challenges they might pose.

A well-implemented retail CBDC would produce a comprehensive ledger of transactions accessible (under defined conditions) to authorities. This could dramatically improve the ability to follow the money in investigations. Suspicious patterns that span multiple banks or payment providers might be easier to see if those transactions all settle on a common CBDC ledger or a unified data format. Law enforcement could get a more holistic network view of financial flows, closing the gaps that launderers currently exploit by moving funds between siloed systems [8]. For example, a drug trafficking network often funnels illicit proceeds through many accounts at different banks; with a CBDC, if those transfers ultimately all use the central bank's ledger, an analytics system might spot the interconnected transactions more readily. Additionally, real-time monitoring could be possible. Instead of relying on after-the-fact bank reports, authorities could (with proper authorization) query certain flows in near real-time if triggers are met (e.g. unusually large rapid transfers between pseudonymous wallets could prompt an automated flag).

CBDCs can reduce reliance on physical cash, which remains a primary vehicle for money laundering (especially at placement stage) and for terrorist financing in many regions. Large cash transactions and cash smuggling become less necessary when more commerce is digital. If payers and payees adopt CBDC for convenience, criminals face pressure to also transact in CBDC or other digital means, which are more traceable than cash. Some governments explicitly link CBDCs to the fight against cash-based illicit activity. China, for instance, views the e-CNY as a tool to “prevent and combat” crimes by replacing untraceable cash exchanges with monitored digital payments [2]. Over time, a successful retail CBDC could shrink the “shadow economy” by bringing more transactions onto official, monitorable platforms. Likewise, tax authorities could benefit (as discussed later) – when business revenues are mostly digital and recorded, they cannot be as easily hidden.

Many CBDCs incorporate a tiered KYC approach, which actually aligns well with FATF's risk-based principles. Lower-risk, low-value users can get access with minimal friction (promoting inclusion), while higher-risk activity demands more verification. Nigeria's eNaira is a prime example: it establishes tiers of wallets – from a basic tier needing only a phone number, up to fully verified wallets linked to bank accounts and formal ID [4, 11]. Each tier has strict transaction and balance limits. A user with just a phone number can only transact a small amount per day (\$20,000, roughly \$50). To move larger sums, they must upgrade to higher tiers with appropriate KYC (providing ID, BVN, etc.). This limits the utility of the eNaira for laundering: a criminal cannot, for example, accumulate millions in unverified wallets – the system's design simply will not permit volume beyond certain thresholds. The Bahamas' Sand Dollar similarly uses tiered accounts: the lowest tier (no formal KYC) is capped at B\$500 holding and B\$1500 monthly transactions, whereas fully KYC'd business wallets can hold much more. These caps dramatically reduce the risk that anonymous wallets could be used to launder large sums. In effect, they force serious money launderers to reveal themselves by undergoing checks (or else stick to traditional methods).

Data generated by CBDC systems can be a goldmine for financial intelligence units (FIUs). Unlike cash that leaves no trail, every CBDC transaction could carry rich information (timestamps, participant identifiers, maybe even purpose codes) that analysts can mine for connections. Modern techniques like network analysis and AI can sift through this data to find clusters of suspicious activity that humans might miss. As noted with BIS's Project Aurora, combining payment data with machine learning greatly improves detection of complex laundering schemes [8]. AML investigators could, for example, rapidly trace the flow of funds through dozens of hops on a

CBDC ledger that would have taken much longer via bank statements and subpoenas in the current system. Quicker detection means quicker freezing of assets before they vanish. Moreover, traceable data is a boon for prosecutors – digital evidence of transactions is easier to present in court than trying to prove a cash exchange took place. In counter-terrorism finance, being able to map out a network of small payments that collectively indicate terrorist support (which often involves many low-value transactions) can be invaluable.

Ironically, having too much data can be a problem. If everyone starts using a CBDC, the volume of transactions to monitor might overwhelm existing AML systems. Authorities could be swamped with reports or flags. As the U.S. Treasury noted in its 2023 illicit finance strategy, modernization is needed so that the AML regime can handle new digital payment ecosystems efficiently [13]. Without advanced analytics, a CBDC might trigger many alerts that turn out innocuous (false positives), potentially wasting investigative resources. Law enforcement agencies will need training and tools to filter signal from noise. The DHS in the U.S. has been advised to prepare support for local law enforcement, as an influx of CBDC data “could overwhelm investigators, especially during early implementation” [10]. In short, the capability to track everything exists, but making sense of it in a timely manner is the real task.

If the public perceives a CBDC as a mass surveillance tool, they might resist using it, or worse, move to less regulated alternatives (like decentralized cryptocurrencies or cash hoarding) in response. This is a paradox: a CBDC too heavy-handed on AML could drive illicit activity into harder-to-monitor channels, undermining its purpose. For example, if a digital euro did not sufficiently protect privacy, individuals engaged in even minor tax evasion or unreported work might avoid it entirely and continue using cash or crypto, maintaining the shadow economy. Thus, over-centralized control might push criminals further underground, using methods outside the CBDC’s reach. Designers recognize this, which is why many emphasize privacy for law-abiding users. The ECB has even stated that the digital euro’s privacy level would be “unprecedented for electronic payments” – likely an effort to reassure users that it will not broadcast their every spending habit to the government [7]. Striking the right balance is crucial: enough transparency to deter criminals, enough privacy to retain public trust.

Criminals are adaptive. They will surely probe CBDC systems for weaknesses. One worry is “smurfing” on a new scale – i.e., breaking up illicit funds into many small transactions across many wallets to stay below detection thresholds. If a CBDC allows easy creation of new wallets (even if limited), a launderer might try to distribute, say, \$1 million into thousands of anonymous tier-0 wallets, each staying under limits, and then gradually consolidate them. To counter this, authorities will need sophisticated algorithms to identify such structuring across the whole network (much like banks manually try to spot structuring across accounts today). Another risk is cross-border arbitrage: if one country’s CBDC has stricter controls, criminals might route funds through another country’s CBDC or crypto and then into the target country. International cooperation (and ideally, interoperability of compliance data) will be needed to close that avenue.

Nation-state adversaries or sanctioned entities could seek to use CBDCs of countries that are outside the dominant dollar-based system. For instance, sanctioned actors might favor a CBDC that does not implement the same level of screening. However, most major CBDC initiatives (China, EU, etc.) are being developed by jurisdictions that actively enforce sanctions and CFT. Indeed, CBDCs could strengthen sanctions enforcement by giving governments direct oversight of currency flows.

A notable consideration is how CFT (terrorism financing) might benefit: terrorist networks often rely on cash couriers or informal value transfer. If CBDCs reach areas with high unbanked populations, they could reduce reliance on opaque informal networks like hawala – but only if paired with outreach and incentives for those communities to use the official channels. Conversely, terrorist financiers, like other criminals, might use more privacy-oriented cryptocurrencies if they suspect CBDCs are heavily monitored. Governments will likely continue a multi-pronged approach: promoting CBDC adoption for the transparency benefits, while also tightening regulation on crypto and other alternatives to prevent displacement of illicit funds.

In summary, CBDCs present a unique opportunity to modernize AML/CFT frameworks for the digital age. If implemented with robust identity controls, data analytics, and international cooperation, they can significantly raise the cost and difficulty of money laundering and terrorist financing. Studies suggest that carefully designed CBDCs can indeed improve AML effectiveness – one recent analysis concludes that the focus should be on leveraging CBDC within strong AML frameworks rather than, say, banning cryptocurrencies outright [14]. However, success will depend on adaptive regulation and addressing the challenges above. Policymakers must update AML/CFT laws (e.g. adjusting reporting thresholds, allowing digital identity verification, etc.) to fit the CBDC context. As the IMF cautions, continuous risk assessment and adjustments will be needed as criminals respond to the new system [1].

2.2.5 Implications for fraud and cybercrime

While AML/CFT deals with illicit use of funds by criminals, fraud concerns the wrongful deception of individuals or institutions to steal assets – and CBDCs introduce new angles to this age-old problem. We consider how CBDCs might help reduce certain types of fraud and what new fraud risks they could usher in, including digital scams, theft, and counterfeit issues.

A digital currency cannot be counterfeited in the traditional sense. You cannot print a fake digital dollar. Each CBDC unit is a cryptographically secured token or account entry validated by the central bank. This means that a major category of fraud – counterfeiting of banknotes – would effectively vanish for the CBDC portion of money in circulation. For example, eNaira transactions are cryptographically signed and recorded on the ledger (built on Hyperledger Fabric), making it impossible to falsify eNaira “notes” [11]. This shifts the focus to securing the system rather than policing physical counterfeit rings. Central banks also will not have to worry about advanced forgery of banknotes, which costs governments and deceives citizens.

If CBDC wallets require strong user authentication (e.g., biometrics or multi-factor login) and perhaps even secure hardware, it can reduce certain fraud like payment instrument theft. For instance, the Sand Dollar wallets mandate multi-factor authentication for transactions [4]. If someone steals your phone, they still could not send your CBDC without, say, your fingerprint or a PIN. This is similar to mobile banking security but could be made universal for all CBDC users. Also, because the central system can have rules, unusual transactions (like a sudden transfer of your entire balance to an unknown party) might be flagged or delayed for verification. In contrast, if someone gets access to your physical cash or even your debit card PIN, they can often quickly drain funds. A CBDC system could incorporate circuit breakers – for example, if a typically inactive wallet suddenly tries to transfer a very large amount, the system might pause it for a manual check. Such measures, while potentially annoying to users occasionally, could catch certain fraud scenarios (like elder financial abuse, where a

fraudster convinces an elderly person to send money – an automated rule might catch that as out-of-character).

In cases of fraud or error, CBDCs might allow more direct and swift resolution. Today, if you are scammed into a bank transfer, recovery is hard unless law enforcement quickly intervenes and the receiving bank cooperates. With CBDC, especially if there are known intermediaries or even direct central control, there might be a window to freeze and reverse fraudulent transactions (subject to legal processes). Some commentators suggest implementing “reversible transactions” for a brief period or for certain fraud scenarios [10]. While full reversal capability has downsides (moral hazard, complexity), limited mechanisms (like an escrow period for unfamiliar new payees, or flagged recall for suspected fraud) could reduce losses. Over the long run, public confidence in using CBDC will depend on whether people feel protected from scams – so user protections similar to those on credit cards (dispute a charge) might emerge, backed by the technology of CBDCs.

The traceability we discussed in AML also helps after-the-fact in fraud cases. If a hacker steals funds, tracing where they go is easier on a transparent ledger than if they stole cash or untraceable crypto. This could deter some fraudsters if they know any stolen CBDC is likely to be tracked and possibly frozen when they try to off-ramp it. Moreover, because each wallet is known to the operator, law enforcement can quickly identify the beneficiary of fraud proceeds (provided they are in the CBDC system). In comparison, a thief today might route money through multiple banks or crypto exchanges under false names; a unified CBDC ledger could shorten that trail.

The most prevalent risk with retail CBDCs is not high-tech hacking but old-fashioned scams repurposed for a new medium. Fraudsters may exploit people’s unfamiliarity with how CBDCs work. For example, scammers could pose as central bank officials or tech support, telling users there’s an “issue” with their digital wallet and tricking them into revealing credentials – much like phishing emails today, but targeting the CBDC app. In countries where CBDCs are novel, people might be more susceptible to false promises (e.g., “upgrade to premium wallet, just send me your login”). If CBDC accounts become as common as bank accounts, fraudsters will simply shift tactics to target them. We might see an increase in “authorized push payment” fraud, where victims are conned into voluntarily sending money to the fraudster’s wallet (thinking it’s a legitimate payee). The UK and others have struggled with this in online banking, and it could carry over to CBDCs. Indeed, research warns that a CBDC could “offer an attractive new medium for criminals” to conduct small-scale frauds, especially targeting vulnerable populations like the elderly [10]. For example, a scam targeting seniors might encourage them to move their savings into “digital cash” for safety, but actually redirect them to a fraudster’s wallet. Public education and anti-fraud measures will need to accompany CBDC deployment, just as governments now frequently warn about phone and email scams.

As with any digital system, a CBDC ecosystem will be targeted by hackers. The central infrastructure itself will be high-value: a successful breach could, in theory, create counterfeit balances or redirect funds (though central banks will invest heavily in security to prevent this). More likely, attackers will go after endpoints – individual users’ devices or the third-party wallet providers. Malware that infects a user’s phone could sniff out credentials or manipulate the CBDC app. There is also risk of SIM-swapping attacks (stealing a phone number to intercept one-time passwords) to get into wallets. If criminals manage to compromise many accounts, they could siphon off lots of small amounts (to avoid detection) in an automated way. This kind of cyber-fraud might increase with CBDCs simply because there will be a new target

and presumably a large user base. We've seen similar trends with online banking and mobile payment apps – as usage rises, so do efforts to break in. Central banks and wallet providers will need top-notch cybersecurity, continuous monitoring for unusual activity, and perhaps even AI-driven fraud detection. Another aspect is endpoint hardware: some CBDC trials include hardware wallets or smartcards for offline use (like prepaid cards for the digital currency). These could be physically stolen or cloned if not properly secured. Ensuring that stolen devices can be quickly deactivated is important.

If the CBDC supports programmability, fraudsters may exploit it. For instance, imagine a malicious merchant programming a payment link that overcharges a user's wallet via a complex contract the user did not understand. Or bugs in a smart contract could be manipulated to divert funds (this has happened in DeFi crypto platforms repeatedly). The RAND report points out that smart contracts in a CBDC could be vulnerable to exploitation for fraud and theft, necessitating new forensic and investigative techniques [10]. Even if the CBDC itself is not fully programmable, integration with other systems might be. For example, if a CBDC connects with an e-commerce API, a hacker might try to manipulate payment requests to their advantage. This is a more technical threat and might be mitigated by limiting CBDC programmability in early stages.

KYC is a pillar of AML, but criminals may attempt to fool it. In a CBDC context, that could mean using stolen identities or synthetic IDs to open wallets, especially in a tiered system. If tier 3 wallets (high limit) require full ID, we might see more document forgery or corrupt insiders enrolling false identities, to bypass limits. Nigeria's eNaira rollout, for instance, identified "poor compliance culture" and insider fraud as potential weaknesses that could undermine the AML controls if not checked [15]. This applies to fraud generally – if bank or fintech employees who serve as intermediaries are compromised, they might help criminals open wallets or approve transactions illicitly. Ensuring strict oversight of any intermediating entities (through audits, etc.) is necessary. Also, implementing strong digital ID systems linked to CBDC can reduce identity fraud (e.g., biometric verification for wallet creation could prevent one person from impersonating another).

In many countries, bank deposits are insured and there are clear procedures if fraud occurs (customers often get reimbursed for unauthorized transactions above certain amounts). It's yet unclear how consumer protections will apply to CBDCs – will central banks or governments compensate victims of CBDC fraud? If not, fraud losses could fall directly on individuals, potentially making CBDCs riskier for the average person than a bank account (from a consumer standpoint). Policymakers will need to decide on frameworks for liability. A lack of clarity or protections might be exploited by fraudsters (knowing the user has little recourse). This is more of a policy gap than a technological one, but it affects the incentive for fraud. We may see, for confidence's sake, governments extending deposit insurance or similar guarantees to CBDC holdings, which indirectly covers certain fraud situations too.

In essence, fraud is likely to persist in new forms with CBDCs. The nature of scams will adapt to digital wallets, and cyber threats will loom large. However, there is hope that many frauds can be curbed through robust security and some of the programmability of CBDCs. A crucial part of mitigating fraud will be educating users: just as people have learned to be cautious of phishing emails from "banks," they will need to be savvy about schemes involving "CBDC support" or fake wallet apps. Law enforcement will also need to update their skills – tracking stolen digital currency, working with the central bank to freeze suspect funds quickly, and understanding the nuances of CBDC technology. The silver lining is that with a centralized system,

it may be easier to coordinate responses (contrast with the challenge of coordinating across hundreds of private banks in a fraud scheme today). As a preventative stance, central banks are building security from day one: for example, The Bahamas vetted all technology partners for Sand Dollar and required strong encryption and security audits at every layer [4]. Those efforts must continue post-launch, as a CBDC will likely become part of national critical infrastructure that requires constant defense against fraud and cybercrime.

2.2.6 Implications for tax evasion and financial transparency

Tax evasion – the illegal underpayment or non-payment of taxes – often relies on opaque transactions and unreported cash income. CBDCs have the potential to significantly alter the equation by pushing more economic activity into traceable digital form.

When transactions happen through a CBDC, they leave a digital record. If a substantial portion of business sales and individual transactions flow through CBDC wallets, it becomes much harder for businesses or individuals to hide that activity from tax authorities. For instance, a shop that currently might under-report cash sales to avoid VAT would, if most customers pay via CBDC, generate an indelible transaction log visible (at least to the intermediary or via audit) to authorities. Even if the tax authority does not see every transaction in real-time (and they likely would not, to preserve privacy), audits could be conducted by analyzing a business's declared revenue against aggregate data from the CBDC system. The result is a shrinkage of the "cash economy" where under-the-table deals happen. China explicitly touts the anti-tax-evasion benefits of its e-CNY; by using traceable digital yuan, authorities aim to detect unreported income more easily. In one noted statement, Chinese officials linked the controllable anonymity of e-CNY with curbing illicit financial activities including tax evasion. This implies that if large payments (say for property or luxury goods) are done in e-CNY, the authorities can follow up on whether appropriate taxes (like property tax, sales tax, etc.) were paid [2].

A government could integrate CBDC data with tax enforcement. For example, smart contracts could be used for tax collection – imagine that whenever a business receives a payment above a certain amount, a portion is automatically flagged or set aside for tax. While not many jurisdictions have suggested automating tax at the currency level, the concept is technologically feasible. At the very least, information sharing can be improved. Tax authorities often have to request banking data during audits, which takes time. With CBDC, they might have faster or more direct access to verified transaction histories (with legal process). In some visions, for small peer-to-peer offline transactions, privacy is preserved; but for larger online transactions, a trail exists that could be shared under proper agreements. This can also tie into the fight against illicit financial flows: money laundering and tax evasion are sometimes linked (laundered money often escapes taxation). A cleaner financial system through CBDCs means both less crime and more captured tax revenue.

Wages paid off the books (to avoid income tax or payroll taxes) could decline if economies move to CBDC for disbursements. Governments might encourage or even require that certain payments (like salaries, government contractor payments, etc.) be made via traceable digital means. For example, a government could pay all its employees in CBDC – this guarantees those salaries are on the record (which they already are, but it sets an example). If businesses pay workers in CBDC, those payments are clearly income that should be taxed. In developing countries, a significant portion of

employment is informal and paid in cash; if CBDC use spreads to even small vendors (perhaps through convenient mobile phone wallets), the scope for completely hidden cash-in-hand jobs narrows. Some emerging market central banks consider financial inclusion and formalization as goals of CBDC – drawing people into the formal economy typically increases the tax base over time.

CBDCs might also help combat international tax evasion. Initiatives like the Automatic Exchange of Information (AEOI) already allow countries to swap data on bank accounts for tax purposes. If foreign individuals hold or use a country's CBDC (possible in future cross-border scenarios), those transactions might be easier to track and report to the relevant country. For example, if a European uses digital euros outside the EU, those could be monitored for reporting thresholds. Or if offshore tax evaders try to park money in a CBDC under someone else's identity, the strong KYC requirements of CBDCs might foil that, or the transparent ledger might reveal patterns that lead investigators to the source. Essentially, the more transparent the global financial system, the less the room for hiding taxable assets. CBDCs, being new, could adopt AEOI and other reporting standards from the start, which banks took years to implement.

Most CBDC proposals do allow a degree of anonymity for small transactions (to mirror cash). This means minor tax evasion could still persist – e.g., a handyman could do a small home repair and be paid in offline CBDC that both parties know will not be reported. If offline functionality allows, say, a few hundred euros to exchange hands unrecorded, then petty tax underreporting at small scale may continue. The key is that large-scale evasion (which contributes the bulk of lost tax revenue) would be harder. A building contractor will not easily hide a \$100,000 job by splitting it into 200 offline micro-transactions without raising suspicion. In the EU's plan, offline digital euro payments would be “mainly for small payments” and subject to strict limits specifically to mitigate AML/CFT and by extension tax evasion risks [7]. Policymakers accept some *de minimis* anonymity as a trade-off for privacy; they just want to ensure it's truly limited to low values.

If CBDCs make domestic evasion difficult, some evaders might turn to cryptocurrencies or other assets (gold, foreign cash) to hide wealth. We could see a shift in how tax evasion is done rather than elimination. For example, an individual might convert ill-gotten or untaxed money into Bitcoin instead of keeping it in the CBDC where it could be noticed. Governments are concurrently tightening crypto regulations to prevent this arbitrage. Also, crypto volatility and complexity make it a less accessible avenue for the average small evader compared to just using cash. Over time, if CBDCs and accompanying policies significantly reduce cash usage, the hope is that all digital forms of value transfer will be regulated in a way that leaves few dark corners (crypto included, through exchanges and on/off ramps oversight). Nonetheless, one cannot assume CBDC alone fixes tax evasion; it must be part of a broader move towards transparency in all payment methods.

Using financial data for tax enforcement walks a fine line regarding privacy. Citizens may accept that obvious evasion should be caught, but they might bristle at tax authorities potentially having too much insight into their finances. Legal safeguards will be needed to ensure that only relevant data is used in audits, and perhaps that automated tax scrutiny does not overreach (e.g., not every person's spending habits are combed through without cause). The ideal scenario is that honest taxpayers have nothing to fear – maybe they even benefit if CBDCs allow simplified tax filing (imagine your digital wallet providing you a statement of income and deductible expenses). However, governments will need to communicate clearly that CBDCs are

not a voyeuristic tool but a means to ensure everyone pays their fair share. Successful examples could persuade the public: if a country can show that CBDC adoption led to a measurable increase in tax compliance, reducing the burden on honest taxpayers or funding better public services, it strengthens the case.

Tax systems are complex. Simply having data does not automatically translate to capturing more taxes – authorities must have the capacity to analyze and act on it. Developing countries with weaker tax administration might not immediately gain from CBDC data unless they invest in their revenue services. Also, legal changes may be required to allow tax authorities to directly obtain CBDC transaction information, as it might currently be protected under banking secrecy or data protection laws. These changes need careful debate and checks and balances.

In conclusion, CBDCs have a generally positive outlook for tax compliance. By illuminating transactions, they constrain the avenues for hiding income. They effectively push the economy towards electronic payments where transparency is the default. This could lead to higher reported incomes, better VAT collection, and fewer opportunities to launder untaxed money into usable form. Countries like China explicitly see digital currency as a way to “improve the overall integrity of China’s financial system”, which includes ensuring people pay taxes owed [2]. The exact impact will vary by jurisdiction – those with already high compliance may see marginal gains, whereas those with large informal sectors could see more substantial improvements. However, it will not abolish tax evasion overnight; rather, it narrows the scope and raises the effort required to cheat the system. Paired with continued international cooperation (so evaders cannot just move offshore), CBDCs can be a powerful tool to bolster financial transparency.

3. Different jurisdiction approaches to regulations

Jurisdictions across the globe have adopted distinct regulatory approaches to CBDCs, each shaped by national priorities, institutional capacity, legal traditions, and risk tolerance. China, for example, has taken a state-centric and security-driven regulatory path with its e-CNY. The People’s Bank of China (PBoC) enforces a tiered wallet system that balances “controllable anonymity” for low-risk transactions with full traceability for higher-value or suspicious activity. The e-CNY is tightly integrated with the country’s social credit system and national ID infrastructure, allowing regulators to embed real-time oversight, enforce capital controls, and support financial surveillance objectives such as anti-corruption and AML enforcement. This approach reflects China’s broader emphasis on state control, national security, and monetary sovereignty.

In contrast, the European Union, through the European Central Bank (ECB), has emphasized privacy-by-design and strong data protection as central pillars of its Digital Euro proposal. The ECB envisions offline payment functionality for small transactions that mimics the anonymity of cash, combined with robust AML/CFT safeguards for online transactions. Compliance responsibilities would be delegated to supervised intermediaries, with the central bank having limited access to personal transaction data. This structure is heavily influenced by the EU’s General Data Protection Regulation (GDPR), which places strict limitations on data collection and usage. The ECB’s stance demonstrates a regulatory preference for safeguarding civil liberties, trust, and democratic accountability in digital currency systems.

Nigeria has taken a more compliance-focused and inclusion-oriented approach with its eNaira. The Central Bank of Nigeria (CBN) designed the eNaira with a

tiered KYC system linked to the country's national ID framework (NIN), allowing unbanked or underbanked individuals to access digital financial services while enforcing transaction and balance limits for less-verified users. This model is aimed at reducing the size of the informal economy, curbing illicit cash transactions, and improving tax compliance. Regulatory oversight is centralized at the CBN, with commercial banks and fintech providers serving as distribution and onboarding channels. Nigeria's approach also includes a public education campaign and merchant incentives to boost adoption, reflecting broader developmental goals beyond financial crime prevention.

The Bahamas, as the first country to fully deploy a retail CBDC, has taken a domestically focused and risk-contained approach with its Sand Dollar. Issued by the Central Bank of The Bahamas, the Sand Dollar is subject to strict identity verification requirements and is confined to domestic use. Wallet types are differentiated by user category—individuals, businesses, and government—each with specific transaction and balance caps. Regulatory objectives center on improving access to financial services in remote islands, reducing the circulation of physical cash, and enhancing transparency to prevent fraud and illicit capital outflows. The central bank maintains a high degree of operational control, including the ability to freeze wallets or trace suspicious activity when necessary.

These regulatory variations underscore how CBDC design and oversight are not one-size-fits-all. Some countries, like China, prioritize centralized control and traceability to support national security and enforcement capacity. Others, like the EU, stress user rights, privacy, and institutional trust. Emerging economies, such as Nigeria and The Bahamas, view CBDCs as tools for inclusion and macroeconomic resilience, while still embedding safeguards against financial crime. The divergence in regulatory models reflects the tension between technological innovation, sovereignty, financial stability, and civil liberties—and highlights the need for international cooperation to address regulatory arbitrage, especially as cross-border CBDC use becomes more feasible.

4. Conclusions

The introduction of CBDCs globally represents a double-edged sword for financial crime. On one side, CBDCs offer unprecedented visibility into financial transactions, presenting a powerful tool to combat money laundering, terrorist financing, fraud, and tax evasion. By embedding compliance features (identity verification tiers, transaction monitoring, traceability) into the very architecture of money, CBDCs could significantly harden the financial system against illicit use. Early evidence and expert analyses suggest that if carefully designed, CBDCs can indeed improve AML/CFT effectiveness and enhance overall financial integrity. The ability to program money, enforce rules automatically, and analyze a unified ledger of transactions can give regulators and law enforcement new advantages in the “cats and mice” game of financial crime [14].

On the other side, new technology always comes with new vulnerabilities. CBDCs could create novel avenues for fraud (from phishing scams to malware attacks on digital wallets) and raise complex questions about data privacy. If poorly designed – for example, if they allowed too much anonymity or had weak cyber protections – CBDCs might inadvertently facilitate certain crimes or simply displace illicit activity into other channels. The key is governance and design: finding the sweet spot where the currency

is secure and transparent enough to catch criminals, but not so draconian or invasive that it drives users (legitimate or illegitimate) away or violates rights. Technical choices like the level of privacy, limits on holdings, degree of programmability, and interoperability protocols must be calibrated with inputs from financial regulators, privacy commissioners, and technologists alike.

From a global perspective, coordination will be vital. Money launderers and fraudsters are adept at exploiting any weakest link. If major economies roll out CBDCs with strong controls, criminals may target jurisdictions with lagging standards or try to bridge into less monitored assets. International standards (via BIS, FATF, IMF guidance) will help ensure a consistent front. FATF already clarifies that CBDCs should be treated as fiat under its standards and urges proactive risk assessment for any higher risks arising from digitization [3]. As CBDCs launch, these standards may need updates – for instance, guidance on sharing CBDC transaction data across borders for AML, or new typologies of misuse to watch for. Encouragingly, experiments like BIS's Project Aurora show that through collaboration and technology, we can counter financial crime while respecting privacy [8]. Privacy-enhancing tech and AI may become staples of CBDC oversight, allowing detection of illicit networks without exposing honest users' data unnecessarily.

In sum, the advent of CBDCs could herald a future where illicit finance has fewer places to hide. Retail CBDCs, in particular, could drastically reduce the anonymity that cash and certain crypto-assets grant to criminals, thereby tightening the loopholes in AML/CFT regimes. Tax evasion could become more difficult as digital transactions dominate. Wholesale CBDCs can improve transparency and efficiency in interbank flows, aiding in sanctions compliance and reducing opportunities for large-scale money laundering through shell institutions. Yet, the fight against financial crime will not be "solved" by technology alone – it will remain a continuous effort of regulation, enforcement, and adaptation. CBDCs will equip authorities with better tools, but also demand that those authorities upskill and remain vigilant for new criminal tactics. As one IMF report noted, each design choice comes with different financial integrity implications, and ongoing evaluation is needed [1].

For policymakers, the recommendation is clear: integrate financial crime safeguards from the ground up in CBDC designs, but do so in a balanced, transparent manner. For law enforcement and regulators: prepare to leverage CBDC data and technology, invest in analytical capabilities, and update legal frameworks to enable effective action in a CBDC-driven world. For the public: engage in the dialog about how much privacy and oversight a digital currency should entail, since societal values must shape these technical systems. If we get it right, CBDCs could significantly tilt the advantage away from criminals and towards those protecting the integrity of our financial systems, all while fostering innovation and inclusion in the digital economy.

Author details

Charles Chan
Independent Researcher, London, UK

*Address all correspondence to: yiulaic@gmail.com

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Liu Y. CBDC Policy: The Legal and Financial Integrity Element [Presentation]. Washington, DC, United States: International Monetary Fund; 2023. Available from: <https://www.imf.org/-/media/Files/Conferences/2023/11/sti-25th/sti-anniversary-cbdc-yan-liu-nov-14-2023.ashx> [Accessed: July 17, 2025]
- [2] Sanction Scanner. China Has Created its Own Digital Currency: Understanding Digital Yuan. Istanbul, Turkey, London, United Kingdom: Sanction Scanner; 2025. Available from: <https://www.sanctionsscanner.com/blog/china-has-created-its-own-digital-currency-understanding-digital-yuan-387> [Accessed: July 17, 2025]
- [3] Fisch EJ, Maalouf KN, Seidner G. FATF Updates its Global Guidelines for the Regulation of Virtual Assets with an Eye to Emerging Technologies. Skadden, Arps, Slate, Meagher & Flom LLP; 2021. Available from <https://www.skadden.com/insights/publications/2021/11/recent-developments-in-the-regulation-of-virtual-assets/fatf-updates-its-global-guidelines> [Accessed: July 17, 2025]
- [4] Branch S, Ward L, Wright A. The evolution of sand Dollar. *Intereconomics: Review of European. Economic Policy*. 2023;58(4):178-184. DOI: 10.2478/ie-2023-0038
- [5] Subrahmanyam V. China's digital currency: The hopes and fears of the e-CNY. *China Currents*, China Research Centre (Atlanta, Georgia, USA). 2023;22(1). Available from: <https://www.chinacenter.net/2023/china-currents/22-1/chinas-digital-currency-the-hopes-and-fears-of-the-e-cny/>
- [6] Ledger Insights. ECB Provides Offline Digital Euro Progress Report. Cyprus: Ledger Insights; 2024. Available from: <https://www.ledgerinsights.com/ecb-provides-offline-digital-euro-progress-report/> [Accessed: July 17, 2025]
- [7] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union. Frequently Asked Questions: Digital Euro and Legal Tender (Cash). European Commission; n.d. Available from: https://finance.ec.europa.eu/digital-finance/digital-euro/frequently-asked-questions-digital-euro-and-legal-tender-cash_en [Accessed: July 17, 2025]
- [8] Bank for International Settlements. Legal Aspects of Retail Central Bank Digital Currencies (OCP Paper No. 66). Basel, Switzerland: Bank for International Settlements; 2023. Available from: <https://www.bis.org/publ/othp66.htm> [Accessed: July 17, 2025]
- [9] Bank for International Settlements. Legal Classification of Retail CBDCs: The Obligations and Liabilities of Stakeholders (OCP Paper No. 88). Basel, Switzerland: Bank for International Settlements; 2023. Available from: https://www.bis.org/publ/othp88_legal.pdf [Accessed: July 17, 2025]
- [10] Mignano J, Egel D, Levine PR, Cunningham D, Jackson BA, Hollywood JS, et al. Central Bank Digital Currency Design Choices and Effect on Law Enforcement. 2025. Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2952-1/RAND_RRA2952-1.pdf#:~:text=A%20programmable%20CBDC%20would%20enable,needed%20to%20detect%20and%20investigate [Accessed: July 17, 2025]
- [11] Ree J. Nigeria's eNaira, One Year after (IMF Working Paper No. WP/23/104).

Washington, DC, United States:
International Monetary Fund; 2023.
Available from: <https://www.imf.org/-/media/Files/Publications/WP/2023/English/wpica2023104-print-pdf.ashx>
[Accessed: July 17, 2025]

[12] Bank for International Settlements, Innovation Hub. Project mBridge: Experimenting with a Multi-CBDC Platform for Cross-Border Payments [Brochure]. Basel, Switzerland: Bank for International Settlements; 2023. Available from: https://www.bis.org/innovation_hub/projects/mbridge_brochure_2311.pdf [Accessed: July 17, 2025]

[13] U.S. Department of the Treasury, Office of Terrorist Financing and Financial Crimes. National Strategy for Combating Terrorist and Other Illicit Financing [Strategy Report]. U.S. Department of the Treasury; 2024. Available from: <https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf> [Accessed: July 17, 2025]

[14] Gaisina A, Finger M. Central bank digital currencies (CBDCs): A countermeasure to anti-money laundering (AML) challenges posed by cryptocurrencies? *Digital Finance*. 2025;7:201-254. DOI: 10.1007/s42521-025-00132-9

[15] Esoimeme E. A Critical Analysis of the Effects of the Central Bank of Nigeria's Digital Currency Named eNaira on Financial Inclusion and AML/CFT Measures [Research Report]. *GRC & Financial Crime Today*. Issue 3, November 2023; 2021. DOI: 10.2139/ssrn.3921396

Perspective Chapter: The Future of Wholesale CBDCs in a Tokenizing and Trumpian World

Michael Lloyd

Abstract

Globally, the private sector is moving towards expanding the growth of tokenized assets trading, using private money channels (stablecoins) as payment systems. At the same time, the public sector, often central banks in alliance with private sector partners, is engaged in ambitious projects, exploring the feasibility of public payment systems using wholesale CBDCs to facilitate the cross-border use of fiat currencies and to ensure universal public trust in global cross-border payments. The advent of the use of distributed ledger technology over the past decade is enabling these activities to take place. This paper outlines these developments and their impacts and the future emergence of a global assets trading and payments ecosystem. The emergence of this system is also considered in the context of the gradual restructuring of global trade and monetary patterns, via private and public sector initiatives, and the potential significant impact of a Trumpian world order. The future seems to imply a more protectionist and, effectively, isolationist US—in monetary as well as trading terms.

Keywords: wCBDCs, tCBRs, United States, Trump, distributed ledger technology, tokenization, regional digital payment systems, stablecoins, unified ledgers

1. Introduction

The chapter is divided into seven main sections: Introduction; Digital Payments, Tokenization, and Distributed Ledger Technology; Stablecoins in Cross-border Trading and their Regulation; Prerequisites for Successful Tokenisation of Assets Trading; A Potential Global Digital Assets Trading and Payments Ecosystem; Geopolitical Trends; Conclusion. Specific topics covered will include digitised and tokenized payments, the permission of blockchains, unified ledgers, regulatory issues, technological interoperability, central banks' global and regional CBDC projects, shifting global trade impacts, and the impact of changing US stablecoin policies on global assets trading and payments.

Central bank money is the core of the fiat money system within monetary jurisdictions, in terms of establishing the *universal* trust of citizens in fiat money within monetary jurisdictions. Moreover, central banks ensure both clearance and, crucially, final settlement of all financial transactions [1]. Central bank money, either

as cash, state-guaranteed commercial bank money, or central bank reserves in the form of wholesale CBDCs (wCBDCs), is unique and stands as a form of social and legal validation for the conduct of monetary policy and the provision of liquidity insurance, as during the aftermath of the Global Financial Crisis (GFC). A key issue in the putative establishment of a functional and financially stable global ecosystem to support digitised assets trading and payments, providing liquidity, security, and universal clearance and final settlements is likely to be the involvement of wholesale CBDCs. Progress in the US of the Genius Act, ensuring the regulation of stablecoins is an important step in this global development.

The United States has hitherto been slow to engage with CBDCs, abjuring retail CBDCs, now prohibited by President Trump [2] and only reluctantly involved with the research of wCBDCs. This unenthusiastic engagement with wCBDCs appears to be because of a general US view of the equivalence of private (and now cryptographic money channels, such as Bitcoin and stablecoins) [3] with public channels. The future position of the US on both stablecoins as settlement currencies and crypto-assets as investments vehicles, in a global context, is currently uncertain. However, given the widespread use of the US dollar in global assets' trading, for instance, 80% of bond trading is done in dollars.

Notwithstanding the US scepticism, a digitised range of globally traded financial assets, including money, is being explored, involving the Bank for International Settlements (BIS) in various projects with central banks, commercial banks, and large financial companies, see Agora [4] and Nexus [5]. The advent of "tokenization" (digital representation of any asset) is accelerating the general development of digitised global ecosystems, potentially underpinned by wCBDCs to provide final payment settlement. These systems could involve tokenized commercial bank deposits and stablecoins in trading a plurality of tokenized financial assets on programmable distributed unified ledger platforms, with an undergirding of wCBDCs to provide universally validated payment.

At the same time, the private sector is exploring and developing tokenized assets trading. Tokenization may best be defined as the digital representation of assets, including money, established on a programmable digital network platform [6]. Any assets, financial or physical may be represented in this manner and are then potentially tradable across the world. Trading in assets may be processed across a variety of private asset-trading platforms. Currently, the relatively modest level of such trading, principally financial assets is conducted via proprietary platforms such as Ripple, using stablecoins such as, USDC or Tether, the two largest stablecoins by market capitalisation. Other companies involved are Blackrock, Fidelity, and Morgan. Assets trading is set to expand significantly from the current amount of 0.6 billion USD in 2025 to 9.4 billion USDC in 2030 and doubling in the next 3 years thereafter, see Ripple and BCG [7].

Our assessment highlights a continuing need for future research to understand the dynamics of global crypto flows. Our analysis indicates that policy measures designed to dampen traditional financial flows may have limited impact on constraining cross-border crypto activity. Yet, as crypto assets become more integrated with main-stream finance, understanding the systemic risks and potential contagion effects between these markets will be essential for policymakers and market participants alike. At the same time, the socio-economic implications of increased crypto adoption, particularly in emerging market and developing countries, warrant a deeper examination. This includes assessing the impact on financial inclusion and economic stability and the potential for crypto-assets to serve as a hedge against local currency volatility and weakness [7].

There is little doubt that progress on the digitization of financial payments has been made in the last decade, both nationally, and increasingly in terms of cross-border transfers. Financial markets have benefitted in relation to lowered costs and risk reduction. One example is the enabling of algorithmic trading on foreign exchange platforms. As indicated above, tokenized assets trading being set to expand substantially in this decade should perhaps lead to the need for clearance and settlement to be provided on public platforms using wCBDCs. This would ensure the provision of essential universal trust and global financial stability. Currently, there is no guarantee that this will happen, though the BIS has been lobbying for such an approach, see BIS citation below, page 4.

One thorny issue is the position of the US and the attitude of the Trump administration, especially towards CBDCs. The advent of the re-election of Trump, and his strong enthusiasm and personal involvement with crypto assets [8] seems likely to reinforce the rejection of the role of CBDCs as a topic to be pursued. However, given the hegemonic, ubiquitous role of the US dollar, and the role of stablecoins in the development of a global assets trading and payments ecosystem, the active participation of the US in such a global system is almost inevitable. The key issue is whether this is viewed as being served via stablecoins as a private money channel of whether central bank wholesale CBDCs will also be involved. Hence, the chapter will also explore three potential scenarios.

First, a scenario based on the continuation of the innovative work being done—much of it involving the BIS, central banks, and commercial banks, together with other private sector financial organisations—in linking the development of assets trading with validated fiat currency payment systems. It will be argued that these technological developments could facilitate a neutral but effective multi-fiat-currency alternative to over-reliance of the US dollar, specifically in relation to trade invoicing, as suggested by Mayer in his 2024 article [9].

Second, a scenario taking into account the changing global economic and trading structure, involving significant substantial shifts to East Asia, and its implications for developments in relation to digitised fiat currency payments, especially those geared to trade invoicing. One example here is the evolving BRICS payments initiative (see page 20), also using a digital ledger technology payments platform.

Third, a scenario exploring how the developing global monetary structure apparently envisaged in a new Trumpian world and its potential impacts that a preference for the use of lightly stablecoins (in comparison with the regulation of commercial banks) as private money channels, perhaps eschewing the integrated use of wholesale CBDC, (wCBDCs)—these are effectively tokenized central bank reserves (tCBRs), see BIS definition [10]—as undergirding fiat currency (including the US dollar) final settlement of payments at global level, as they do *within* monetary jurisdictions.

2. Digital payments, tokenization, and distributed ledger technology

2.1 Digital payments

There is little doubt that progress on the digitization of financial payments has been made in the last decade, both nationally, and increasingly in terms of cross-border transfers. Financial markets have benefitted in relation to lowered costs and risk reduction. One example is the enabling of algorithmic trading on foreign exchange platforms. However, much remains to be achieved, especially in relation

overall trading efficiency, including overcoming access to securities trading and the inevitable legacy system barriers. With continuing reductions in the number of “correspondent banks” available internationally.

Hence, cross-border payments are still cumbersome, often slow, and, above all, costly, especially compared with the far speedier payments now made *within* monetary jurisdictions. Inadequate cross-border payments hamper the efficiency of global trading and international capital flows and hence impose cost constraints on global economic growth, facilitated by low-cost cross-border transfers. See high cost of cross-border financial transfers in Morgan [11].

Indeed, one of the G20’s primary objectives for this decade, set in 2020, is to substantially improve cross-border payment systems. The aim is to have retail cross-border transfers settle within a day and cost no more than 1% of the transaction value, see G20 roadmap in 2020 [12]. A key enhanced role for the Society for Worldwide Interbank Financial Telecommunications (SWIFT) messaging service is envisaged in this endeavour, see SWIFT progress and innovation announced in 2024 [13]. However, the domination and manipulation of SWIFT by the US for geopolitical ends [14] has concerned other countries, especially to those countries allied to the BRICS group. Nonetheless, the Chinese CIPS system, sometimes advertised and used as an alternative to SWIFT, for the time being is still reliant on SWIFT for outside international transactions.

A number of projects have been initiated by the Bank of International Settlements (BIS), involving central banks, commercial banks, and other relevant major financial players. Some of these are briefly discussed in following sections and in the penultimate section (Page 16 ff) ledgers and are also referenced. Two others are not discussed, but are also referenced (Project Helvetia [15] and Project Jura [16]).

2.2 Tokenization

Further progress on digitization, especially the opportunities presented by *tokenization*. In combination with DLT, offers a new way forward for global assets trading and payments. Tokenization, in digital terms, may best be defined as the digital representation of assets, including money, established for operational purposes on programmable distributed ledger technology platforms [6]. (A bank note is also a token, a *physical* representation of a fiat currency.) Stablecoins are another form of tokenized currency/assets. Another form of currency/asset, tested in projects, are tokenized commercial bank deposits. The advent of a more substantial use of stablecoins, and the prospects of unified ledgers, see below Page 9, may accelerate this tokenization development.

2.2.1 Tokenized commercial bank deposits

From a private sector standpoint, a recent article by Marcy Dumitrescu, Senior Product Manager, R3, indicates the potential for tokenized commercial bank deposits in a global context [17].

Tokenized deposits are the next evolution of digital money in financial markets, enabling banks and other institutions to optimise liquidity and treasury management, enhancing their capital efficiency to unlock significant value. Tokenized deposits are *digital representations of bank deposits* recorded on a *DLT or Blockchain*, issued and maintained by depository institutions. Tokenized deposits support banks in providing their clients with:

- *Faster and more efficient transactions*—Tokenized deposits enable real-time, programmable settlement, reducing delays and enhancing liquidity management.
- *Reduced counterparty risk*—By minimising reliance on traditional payment rails, tokenized deposits mitigate counterparty and settlement risks.
- *Enhanced security and transparency*—Built on secure, permissioned DLT infrastructure, tokenized deposits provide improved auditability and regulatory compliance while ensuring privacy and control.
- *Greater security and trust*—Improved transparency helps protect customers from fraud and financial crime, ensuring safer and more reliable transactions.

Tokenized deposits also have the potential to significantly advance the repo market, enabling banks to bypass traditional payment rails, delay final settlement, and facilitate atomic transactions on their preferred schedule. In the traditional repo market, every transaction *must be settled before the next one can take place*, meaning that liquidity is locked up until payment processing is completed. *Delaying final settlement with tokenized deposits* allows banks to optimise liquidity and execute repo transactions more flexibly throughout the day. This flexibility and optimization support both internal and client trading activity, with reconciliation over traditional rails consolidated into a single transaction at the end of the day, reducing counterparty and settlement risk, as well as generating potential cost savings [17].

Tokenization of payments structures, including tokenized commercial bank deposits, is important to facilitate the burgeoning development of trading with tokenized financial assets. The application of these technological innovations to cross-border trading, coupled with the use of wCBDCs/tCBRs offers an effective means—independent of SWIFT—of automating cross-border transactions, including cross-border payments.

In 2024, the BIS announced Project Agora. This project not only brings together seven central banks—Bank of France (representing the Eurosystem), Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England and the Federal Reserve Bank of New York—but also seeks to work in partnership with a wider and large group of private financial firms, convened by the Institute of International Finance.

The announcement came on the heels in 2024 of the findings of SWIFT (The Banker 2024), from the second phase of its industry-wide sandbox testing on its central bank digital currency interlinking solution for cross-border payments.

In a press conference held on April 3, 2024, Cecilia Skingsley, head of the BIS Innovation Hub, described the initiative as “an exciting new project which will experiment with how tokenisation can improve the global monetary system.” She went on to say that the BIS is starting with a use case that is “near and dear to the BIS” on cross-border payments [18].

“We believe that tokenisation is the next frontier in terms of the digitalisation of money and payments. Agora is the most ambitious project launched by the BIS Innovation Hub so far,” said Skingsley. “We will not just test the technology, we will test it within the specific operational, regulatory and legal conditions of the participating currencies, together with financial companies operating in them” [18].

The project builds on the unified ledger concept proposed by the BIS and will investigate how tokenised commercial bank deposits can be seamlessly integrated with tokenised wholesale central bank money in a public-private programmable core financial platform.

Speaking at the same press conference, Hyun Song Shin, BIS economic adviser and head of research said an important guiding principle for the BIS is the singleness of money, the idea that a payment should go through at the point of transaction irrespective of the means of payment used, whether as cash, by an electronic transfer from a bank, or from a payment app on a phone.

“A dollar is a dollar, a euro is a euro, a pound is a pound, and so on,” he added.

“We’re so used to the singleness of money that we take it for granted, but it’s worth reminding ourselves that it holds because of the settlement function of the central bank” [18].

Shin went on to say that in the context of Agorá, tokenisation is not merely the digital representation of claims, it is a digital representation which also incorporates the rules and logic governing transfers.

“Tokenisation of deposits and wholesale central bank money means that both the primary means of payment, as well as the settlement function of central bank money, can be integrated seamlessly on the same programmable platform,” he added [18].

2.3 Distributed ledger technology (DLT)

The advent of distributed ledger technology (DLT) has facilitated a number of initiatives as it has been applied to both private and public development in the financial and monetary spheres, especially in cross-border payments and, increasingly, cross-border assets trading. Progress on digitization, including crypto-assets, stablecoins, and CBDCs has been facilitated by the use of this technology, sometimes referred to blockchains, though blockchains are, in fact, a subset of DLT. For a detailed discussion of distributed ledger technology and blockchains in Lloyd [19]. A comprehensive technical discussion is to be found in Kannengiebr and Lins [20].

The definition of DLT has been provided by the Committee on Payments and Market Infrastructures (CPMI) in 2017.

“DLT refers to the technological infrastructure and protocols that allow simultaneous access, validation and immutable record updating to a synchronised ledger that is used by a network of participants that may spread across multiple entities and/or locations. In the context of payment, clearing and settlement, DLT enables entities, to carry out transactions without necessarily relying on a central authority to maintain a single ‘golden copy’ of the ledger” [21].

Blockchain, a specific type of DLT, was developed in 2009, it establishes a group of stakeholders, who may or may not be unrelated, but who might all have a valid reason to alter their shared data held on the data network. The validated network participants—validated by “proof of work,” in the case of Bitcoin, and by “proof of stake” in the case of Ethereum and other crypto-assets—will agree and maintain a single dataset across an entire network. (see Lloyd [19]).

The other key characteristic in the case of a blockchain is that the data are grouped into sets called “blocks.” Once validated, each data block is linked or “chained” to the previous blocks to form a historical record or “blockchain,” giving this type of distributed ledger its name. The validation of each dataset/block is made cryptographically, enabling all registered stakeholders to confirm acceptance. It is important to recognise that blockchains, unless modified, are self-contained and sealed to any participant other than those validated by “proof of work,” Bitcoin or “proof of stake,” later versions of Ethereum. Trust in these systems is *embedded and sealed within* the blockchain.

Trust is hence provided as an *internal* feature for the validated participants. Trust is not a feature present in any outside interaction with outside actors. There are attempts to use algorithmic approaches, utilising past externally-generated data, to provide trust for blockchains where, necessarily, interaction with real world organisations occurs. Solutions to the so-called “oracle” problem, providing a trusted interaction, have not achieved sufficient viability. Given the need for CBDC interaction with outside entities, trust for central banks and other participants such as commercial banks needs to be provided elsewhere other than *within* the DLT database.

From a CBDC perspective, the DLT consensus mechanism also needs to provide *finality* in the execution of transactions. After total finality, that is, non-reversibility/immutability, has been reached across the validating network nodes, committed transactions cannot be retroactively changed. One issue is that such finality is problematic, except with a comparatively small set of validating nodes. Here, with the tCBR data provided by a modest number of already trusted, regulated commercial banks, as in the contemporary monetary systems, this is not a problem. The network of nodes is relatively small, and scalability is not therefore an issue. Bitcoin, on the other hand, has unlimited, though in practice not infinite, number of validated participants (by “proof of work”).

In the case of a financial payments network, including cross-border payments, each payment, once transferred and validated as a correct payment between verified payers and payees across the network, is recorded and a linked/chained historical dataset is formed and retained on the ledger. In most cases, the involvement of regulated commercial banks together with central bank means that trust is verified outside the system, whichever database platform is used [19].

In the monetary architecture established in fiat monetary jurisdictions, central banks, in combination with regulated commercial banks, ensure for all financial transactions both clearance and, crucially, final settlement of all financial transactions.

2.4 Permissioned and permissionless blockchains

Permissioning refers to the rules governing who can participate in running the network platform. Despite the terminology such DLT networks are still open, transparent, and distributed. Permissioned (private) DLT networks are preferred by central banks. The aim is to ensure that the validated participants, usually central banks, commercial banks, and other regulated financial organisations are linked in a peer-to-peer nodal structure in a decentralised (or partly decentralised) environment.

Permissionless (public) environments, by contrast, open themselves up to broader resources, a large pool of participants, continuous innovation and considerable cost

savings. Most stablecoins are established on this type of network. The challenge for such DLT networks will need to ensure that the digital tokens involved are secure to use for transaction purposes and will provide final, immutable settlement within the network. It is whether the requirement for final, *immutable* settlement is met by many of the permissionless DLT platforms that concerns central banks, given the need to ensure global financial stability. It has been suggested that there are design mechanisms that may provide similar validation as is achieved by permissioned networks. The validation would involve, as is done on the XRPL blockchain created by Ripple [22]. The methodology is to operate an internal/external validation process via the complete range of network nodes, validating the potential members via a past performance referencing system. However, the problem of ensuring immutability of settlement remains a problem, to which it is not clear there is a technical solution. It is possible that this uncertainty on decentralised blockchain ledgers may not be seen as a legal problem in some monetary jurisdictions. The position of the US on this issue is currently unclear.

The global use of such open DLT networks offers the ability to develop a developing ecosystem of tokenized trading and payments, eventually linking the use of private settlement currencies, that is regulated stablecoins and tokenized commercial bank deposits, and public (state) tokenized central bank reserves, connected across unified ledgers. This structure of an ecosystem—with open, transnational, and decentralised programmable DLT platforms—would present a secure future for the next generation of global assets trading and payments systems, providing global financial stability.

Different DLT platforms are likely to coexist and, ideally, should be interoperable. A useful article on the various issues involved with permissioning and interoperability is provided by Rubin and Arredondo [23].

2.5 Unified ledgers

A DLT unified ledger may be defined as one that combines multiple ledgers into a single, shared ledger, achieving interoperable transactions across different financial platforms. For a full accounting definition and comparison with traditional modular ledgers, see Aquila [24].

Various central banks, encouraged by BIS, are exploring the development of DLT-based “unified ledgers” that bring together tokenised assets and money. The argument is that a single infrastructure is needed to ensure financial market integrity and maximise the technical advantages of one platform.

In the past, the US has been wary of engaging in the variety of BIS and central bank-led global CBDC projects examining the potential for translating the use of fiat currencies in the context of cross-border trade and payments, utilising *wholesale* CBDCs across unified ledgers as indicated by the BIS [25] and also by Morgan [26]. Whether this involvement will continue seems unlikely, given the position of the Trump administration.

US financial corporates, notwithstanding US political scepticism, are involved in private sector innovation in the areas of tokenized assets trading and DLT-based payments infrastructures, including unified ledgers. The programmability of DLT platforms, within regionally and internationally based trading and payment environments, using stablecoins, is already operational.

Interestingly, the official reluctance to adopt multi-jurisdiction unified ledgers may lead, in some cases, to avoiding, at this stage, decentralised DLT, in favour of a centralised approach. The Buna project (Buna.Co) [27] is a Middle East's cross-border

payments initiative that has eschewed DLT and set up regional network based on a central bank “standard” closed, *centralised* system. In this manner, it establishes a centralised unified ledger, built on existing real-time gross settlement platforms, across the participating central banks. The project is owned by the Arab Monetary Fund and supported by the regional Arab central banks and involves commercial banks in the area.

3. Stablecoins in cross-border trading and their regulation

Stablecoins are established on permissionless (public) blockchains, on program-mable platforms and are backed by reserves, including cash and other safe assets, such as Treasuries, to ensure that they remain “pegged” to the selected fiat currency, in almost all cases the US dollar. Trust in this context is essentially *embedded* within the blockchain and validated by the adequacy of the reserves held. The use of DLT and blockchains by central banks tend to employ permissioned (private) DLT structures where trust is granted *external* to the DLT structure, such as to tightly regulated commercial banks. In a global trading and payments context, trust is of crucial importance. Although trust can be provided via private money channels, such as stablecoin platform networks, the still unresolved issue is whether global financial stability can be achieved, except via the “undergirding” of private money systems by tCBRs as argued in the previous subsection.

There is increasing evidence, see BIS below [28], of the use of stablecoins in cross border trading, including by large international companies, see the article by Liao and Caramichael in 2022 [29]. Of itself, contained within these firms using DLT program-mable platforms, it is not necessarily a major problem. However, it appears that if its rate of growth is very high then it may pose a threat to global financial stability.

A recent investigation by BIS of the use of Ether, Bitcoin, and other stablecoins (such as USDC [30] in cross border transaction flows indicated the need to find new regulatory approaches to ensuring global financial stability in the new cross border monetary environment [28].

Our analysis indicates that policy measures designed to dampen traditional financial flows may have limited impact on constraining cross-border crypto activity. Yet, as crypto assets become more integrated with mainstream finance, understanding the systemic risks and potential contagion effects between these markets will be essential for policymakers and market participants alike. At the same time, the socio-economic implications of increased crypto adoption, particularly in emerging market and developing countries, warrant a deeper examination. This includes assessing the impact on financial inclusion and economic stability and the potential for crypto assets to serve as a hedge against local currency volatility and weakness [28].

The EU has already regulated stablecoins, together with other crypto-assets in the Markets in Crypto-Assets Regulation (MiCA) see ESMA [31], though not distinguishing stablecoins as potential alternative settlement currencies, by effectively subjecting them to strict bank regulation, aiming to avoid competition from US dollar-linked stablecoins from competing with a digital euro if and when established. However, despite concerns expressed by the ECB about stablecoins, the European Commission has recently eased the application of the MiCA rules [32].

The UK position is not yet clear but is moving closer to the EU position than the US approach. Andrew Bailey, Governor of the Bank of England, recently raised concerns

about the domestic issuance of stablecoins. However, unlike the EU, he cast the doubt of whether the UK should adopt a retail CBDC, suggesting instead that a better defence against stablecoins might be tokenized commercial bank deposits [33].

The US, somewhat belatedly, is preparing legislation on the stablecoins, treating them differently from crypto-assets. The Genius Act is currently going through Congress. The Act passed its final Senate vote on June 14 by a substantial majority, before being passed back to the House of Representatives. In effect, the US approach is to make regulated stablecoins the alternative to CBDCs in the US. However, the use of stablecoins in global assets trading and payments means that this will have implications for both innovation and the development of the role of tCBRs in this arena.

Bloomberg's recent 2025 comments [34] on the proposed US legislation are correct to suggest that how Tether—as an issuer of USDT coins, having by far the largest share of the stablecoin market—is treated may be a good test of the strength of the legislation. As they suggest, the legislation, properly, requires stablecoins:

to be fully backed by cash and safe assets (such as short-dated Treasuries or government money-market funds). That will help ensure holders can always redeem tokens. The bills also make issuers subject to the Bank Secrecy Act and to anti-money-laundering regulations.

So far so good. But legislators surely know that Tether accounts for more than 60% of the stablecoin market and has had multiple run-ins with state and federal authorities, and has never been audited. Its reserves more Treasuries than Germany's. It is USDT coins have been seized and forfeited in cases involving fraud, terrorist financing, sanctions violations and other criminal activity. (The company denies any wrongdoing.)

One might argue that such risks are part of the innovative process. But the more intertwined Tether and its competitors become with the broader financial system the greater the risk that a crypto crisis may spread.

With that in mind, Congress should clarify exactly how these proposals will deal with Tether. Although both bills would allow regulators to sign off on foreign issuers if they are subject to “comparable” rules overseas, the big question is how strictly the law will deal with those that do not comply [34].

It may be that Bloomberg is, at this stage, being too alarmist. However, the market dominance of Tether as the issuer of USDT is extremely concerning. The positive attitude of US authorities to stablecoins, and crypto generally, should not lead to weak legislation in regulating stablecoins as potentially major private money channels.

As importantly, the regulation applied to stablecoins should be less restrictive than that applied to banks. The quid pro quo is that stablecoin issuers should not be permitted to become involved in credit creation, as are commercial banks together with the direct link with the central bank to provide clearance and *final* settlement.

However, the discussion in the US, has intensified under Trump: His January 23rd executive order, the potential implications of the Genius Act, and Trump's unnerving over-enthusiastic endorsement of all things crypto is concerning.

Apparently, according to Bloomberg, a key official whose job is to consider the digitalisation of money at a developed world central bank returned from the Spring International Monetary Fund-World Bank meetings with a deep sense of unease.

While unperturbed by the customary condescension from ‘crypto-native’ digital assets disruptors at closed-door meetings, this person instead came away profoundly unsettled from similar gatherings of central bankers discussing the potentially radical implications of the forthcoming Genius Act – the US stablecoin bill expected to become law in 2025 [34].

Another key issue for financial stability and the preservation of universal trust in fiat currencies rests on whether or not stablecoins have access to central bank reserves and the conditions applied to their issuers. Currently, the tight regulation applied to commercial banks not only allows access to central bank reserves but also limits to regulated banks the ability to create credit. Given the lighter regulation applied to stablecoin issuers, they should not be able to create credit. In other words, they would become “narrow banks,” allowed to lend, but only to the extent of their deposit base [29].

The current trajectory of Trumpian-led US policy in this complex and sensitive area of the fiat monetary system is explored further under the penultimate section below (Page 16 ff) examining three global scenarios, including one considering how Trumpian policies on the issues of stablecoins and of crypto-assets may impact on the global monetary system.

The unresolved issue of the differing US and EU regulatory approaches, as argued in the next section, is that, for global progress on assets trading and payments, there is a need for significant international regulatory conformity.

4. Prerequisites for successful tokenisation of assets trading

Noting the above comments on stablecoins, a key prerequisite is to ensure that there is an appropriate international regulatory framework both to foster innovation and to ensure financial stability. Without it, innovation can lead to a reduction in the security, efficiency, and stability of the developing global monetary ecosystem. It is worth taking into account the positioning of central banks on the issue of tokenization in relation to asset trading payments. The European Union and the UK are adopting approaches on the matter that are diverse in form yet similar in substance with their pilot tCBR regime and digital securities “sandboxes,” respectively. Unfortunately, at present, the US position on this issue appears to be more concerned about encouraging private money channels with perhaps less concern about global financial and monetary stability or cooperative international regulation, especially given the pivotal monetary guarantor of the US and the Federal Reserve as indicated by Merhling in 2015 [35].

It is important to recognise that regulatory interoperability as well a technological interoperability is required. Moreover, global financial stability is probably best achieved by proving access to validated clearance and final, immutable financial settlement of the asset trades involved. The aim should be to achieve a combined and trusted digital ecosystem for tokenized trade and payments, involving both the private sector and the public sector in the form of state regulation and central banks.

Currently, regulation and legal compatibility appears to be moving only slowly at international level. Attempts to achieve international standards via existing international standards bodies are likely to be a time-consuming and probably fruitless exercise. An approach based on mutual recognition of national or preferably regional permissive standards may be the most efficient path to achieving the desired international regulation.

Pursuing such a path to mutually accepted standards while also establishing, at the same time, a public payments platform, using tCBRs, would provide a globally stable network structure and framework, also involving stablecoins, tokenized commercial bank deposits. Such an approach would provide the essential universal trust and clearance and final, immutable settlement to enable a variety of private players to establish their DLT asset-trading superstructures, on top of tCBR payments platform(s) and unified ledgers.

4.1 Regulatory compliance and interoperability

Without international public co-operation, the development of new private market infrastructures, is likely to lead to an unregulated fragmentation of the global ecosystem, dominated by a few major private players, and a potential threat to global financial stability.

Currently, regulation and legal compatibility appears to be moving only slowly. Attempts to achieve international standards via existing international standard bodies is likely to be a time-consuming and probably fruitless exercise. An approach based on mutual recognition of national or regional permissive standards may be the most efficient path to achieving the desired international regulation.

Pursuing such a path to mutually accepted standards while also establishing, at the same time, a public payments platform, using tCBRs, would provide a globally stable network structure and framework, also involving stablecoins, tokenized commercial bank deposits. Such an approach would provide the essential universal trust and clearance and final settlement to enable a variety of private players to establish their DLT asset-trading superstructures, on top of a tCBR payments platform(s). The next major section of the article explores how this structure might be developed.

4.2 Technological interoperability

Regulatory interoperability is a necessary condition for stability and integrity of trading. However, notwithstanding the ability and desirability of private sector innovation in this rapidly emerging environment, it is also the case that technological interoperability is also required for development of efficient systems. This is especially the case at the international level, with a variety of proprietary private programmable platforms needing to be able to work with each other. These DLT data networks can be permissioned or permissionless. Generally, decentralised permission networks are preferred, especially by central banks as they provide trusted governance, security, and risk management. In practice, the issue of choice is about governance.

There will be a requirement, at this stage, in the development of a coherent system for private and public cooperation to encourage the technological compatibility of innovative systems to evolve. Competition between systems and platforms will be important, but this stage should probably be followed by a limited number of optimum interoperability solutions emerging.

5. A potential global digital assets trading and payments ecosystem

Already there are a considerable number of cross-border tokenized *projects* involving tCBRs. Three of these projects, mBridge [36], Nexus, and Agora (see References),

are briefly described below to provide a useful picture of the likely future of tokenized cross-border financial transfers and assets trading, and how this preparatory work is helping to usher in a digitised and tokenized global trading and payments ecosystem.

These projects involve the BIS, central banks, commercial banks, and large financial companies. The projects demonstrate how the advent of tokenization is accelerating the development of a global ecosystem, underpinned by tCBRs to provide final, immutable payments settlement, potentially involving commercial bank deposits and stablecoins in trading a plurality of tokenized financial assets on programmable distributed ledger platforms.

There is also the progressive development of the ubiquitous SWIFT network, reported in 2024 [13], indicate the rapid progress that is being made to establish integrated public cross-border payment channels involving central banks, commercial banks, and other financial organisations. Although not yet fully operational globally, the beginnings of such an empirical international development are already evident and will emerge over the next few years, spurred on by private sector tokenization development and trading. A third on-going project, Agora, is indicative of the potential global reach of the technological, operational, and legal experimentation taking place.

There is already private sector trading of tokenized financial assets taking place, using stablecoins (such as USDC) and intermediary trading and payment private DLT platforms, such as those developed by Stellar, Ripple, and R3. These trading activities are processed across these networks facilitated by a shared synchronised ledger, distributed via the network's nodes, other platforms may be based on permissionless blockchains.

Extensive global coverage of tokenized assets trading and tokenized payments and acceptance is likely also to require the involvement of tCBRs, to provide the requisite clearance and final settlement of payments, and universal trust. Joint development of a global ecosystem, involving both public sector and private sector participation, stablecoins, and CBDCs, is a desideratum. See Zelmer and Kronick [37].

6. Geopolitical trends

The development of a widespread digital geoeconomic asset trading and financial payments system has considerable implications for the wider geopolitical environment that this chapter now addresses.

There are three principal areas of concern and contention. First, the increasing number of private money channels, providing not only digital ledger technology and tokenized trading platforms but also clearance and internalised final settlement facilities within blockchains. The issue here is the potential impacts of global financial stability. It is for this reason that the private innovative development is accompanied by a number of important BIS and central bank projects involving the use of tCBRs. These projects, involving the participation by commercial banks and other financial players such as investment banks, point the way to a public/private global partnership approach to the development and secure expansion of tokenized financial assets trading and payments ecosystem.

Second, the developing division of the world into four major geoeconomic trading blocs: East Asia, Europe, the US, and the Global South, represented to an extent by the BRICS Plus group. Albeit with some divisions within these four blocs, this division

is leading to the gradual development of trade invoicing and settlement in various fiat currencies, rather than the US dollar. Indeed, beyond even these four broad goods trading blocs, bilateral trade invoicing in many individual fiat currencies has become prevalent as indicated in an article by Arslanalp and Eichengreen et al. in 2021 [38]. Hence, a *gradual* erosion of trade-invoice settlement using the US dollar. Nonetheless, the dollar *currently* still represents the main trading and settlement currency—notwithstanding the 20% plus share of the euro. Given its extensive use and liquidity, and its relative global overall dominance is not likely to be threatened any time soon.

Third, the short-term uncertainty and potential longer-term instability of global trading and monetary relationships created by the unpredictable policies of the Trump administration, especially, in the context of the global trading and payments area that is the subject of this chapter. The final shape of the expansion of the use of soon-to-be regulated stablecoins into the global trading and payments arena is not yet known. However, the preference of the US—already exhibited prior to Trump’s second term see speech by Fed. Governor Waller in 2021 [3]—for the suggested equivalence of private and public, fiat currency channels and the netting, clearance and final settlement structure is concerning in a global context.

In relation to the substantive trust issue, although private money systems may be sufficient to provide an adequate level of trust for the network participants as far as payment clearance and settlement is concerned, they cannot provide the *universal level of trust* provided by advanced fiat currency systems within monetary jurisdictions. The role of strongly regulated commercial banks, as private money channels, together with central banks, *within* the existing fiat monetary systems is crucial. A situation leading to the development of independent private money payment silos across the world, though there may be limited interoperability with lightly regulated stablecoins, is likely to lead to global financial instability. Such an ecosystem is unlikely to provide the requisite universal trust across the complex international trading and financial system.

The main trends involved may now be explored via three potential global development scenarios. Each of the scenarios are based on existing developments that all have some momentum and where major promoters—central banks supporting tCBRs; BRICS payment system commitment; Trump administration support for US private stablecoin—are committed to moving forward. It is important to recognise that the three scenarios are not alternatives. Rather is the issue as to how and to what extent they will interact and hence influence the development path of the global ecosystem over the next 5 years.

6.1 Supporting existing trends of central bank orthodoxy: Scenario 1

6.1.1 Action at international level

Currently, a global unified payments ledger does not yet exist. However, one international project, supported by the BIS and a group of important central banks is exploring how such a global unified ledger might be developed, in the context of a broader global trading and payments ecosystem.

At an international level, further development of cross-border payments is being pursued with Project Agorá, based on a DLT approach. This project, launched in April 2024 by the BIS, brings together seven central banks, including Banque de France, representing the Eurosystem, and the Bank of England, among other public and private financial institutions.

The project incorporates central banks, including the Federal Reserve Bank of New York, Bank of England, Bank of France, Bank of Japan, Bank of Korea, Bank of Mexico and the Swiss National Bank.

These banks will engage with private sector banks like Citi, HSBC, Deutsche Bank, Standard Chartered, Lloyds Bank and global infrastructure providers such as SWIFT, Euroclear, SDX, Visa and Mastercard, all brought together by the Institute of International Finance (IIF).

The project will explore further enhancements of the monetary system and provide new solutions potentially using smart contracts and programmability, while maintaining the two-tier structure of the monetary system—central bank money and commercial bank money. The testing of a possible global unified ledger is at the core of this BIS-led project, with the design phase having started in 2024.

The project is ambitious. Even if the technological and operational conceptualization proves feasibility and robustness, especially in relation to global interoperability, there will also be legal and political challenges for any implementation of such an international structure. The participation of the US dollar in any developed system will be important if a global focus is to be comprehensive. Political attitudes in the US, even prior to the current Trump presidency, have been relatively negative. Nonetheless, Agora's successful prosecution, at a minimum, may be to demonstrate the technological and financial feasibility of a truly global system and to produce draft standards of regulatory interoperability.

Another interesting major regional project is Project Nexus. The five central bank partners in Project Nexus—Indonesia, Malaysia, the Philippines, Singapore and Thailand—have agreed to establish a managing entity, the Nexus Scheme Organisation (NSO), which will manage the project in its live implementation stages, in Singapore.

Since 2022, the BSIH Singapore Centre has worked with the central banks and IPS operators of the five central banks to evaluate the model against the reality of their IPS. The project team also consulted with central banks, standard-setting bodies, IPS operators, and commercial banks from around the world to validate that Nexus is scalable and interoperable with IPS beyond those five countries.

In over 70 countries, today, domestic payments reach their destination in seconds at near-zero cost to the sender or recipient, thanks to the growing availability of instant payment systems (IPS). Connecting these IPS to each other can enable cross-border payments from Sender to Recipient within 60 seconds (in most cases).

Rather than a payment system operator building custom connections for every new country that it connects to, the operator can make one connection to the Project Nexus platform. This single connection allows a fast payments system to reach all other countries on the network. Nexus could significantly accelerate the growth of instant cross-border payments. The project team also consulted with central banks, standard-setting bodies, IPS operators and commercial banks from around the world to validate that Nexus is scalable and interoperable with IPS beyond those five countries.

6.1.2 Action at European level

At the European level, the potential of a DLT-based European unified ledger that would include tokenised assets while retaining a two-tier monetary system is being

explored. A further project is pursuing a similar approach to a potential European unified ledger. Led by the Banque de France. This two-pronged approach to unified ledgers, indicates that the evolution towards a unified global may be approached by initially creating an inter-connected multi-fiat currency layer, given the absence of a widely-accepted global unit of account, save for the limited issuance of International Monetary Fund (IMF) Special Drawing Rights (SDRs).

The European Central Bank is running a twin-track approach through projects at Deutsche Bundesbank and Banque de France, and Banca d'Italia with the former creating a bridge between the existing Target 2 RTGS arrangement and DLT-based tokens; the latter creating a DLT-native setting for DLT-based tokens to be settled atomically in tokenised wholesale CBDC/tCBRs.

Various solutions for the settlement of tokenised assets in central bank money are being tested. The Eurosystem banks' partners Banca d'Italia and Deutsche Bundesbank have put forward different proposals regarding the settlement of tokenised assets in ECB central bank money.

It will build on the Eurosystem's exploratory work on new technologies for wholesale central bank money settlement, conducted between May and November 2024. This work gave 64 participants – comprising central banks, financial market participants and DLT platform operators – the opportunity to conduct over 50 trials and experiments. Trials included actual settlement in central bank money, while experiments were tests with mock settlement [39].

The approach is cautious, as Banque de France indicates.

Of course, none of these projects intends to abruptly replace the current infrastructures that have been meticulously developed and already provide state-of-the-art services for most use cases in payments and securities settlement. However, we need to plan forward and ensure that our infrastructures are not only up to date but future-proof [40].

Some of these European regional projects are aimed at piloting a global trading and payments platforms, establishing regional DLT network platforms that utilise a number of connected payments platforms, utilising a limited number of fiat currencies to provide clearance and final settlement.

There are also other regional pockets of progress, one eschewing DLT, as already indicated above (page 9), the Buna project [27]. This project is a Middle Eastern cross-border payments initiative, setting up regional network based on a central bank “standard” closed and centralised system. Hence, fiat currencies of the member countries are linked across a centralised unified ledger, built on existing real-time gross settlement platforms, involving the participating central banks. The project is owned by the Arab Monetary Fund, supported by the regional Arab central banks and involving commercial banks in the area.

6.2 Implications of a changing trading world and BRICS+: Scenario 2

Partly linked to the trade vision of the Trump administration and its actions, but also because of secular trends in global economic development and trading relationships, we appear to be moving towards a quadripartite global trading structure (the US, the EU, Asean, and the BRICS), with a similar structure of evolving supply networks. The size of the South-East Asian economy is impressive, ASEAN+3

(China, Japan, and South Korea) account for 30% of global GDP, 28% of global trade, and 20% of inward FDI [41]. The BRICS grouping is expanding via new members (BRICS+ has 11 members) and associate countries and includes some key countries in the Global South.

It may also be argued that Russia and the Eurasian bloc suggests a further global trade grouping. However, *in relation to trade finance invoicing*, it is not unreasonable to suggest that this Russian-led grouping may be subsumed under the BRICS plus umbrella.

China has now taken over from the BIS as the leader of the mBridge project, involving the central banks of China, Thailand, the UAE, and the Hong Kong MA, has been running since 2021 (and since 2024 the Saudi central bank).

The project is a cross-border, decentralised, multiple CBDC DLT platform that seeks to support real-time, peer-to-peer, cross-border payments and foreign exchange transactions. The aim is to provide a multipolar global financial system, where individual countries' digital currencies can play a much larger role in international trade, thus also avoiding use of the US dollar.

In 2024, at the BRICS annual meeting, such a cross-border payments network, even the limited to the adherents to BRICS would be transformative in shifting some significant trade finance from the US dollar, within this grouping.

The potential for using the latest DLT is relevant to the recent activity and monetary instruments development within the BRICS plus grouping as Michael Lloyd's BRICS 2024 annual meeting report indicates:

Given the collective scope of BRICS Plus, there are clearly divergent interests. Achieving consensus on any major geopolitical issue is going to be difficult as the issue of UN security council membership reform indicates. For this reason, it is the development of technical monetary and trade initiatives where one should look for BRICS progress [42].

For some BRICS states, such a digital payments system would offer a path to new markets. For others, it would permit the circumvention of US sanctions. The BRICS Pay initiative from 2018 first proposed linking the credit or debit cards of BRICS citizens to online wallets, accessible 24/7 for payment via a mobile application installed on their smartphones. The pilot project started in South Africa in early April 2019 and has intensified. The commitment is demonstrable. In 2020, the Russian BRICS Presidency proposed the idea of a commercial "BRICS Pay" for "BRICS" countries for the consideration of the BRICS Business Council as reported by Lloyd in 2023 [43].

There is no substantial direct challenge from the BRICS to the US dollar in the form of a supplanting of the hierarchical monetary structural position of the dollar at its apex. Nonetheless, there are various initiatives that are being pursued by the BRICS that are likely to attempt to partially supplant the role of the US dollar in both bilateral trade finance between BRICS countries and in supplanting the role of the US-dominated SWIFT global financial payments system. The earlier launched BRICSPay initiative is utilising the results of mBridge to develop the system for wider trade invoicing among the BRICS+ members.

As Lloyd suggests:

The biggest advantage of BRICS Pay is in developing an integrated network payment system, using distributed ledger technology (DLT). Such a structure would make possible the use of BRICS members' national digitised currencies used for external payments, over the DLT network, and thus avoiding the use of the US dollar for trade

payments. Currently, external settlements between BRICS members still require a conversion into US dollars, which requires the engagement of US banks. The BRICS Pay system would thus allow the members to reduce their dependence on Western-dominated international systems [42].

Two aspects of this technological initiative are worth noting. First, that development of tCBRs in payments systems is likely to be *regional* in terms of digital currency areas. Second, given the key role of China in the BRICS digital payments system, and their long-standing support for a global unit of account, independent of any single country, it is highly unlikely to support any suggested attempt to establish BRICS+ reserve currency. What this putative development suggests is that this BRICS+ evolving payments initiative is paving the way for using the technological opportunities discussed in this chapter to reduce significantly reliance on the US dollar, and initially on the use of the SWIFT network. This task involves, however, a difficult, long-term commitment and is not an imminent development.

6.3 A geopolitical payments future in a Trumpian world: Scenario 3

The Trumpian global trading vision—which may become more entrenched than some observers are assuming—will have implications for its impacts of the above scenarios. In 2023, the Biden Administration initiated a foreign policy process that it termed the New Washington Consensus (NWC), for definition see Lloyd article published in 2025 [44]. The aim was to establish a US-led alliance of Western liberal democracies, to set against a supposed autocratic alliance led by China, including *inter alia* Russia, Iran, North Korea and other autocratic countries. Trump may agree with some elements of the NWC, but *not* the idea of any quasi-formal alliance with other Western nations, the US under Trump is likely to become more isolationist, demanding “tribute” from its allies for protection [44].

The advent of the Trump presidency, including Trump’s own involvement with crypto-assets, only strengthens the US preference for private money channels and reinforces doubts on US participation in international government fora on issues of global regulation of private money channels.

It is also important to recognise that even regulated US stablecoins will still represent private money channels. They will not be equivalent to the issued fiat currencies of *regulated commercial banks* whose issued currencies become fiat currencies as a result of the banks’ access to central bank reserves, so providing full clearance and final settlement. It is this fiat currency system within monetary jurisdictions that provides the universal trust that enables a functioning monetary economy and society to function. This position was only arrived at over a period of the past 200 years, leaving behind earlier unregulated and uncoordinated independent private banks.

It would, however, be possible for stablecoins, or at least the dominant issuers, to be given access to central bank reserves, this may happen in the US. It may be argued that such access would simply increase the number of “banks.” The problem would be that, unless the stablecoin issuer’s regulation was as tight as that of the current commercial banks, then there would be direct competition between stablecoins and commercial bank deposits, echoing the concern that has been expressed by some commentators have expressed about retail CBDCs. Moreover, it is not clear in the US whether stablecoin issuers would be permitted to create loans, beyond their deposit base, despite being less strongly regulated than commercial banks, for a discussion see Lloyd [19].

At a global level, there is a need for any putative global ecosystem to establish the same level of universal trust between monetary jurisdictions as within those jurisdictions. Such an ecosystem may only be credibly established with the participation of tCBRs, providing the underpinning payments platforms.

There is a serious danger that the current US position may prevent such a desired outcome. Attempts to trade in financial assets may then lead to emerging global financial uncertainty and instability. Trump has already ruled out any idea of the US establishing a US retail digital central bank currency and he may also rule out wholesale US digital central bank currency participation in global payments. In practice such participation, via supporting US-regulated stablecoins would further strengthen the role of the US dollar in assets-trading, so he may not.

As ever in the Trumpian world, we are left with a high degree of unpredictability. It might be argued that the above potential problems can be ignored. Such an insouciant argument ignores the crucial fact of the pivotal role of the US dollar in monetary and trading terms and the role of the US central bank (the Fed.) as, effectively, a global central bank, in addition to its internal US monetary jurisdiction role.

Trump issued an early executive order [45] that challenged the view of its previous chair, Gary Gensler—that crypto-assets, including some stablecoins—were to be regarded unequivocally as securities. Gensler resigned immediately. Under the new chair, Paul Atkins, appointed by Trump, the SEC US regulatory role as far as crypto-assets are concerned is currently under review as indicated by Ralhi, Georgetown Law School [46]. It appears likely that any new SEC regulatory regime will be less severe than that under Gensler. However, though the regulatory balance may shift to being in favour of innovation, risks to investors will still have to be assessed and investors protected. The risks were clearly demonstrated in the Terraform stablecoin case. The TerraUSD (UST) stablecoin protected its peg to the US dollar by an algorithmic system link with its governance token LUNA, which promised high returns, but the system collapsed, losing \$40 billion of its market value, resulting in a legal judgement against the company [47].

On the positive side, though somewhat belatedly, the US Genius Act—aimed at regulating stablecoins and stablecoin issuers such as Tether—is going through Congress. How far and well this legislation will ensure financial and monetary stability will depend on the final legal text of the act and how this will be interpreted by US regulators and US courts. It does appear that the Act, appropriately, separates the regulation of stablecoins as settlement currencies, from the plethora of speculative investment crypto-assets more widely.

If any potential concerns about adequate regulation in the crypto area could be restricted to the US, then it might not be a global problem. The difficulty is that despite Trump's apparent desire to isolate the US in some respects, it cannot be quarantined or isolated in the international trading or monetary terms. US policies and actions in the area of global monetary policy and the global monetary system affect all countries, given the omni-present role of the US dollar. Despite some movement away from the use of the US dollar in relation to trade invoicing and settlement, the US dollar remains at the apex of the global monetary system.

7. Conclusion

There are clear challenges, both to the private sector and the public sector in the developing global context of tokenized assets-trading and payments. For the private

sector, there are issues of technological interoperability for the many digital ledger technology databases and networks. Clearly, it will be important to preserve innovation, though it is likely that, over time, there are likely to be only a handful of major players, and here, there will be a need for compatibility. It is already the case that there are perhaps four dominant US stablecoins, with perhaps some question of the USDT issued by Tether being preponderant. This issue may be addressed by US legal regulation.

For the public/state sector the challenges appear to be considerable, especially given the need to ensure global financial stability. The main international organisations involved—the BIS, the IMF, and the World Bank—and perhaps notably the BIS, have all discussed the issue of the impact of private money payment channels in the context of global financial stability. There is a potential for the development of regional assets-trading networks underpinned by tCBR fiat currency unified ledger systems. Such regional network systems may likely involve both stablecoins and tokenized commercial bank deposits, combining both private and public sectors technologies.

There are also strong challenges for any attempt, for instance, by the BRIBS, to establish an alternative, widespread multi-currency platform cross-border payments platform to compete with an innovating SWIFT, given the liquidity and dominance of the use of the US dollar. The BRICSPay cross-border initiative is a potential, long-term challenger, though there are substantial geopolitical barriers to be overcome.

The future situation would perhaps be clearer were it not for the current uncertain global trading and monetary environments. The more likely evolution would appear to be towards the creation of a network of regional multi-fiat currency platforms with a foreign exchange conversion and central banks' payments layer, as suggested above.

This approach which is argued could provide a significant step forward towards a multipolar structure with regionalized operational systems. Such a regional DLT platform structure development would still leave the US dollar, including US stablecoins, as the dominant trading and reserve currency, but with a more balanced utilisation of other digitised fiat currencies, such as the euro, the yuan, and the yen.

Author details

Michael Lloyd
Global Policy Institute, London, United Kingdom

*Address all correspondence to: lcaeurope@btinternet.com

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Kregel J. The economic problem: From barter to commodity money to electronic money. In: Levy Institute Working Paper 982. 2021. Available from: www.levyinstitute.org/wp-content/uploads/2024/02/wp_982.pdf
- [2] Trump D. Executive Order on Digital Assets. 2025. Available from: <https://www.reedsmith.com/en/perspectives/2025/02/trump-signs-executive-order-digital-assets-american-financial-technology>
- [3] Waller F. Federal Reserve Speech by Governor Waller. Reflections on Stablecoins and Payments Innovations. 2021. Available from: <https://www.bis.org/review/r211119e.htm>
- [4] Project Agora. Top Commercial Lenders Join G7 Central Bank-Dominated Digital Currency Trial. 2024. Available from: <https://uk.finance.yahoo.com/news/top-commercial-banks-join-g7-161916215.html>
- [5] Project Nexus. Connecting Instant Payment Systems. 2025. Available from: <https://www.bis.org/about/bisih/topics/fmis/nexus.htm>
- [6] BIS. Tokenization May Create New Risks for Central Banks. 2024. Available from: <https://www.pymnts.com/blockchain/2024/bis-tokenization-may-create-new-risks-central-banks/>
- [7] Ripple and BCG. Future Expansion of Assets Trading. 2025. Available from: <https://ripple.com/ripple-press/global-financial-infrastructure-entering-a-new-era/>
- [8] Trump. Trumpy Launches His Own Crypto Currency. 2025. Available from: <https://www.bbc.co.uk/news/articles/c9vmym2jvy9o>
- [9] Mayer J. De-dollarization: The global payment infrastructure and wholesale central bank digital currencies. In: FMM Working Paper 102-2024. IMK at the Hans Boeckler Foundation, Macroeconomic Policy Institute; 2024. Available from: <https://ideas.repec.org/f/pma1008.html>
- [10] BIS. Central Bank Digital Currencies—Executive Summary. 2023. Available from: <https://www.bis.org/fsi/fsisummaries/cbdc.htm>
- [11] Morgan JP, Wyman O. Unlocking \$20 Billion Value in Cross-Border Payments. 2020. Available from: <https://www.jpmorgan.com/kinexys/documents/mCBDCs-Unlocking-120-billion-value-in-cross-border-payments.pdf>
- [12] G20. G20 Roadmap for Enhancing Cross-border Payments. FSB; 2020. Available from: <https://www.fsb.org/uploads/P131021-1.pdf>
- [13] SWIFT. New Collaborative Experiments Explore more Complex CBDC Use Cases. 2024. Available from: <https://www.swift.com/news-events/news/new-collaborative-experiments-explore-more-complex-cbdc-use>
- [14] Russia Ban from Using SWIFT—Australian Parliament Explainer. Available from: https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2022/March/Exclusion_of_Russia_from_SWIFT
- [15] Project Helvetia. 2022. Available from: <https://www.bis.org/about/bisih/topics/cbdc/helvetia.htm>
- [16] Project Jura. 2021. Available from: <https://www.bis.org/about/bisih/topics/cbdc/jura.htm>

- [17] Dumitrescu M. Tokenized Deposits: The Future of Banking. 2025. Available from: <https://r3.com/tokenized-deposits-unlocking-the-future-of-banking/>
- [18] Skingsley C, Shin H, BIS. Project Agora Press Conference. 2024. Available from: https://www.youtube.com/watch?v=7EQKwB_DDmk
- [19] Lloyd M. Central Bank Digital Currencies: The Future of Money. Agenda Publishing; 2023. Available from: <https://agendapub.com/page/detail/central-bank-digital-currencies/?k=9781788216326>
- [20] Kannengiebr N, Lins S. Trade-offs between distributed ledger technology characteristics. *ACM Computing Surveys*. 2020;**53**(2):42, 37 pages. DOI: 10.1145/3379463
- [21] CPMI. 2017. Available from: https://www.bis.org/cpmi/info_pfm.htm
- [22] Ripple X. Available from: <https://xrpl.org/>
- [23] Rubin, Arredondo. Decentralized Finance is Not All Block and White. 2025. Available from: <https://www.omfif.org/2025/05/decentralised-finance-is-not-all-block-and-white/>
- [24] Aqilla. Unified Ledgers vs Modular Ledgers. 2025. Available from: <https://www.aqilla.com/resources/do-you-wish-your-finance-system-was-always-in-balance-unified-ledger/>
- [25] BIS. Speech by A Carstens in May 6th, 2024. 2024. Available from: <https://www.bis.org/speeches/sp240506.htm>
- [26] Morgan JP. Speech by U. Farooq, May7th, 2024. 2024. Available from: <https://www.ledgerinsights.com/jp-morgan-explains-why-it-prefers-unified-ledger-over-public-blockchain-for-tokenization/>
- [27] BUNA Middle-East Unified Ledger. 2025. Available from: <https://buna.co/>
- [28] Stablecoins Pose Risks and Fall Short of Monetary Standards, Warns BIS. Available from: <https://www.thebanker.com/content/44a3906d-18b0-4843-9d00-0b70225c2873>
- [29] Liao, Caramichael. 2022. Available from: <https://www.federalreserve.gov/econres/ifdp/files/ifdp1334.pdf>
- [30] USDC. Regulated Stablecoin. 2025. Available from: <https://www.circle.com/usdc>
- [31] ESMA. Markets in Crypto-Assets Regulation. 2025. Available from: <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>
- [32] European Commission Eases Stablecoin Rules Despite ECB Concerns. Available from: <https://www.ainvest.com/news/european-commission-eases-stablecoin-rules-ecb-concerns2506/>
- [33] BOE Governor Bailey Warns Banks Against Issuing Own Stablecoins. Available from: <https://www.bloomberg.com/news/articles/2025-07-13/boe-governor-bailey-warns-banks-against-issuing-own-stablecoins>
- [34] Bloomberg UK. Potential Problems with the Genius Act. 2025. Available from: <https://www.bloomberg.com/news/articles/2025-06-10/stablecoins-bring-crypto-closer-to-the-mainstream-what-could-go-wrong>
- [35] Mehrling. Elasticity and Discipline in the Global Swap Network. 2015. Available from: <https://www.>

ineteconomics.org/uploads/papers/WP27-Mehrling.pdf

[36] mBridge. Connecting Economies Through CBDC. Available from: <https://www.bis.org/publ/othp59.htm>

[37] Zelmer, Kronick. Stablecoin and CBDCs Together. 2021. Available from: <https://cdhowe.org/publication/two-sides-same-coin-why-stablecoins-and-central-bank-digital-currency-have/>

[38] Arslanalp S, Eichengreen B, Simpson-Bell C. The Stealth Erosion of Dollar Dominance: Active Diversifiers and the Rise of Nontraditional Reserve Currencies. IMF WP/22/58. Washington, DC, USA: IMF; 2022

[39] ECB Unified Ledger Eurosystem Project. Available from: https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250220_1~ce3286f97b.en.html

[40] Banque de France wCBDCs Project. Available from: <https://www.banque-france.fr/en/financial-stability/financial-stability-mandate/supporting-digital-transformation-financial-sector/wholesale-mnbc>

[41] AMRO Asia. Asean+3 in a Fragmenting World. 2025. Available from: <https://amro-asia.org/asean3-in-a-fragmenting-world>

[42] Lloyd M. BRICS Plus 2024 Annual Meeting. GPI; 2024. Available from: <https://gpilondon.com/publications/brics-annual-meeting-2024>

[43] Lloyd M. BRICS Plus 2023 Annual Meeting. GPI; 2023. Available from: <https://gpilondon.com/publications/brics-annual-meeting-2023>

[44] Lloyd M. Biden's new Washington consensus in a Trumpian world. Atlantic Economic Journal. 2025. p. 3. Available

from: <https://uk.search.yahoo.com/yhs/search?hsparm=sz&hsimp=yhs-002&p=Lloyd%2C+M+%282025%29+Biden%E2%80%99s+New+Washington+Consensus+in+a+Trumpian+World%2C+Atlantic+Economic+Journal&type=type80260-4258542761&gdpr=1¶m1=475798463>

[45] Strengthening American Leadership in Digital Financial Technology. Available from: <https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/>

[46] Ralhi AS. Beyond Enforcement the SEC's Playbook on Crypto Regulation. 2025. Available from: <https://www.law.georgetown.edu/ctbl/blog/beyond-enforcement-the-secs-shifting-playbook-on-crypto-regulation/>

[47] SEC. Judgement on Terraform. 2023. Available from: <https://www.sec.gov/newsroom/press-releases/2023-32>

Blockchain Reshaping Energy Markets: Regulatory Frameworks for Sustainability-Driven Energy Tokens

Karisma Karisma and Sam Goundar

Abstract

This chapter examines how blockchain is revolutionising energy production, distribution, consumption, and trading, with a particular focus on sustainability-driven energy tokenisation that aims to decarbonise the grid, incentivise renewable energy generation, and democratise energy access. Projects such as WePower and Power Ledger are not just examples but beacons of hope, showcasing the potential of blockchain in realigning traditional energy systems toward climate-conscious paradigms. Nevertheless, these innovations confront unresolved legal and regulatory challenges. The chapter's central contribution is a comparative legal analysis of how jurisdictions are grappling with the classification and regulation of utility tokens and smart contracts in energy markets. In Malaysia, the Capital Markets & Services (Prescription of Securities) Order 2019 excluded utility tokens from the definition of securities, reflecting their functional character. However, the ongoing reforms to the Guidelines on Recognised Markets are significant, as they suggest a potential policy shift that could bring such tokens within the regulatory perimeter of Digital Asset Exchanges, potentially reshaping the regulatory landscape for blockchain in energy markets. In contrast, Australia, despite recognising the heterogeneity of crypto-assets, continues to rely on securities and financial services law in ways ill-suited to the hybrid nature of utility tokens, leaving issuers and consumers vulnerable to gaps in disclosure and protection. Going beyond token classification, this chapter explores the complex challenges presented by smart contracts in energy markets. These issues underscore the critical need for tailored, forward-looking regulation that can effectively balance investor protection, technological neutrality, and the decentralising ethos of blockchain-based energy systems.

Keywords: Blockchain, tokenisation, energy trading, smart contracts, legal and regulatory frameworks

1. Introduction

Blockchain found its origins in advancements across ledgers, cryptography, economics, and computer science, ultimately bringing forth Bitcoin in 2009. However, the conceptual seeds were sown much earlier. Dating back to 1991, 34 years ago, Haber and Stornetta built a cryptographically secured chain of blocks to establish a

digital record that is append-only and tamper-resistant [1]. Their work formed the basis for what became blockchain. In 2008, amid the global financial crisis, Satoshi Nakamoto authored a breakthrough whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System,” proposing a decentralised digital currency that relied on a type of distributed ledger which we now refer to as blockchain [2]. Bitcoin’s innovation was in solving the double-spending problem without needing a trusted central authority, using a combination of proof-of-work consensus and cryptographic hashing. Therefore, the primary impetus for such innovation was circumventing the trust gap embedded in trade and business processes between participating entities. Bitcoin essentially allows participants to engage in peer-to-peer digital transactions without having to rely on intermediaries. In 2013, Vitalik Buterin proposed the use of Ethereum to circumvent the limitations of Bitcoin, which led to a breakthrough shift in 2015 with its launch, raising \$18 million worth of ether [3]. Ethereum introduced a programmable blockchain with enhanced functionality, allowing developers to write decentralised applications (dApps) through smart contracts which are self-executing codes. The underlying technology, blockchain, began to receive attention beyond the context of cryptocurrencies. The blockchain space has diversified significantly. Today, blockchain is recognised as a “general-purpose technology” with the potential to transform not only financial systems but also sectors like supply chain, energy, healthcare, governance, and education [4]. With its continuous evolution, blockchain is increasingly intertwined with other emerging technologies, such as Artificial Intelligence and Internet of Things, amplifying its role in shaping disruptive business landscapes.

The idea of disruptive innovation, first introduced by Clayton Christensen, explains how such innovations transform the dominant industry logic, altering value creation, delivery, and capture simultaneously [5]. Blockchain technology exemplifies the disruptive innovation phenomenon by redefining the value chain. It has evolved into a foundational technology, disrupting conventional systems and centralised infrastructures across finance, energy, and supply chain, radically altering how individuals and organisations conduct transactions [6]. It is reshaping core industries with the prominent features of decentralisation, transparency, and immutability [7].

More importantly, blockchain technology enables systems in which authority is distributed, decision-making is transparent, and trust is embedded in code rather than centralised institutions and intermediaries [8]. In economies of scale and scope, decentralisation as a key feature of blockchain presents a disruptive force capable of flattening hierarchies, reducing transaction costs, and increasing system resilience [9]. Furthermore, it provides a range of benefits that enable the development of diverse use cases with real-time integration between stakeholders, automated operations, and data sharing, thus accelerating the viability and efficiency of various sectors. The intersection of blockchain technology and energy markets presents a transformative opportunity for advancing global sustainability goals through decentralised, transparent, and secure systems. However, these potentials are not without undue friction. The decentralised architecture often clashes with regulatory frameworks, dominant and centralised business models, and institutional inertia.

2. Research objective and methodology

This chapter examines how blockchain is revolutionising the landscape of energy production, consumption, and trading, with a particular focus on

sustainability-driven energy token initiatives that aim to decarbonise the grid, incentivise renewable energy generation, and democratise energy access. Projects such as WePower and Power Ledger are not just examples but beacons of hope, showcasing the potential of blockchain in realigning traditional energy systems toward climate-conscious paradigms, offering mechanisms for peer-to-peer energy trading, energy tokenisation, and regenerative ecological finance. Despite the promise of these innovations, their integration within existing legal and regulatory frameworks remains a pressing challenge.

This chapter briefly introduces the key features, elements, and characteristics of blockchain to better comprehend the technology's transformative potential as a multi-dimensional force. While the technological promise of blockchain is widely acknowledged, grounded in decentralisation, transparency, and automation, the legal, technological, and societal dimensions remain contested and complex. Many jurisdictions are still grappling with whether and how to regulate decentralised systems, often applying outdated legal doctrines to a technology that challenges traditional notions of authority and control. Further, public understanding remains limited, and resistance often emerges from institutional or behavioural inertia. Without broader awareness and stakeholder engagement, even the most innovative use cases risk remaining at the margins rather than achieving transformative scale.

As regulatory instruments become more formalised and comprehensive, an important normative and practical question surfaces in this chapter:

Do legal frameworks in Malaysia and Australia inadvertently constrain the decentralising potential of blockchain in energy markets?

In other words, could increase regulatory intervention function as a deterrent to decentralised innovation, undermining the core premise of disintermediation that underpins blockchain-based energy tokenisation? Here, we examine the tension between regulatory certainty and technological autonomy. While regulation is necessary to safeguard public interests, it must be calibrated in a manner that preserves the integrity and transformative promise of decentralised energy infrastructures. Striking this balance is not just a challenge but a strategic imperative.

To answer the research objectives, the authors utilised desk research and doctrinal legal research methods. The authors employed deep desk research that provided distinctive insights into this multidisciplinary area. In an emerging field with the adoption of cutting-edge technology such as blockchain, desk research proves helpful in obtaining detailed and impartial information. The desk research involved systematic collection and analysis of primary and secondary documents on blockchain-based use cases and business models, including but not limited to policy documents, government reports, energy industry reports, academic work, journal articles, commentaries, working papers, scientific web-based literature, technical reports, and other relevant publications. Besides deriving valuable data from desk research, the authors adopted doctrinal legal research methodology and textual analysis to discern and critically analyse the legal challenges, with particular reference to the legal and regulatory frameworks of Malaysia and Australia.

3. Blockchain fundamentals

The unique features and characteristics of blockchain interact coherently and add value to the sanctity of its architecture. Traditional business processes adopt centralised systems which rely on multiple intermediaries and central governing

bodies to verify transactions and streamline operations. Blockchain has attracted growing interest in recent years, largely because of its core feature of decentralisation. By dispelling the need for central authorities or intermediaries, blockchain networks simplify peer-to-peer interactions and reduce costs and complexity generally present in centralised systems [10]. Blockchain can be seen as a technological move toward a more distributed and inclusive landscape, as it challenges dominant and well-entrenched systems and embraces alternative forms of business governance [11, 12].

Transparency is a defining feature of blockchain technology. Network peers can equally assess and trace transaction data aggregated and recorded on the blockchain ledger [13]. All nodes on the network go through consensus protocols before a new block is added [14]. It ensures that no party has individual control over the verification process and that blockchain enhances transparency and data integrity, reducing the threat of falsification and malicious tampering of data [15]. Ultimately, a public blockchain is built on an open-source framework, which allows the usage and modification of open-source blockchain protocols, which are, in numerous instances, available for public viewing [11]. A public blockchain has high transparency with its fully decentralised system. However, a private blockchain may lack transparency. This is because participation is restricted to a defined group of users and participants, typically managed and maintained by a single entity [16].

Autonomy is blockchain's critical trait because of its self-governing infrastructure, in that the network operates independently of centralised oversight [17]. Functionality and consensus are upheld by distributed nodes rather than a single authority. However, the degree of autonomy is dependent on the architectural framework of blockchain. Public blockchains are permissionless systems that enable open participation. It allows any user to contribute to validate, verify, and record transactions on the ledger [18]. In contrast, private blockchains restrict these functions to selected actors, thereby reinforcing centralised governance within a distributed framework. Only predetermined nodes can participate in the blockchain network [19]. Generally, blockchain disrupts monopolies by reducing dependence on centralised operators or authorities, offering a model of autonomous, transparent, and user-driven energy markets.

The transaction data or information on the ledger cannot be modified or deleted without altering all subsequent blocks in the chain. Each block is timestamped, hashed, and cryptographically linked to the others, establishing a permanent record on the ledger [20]. Any attempt to modify data on the blockchain ledger necessitates the recalculation of new hash values for all subsequent blocks [15]. This is because even a minor change alters the original block's hash, thereby breaking the cryptographic link to the next block and invalidating the chain unless recomputed. The recomputation involves high cost and complexity, sufficient to deter any blockchain modification or deletion [21]. The immutability feature enhances data integrity and trustworthiness of blockchain transactions.

Furthermore, the blockchain's cryptographic feature preserves the anonymity and security of shared data, making it difficult for adversaries to gain unauthorised access or tamper with the data. Cryptography mechanisms like asymmetric cryptography involve public and private keys [22]. The public key serves as a unique address that remains untethered to the participant's real-world identity [23]. The private key comprises a unique cryptographic passcode that grants the user control over their digital assets and authorises transactions [24]. It serves as the user's digital identity, where only those with access to the private key can initiate, approve, or sign transactions on the network.

4. Peer-to-peer energy trading

Historically, centralised monopolies and utility companies controlled the generation of energy, its distribution, and transmission, with a push toward decarbonising and decentralising energy systems. This position promoted greater ownership and autonomy over renewable energy sources and distributed energy resources (DERs). The application of blockchain in the energy realm centres around facilitating distributed energy systems, charging electric vehicles, producing green certificates, facilitating grid management, integrating Internet of Things (IoT) devices, and easing the functions of peer-to-peer energy trading platforms [25]. Utilising blockchain can eliminate third-party intermediaries for the direct performance of peer-to-peer energy transactions between energy producers and consumers. Prosumers and consumers who utilise blockchain can trade energy without being exposed to high intermediary costs [26]. This position is facilitated by integrating technology with distributed energy infrastructures such as energy conversion devices and storage units, which can create new energy “production-supply-consumption systems”.

With the prominent application of distributed and decentralised energy systems grounded on blockchain technology, users can trade surplus energy in real-time [27], negating the monopoly of power industries and reducing energy loss in the transmission and distribution of energy over long distances.

The term ‘zero-sum activities’ connotes the absence of active demand-side and supply-side RE processes and operations, yielding no net RE production or consumption. Instead, zero-sum activities are proactive catalysts to employ DERs efficiently [28]. With increasing digitalisation, a large amount of data is collected and analysed. “Energy Data-as-a-service” constitutes innovative prosumer-driven business models in which prosumers can actively engage to provide data-related services that market actors require [29]. Blockchain technology can facilitate real-time information sharing and exchange between prosumers, consumers, network providers, and system operators to ensure information accessibility and efficacy in energy sharing and trading.

Malaysia, as a developing economy, is still in the nascent stages of integrating renewable energy into its national grid. In contrast, Australia, a developed country, possesses a comparatively mature and diversified renewable energy sector. Historically characterised by centralised monopolistic control, Malaysia’s energy market has progressively moved toward liberalisation and decentralisation, particularly through the engagement of independent power producers (IPPs) [30]. The country now aims to foster a more horizontally structured, bottom-up energy ecosystem. However, key challenges persist, including the need for infrastructure enhancements, the formulation of dynamic and cost-reflective pricing mechanisms, and the development of policy instruments that can accommodate technological and market shifts [26]. Australia, by contrast, grapples with the complexities of incorporating a growing number of prosumers into an already liberalised market. Its regulatory focus has shifted toward grid stability, addressing network-related externalities such as thermal overloading, reverse power flows, and safety concerns arising from the proliferation of distributed energy resources (DERs) [26]. This contrast highlights the differentiated industry-specific regulatory priorities and market conditions shaping the deployment of blockchain-based energy innovations in both jurisdictions.

5. Energy tokens

At the cutting edge of blockchain innovation lies tokenisation, a process that transforms units of energy, often measured in kilowatt-hours, into digital tokens recorded on the blockchain. This revolutionary process goes beyond mere digitisation of metering data; it creates a versatile asset that can be traded, stored, or combined with other digital assets. Unlike simple data entries, tokens are programmable and self-enforceable through smart contracts, enabling energy to be transacted like any other commodity within a digital marketplace.

Tokenisation's potential is particularly transformative in P2P energy markets. In these systems, households, or 'prosumers' with surplus renewable electricity (typically from rooftop solar) can sell directly to neighbours, local businesses, or energy communities. The blockchain ledger ensures that each unit of electricity produced is uniquely represented and cannot be double spent, addressing a significant challenge of digital exchange. Tokens also provide liquidity in otherwise fragmented local markets, preventing the waste or sale of surplus electricity at unfavourable tariffs. Instead, tokenisation allows it to be packaged and resold dynamically, ushering in a new era of energy trading.

The broader implications of tokenisation are significant. First, it allows energy to be treated as a tradable, portable digital asset, bridging the gap between physical flows of electricity and the financial instruments that govern energy markets. Second, it enables new business models that go beyond the sale of electricity itself. Tokens can represent not only consumption rights but also environmental attributes such as renewable energy certificates or carbon offsets, thereby embedding sustainability incentives directly into the architecture of trading systems. Third, the immutability and transparency of blockchain records play a crucial role in reducing disputes and verification costs, which are exceptionally high in decentralised energy contexts. This scenario reassures us of the reliability and efficiency of blockchain technology in the energy sector, a practical benefit that cannot be overstated. Further, prosumers use these applications for real-time representation of energy assets in the form of tokens, which they subsequently trade on blockchain platforms, facilitating considerable changes in energy processes and landscapes. While asset tracking, management, and optimisation applications facilitate improvements to energy infrastructures, they constitute zero-sum activities.

However, the introduction of tokenisation also brings about regulatory and conceptual challenges. Suppose energy tokens can be traded on secondary markets. In that case, they may start to resemble investment instruments, raising questions about their legal classification as securities or financial products (as seen in the next section). Moreover, tokenisation does not eliminate the technical complexities of grid balancing or the volatility of renewable generation; instead, it overlays these issues with inherent financial and legal uncertainties. Yet, blockchain-enabled tokenisation fundamentally transforms P2P energy trading by making electricity tradable as a secure and programmable asset, leading to greater efficiency, transparency, and inclusivity. Still, it also compels regulators and policymakers to rethink the legal and economic frameworks within which electricity markets have historically operated.

6. Token creation in P2P trading systems

The creation and circulation of energy tokens are foundational to the functioning of blockchain-enabled peer-to-peer (P2P) energy markets. Without a robust mechanism for token creation, P2P systems would struggle to match energy supply

with demand or incentivise participation. Token creation, therefore, plays a dual role: it represents real-world electricity production while simultaneously underpinning the financial and operational structure of decentralised energy markets. Each token is typically pegged to a measurable quantity of electricity, usually 1 kilowatt-hour [31]. The minting process, executed by a smart contract, issues new tokens to prosumers when they generate renewable electricity [32]. These tokens serve as both proof of production and instruments of exchange, effectively digitising electricity in a form that can circulate among peers. This process ensures that every kilowatt-hour produced is recorded and accounted for in real time, eliminating duplication or fraud. The importance of token creation extends beyond mere representation. By issuing tokens to prosumers, platforms provide an immediate economic incentive for renewable generation. Rather than waiting for monthly feed-in tariffs or relying on subsidies, households can receive tokens in near real time, which they can use to offset their own consumption, exchange with neighbours, or resell. This mechanism lowers entry barriers for small-scale producers, fostering greater participation and accelerating the transition to distributed renewable energy.

Equally significant is the role of token supply management in ensuring the stability of P2P markets. Token economies must balance the creation and destruction of tokens to reflect actual energy flows. The mint function increases supply by rewarding generation [32]. In contrast, the burn function reduces it by removing tokens from circulating in the decentralised energy market once they are redeemed for electricity consumed [32]. These mechanisms prevent inflation of token supply and maintain parity between digital assets and physical energy. Supply control is not only a technical necessity but also a governance tool, ensuring that token markets remain credible and stable. Token creation also underpins the liquidity of P2P markets, transforming electricity into a tradable asset [31]. In conventional grids, energy surpluses are difficult to monetise and often wasted. In tokenised systems, surplus energy is minted into tokens that can be stored or traded later, effectively transforming electricity into a storable financial asset. This liquidity is what makes P2P markets viable, allowing energy to flow seamlessly between multiple small producers and consumers.

Nevertheless, token creation raises significant challenges. If tokens are readily tradable on secondary markets, they may be purchased not for consumption but for speculation, blurring the line between utility and investment. Regulatory systems are often ill-equipped to distinguish between these functions, leaving token economies vulnerable to either under-regulation (exposing consumers to risks) or over-regulation (stifling innovation). In essence, token creation is the linchpin of blockchain-based P2P energy trading. It transforms electricity into a fungible, tradable, and incentivising asset, enabling decentralisation and efficiency while simultaneously creating new regulatory and economic complexities.

6.1 Case study 1: WePower

WePower, a blockchain-based energy trading platform established in 2017, exemplifies the application of decentralised and distributed ledger technology to RE procurement and trading. Its most prominent pilot took place in Estonia in collaboration with the national transmission system operator, Elering [33]. Leveraging the country's complete smart-metre coverage, WePower uploaded 24 terawatt-hours of historical consumption and production data, amounting to 26,000 hours, onto a blockchain infrastructure. This dataset was converted into approximately 39 billion Smart Energy Tokens, with each token constituting 1 kilowatt-hour of electricity [34]. Each

utility token functions as a self-executing smart contract, stipulating the energy type, production and delivery time, and price, thereby serving as a digitised analogue to a conventional power purchase agreement (PPA) [35]. Further, these tokens represent fractional ownership of energy assets /projects under the PPA, meaning that the token holders have a share in the revenue generated by the energy project. The tokens can be traded or exchanged through auctions [36]. By disintermediating traditional utilities and retailers, the platform enables renewable energy producers to sell directly to corporate and individual buyers. This democratisation of access lowers transaction costs and provides smaller actors with entry into energy markets previously dominated by incumbent suppliers.

From a financing perspective, tokenisation allows energy developers to pre-sell future production, diversifying counterparties and potentially enhancing project bankability. The 2018 initial coin offering, which raised \$40 million, further underscored the appetite for blockchain-enabled energy solutions, though subsequent token volatility highlighted investor risks [37]. Beyond Estonia, WePower expanded its model through “Elemental,” a white-label marketplace deployed with Mojo Power in Australia [38]. This model allows other energy companies to use WePower’s platform under their own brand, thereby expanding the reach and impact of WePower’s technology. In Australia, Elemental tokenised energy is generated from the Robinvale Solar Farm [38]. Despite these advances, critical challenges remain regulatory uncertainty regarding tokenised contracts, volatility of utility tokens such as WPR, and the limited integration of blockchain-based assets into broader clean energy investment flows. Scholars have observed that WePower exhibits unusually high “self-connectedness”, suggesting speculative investor behaviour and limited spillover into traditional energy markets [39]. Overall, WePower demonstrates both the promise and the fragility of blockchain-mediated energy markets: while capable of enhancing transparency and democratising access, such initiatives remain contingent upon legal recognition, regulatory harmonisation, and investor confidence.

For producers, they enable upfront financing by selling fractional units of future energy, lowering project risk, and enhancing bankability. For buyers, including corporations, SMEs, and households, they provide transparent and flexible access to clean energy without needing large-scale and long-term energy contracts. Investors benefit by gaining a new class of tradable green assets, while RE communities can pool resources to purchase or resell local renewable power. Finally, policymakers gain from the transparency and traceability of tokenised energy, which supports climate accountability and ESG reporting.

6.2 Case study 2: Power ledger

Power Ledger, a trailblazer in the energy industry, was founded in Australia in 2016 [40]. It stands out as one of the most innovative blockchain-based energy trading platforms, with a core ambition to revolutionise energy markets by enabling peer-to-peer (P2P) trading of renewable electricity. This groundbreaking approach reduces dependence on incumbent utilities and opens new possibilities for the energy sector. The system relies on a dual-token model: POWR, a publicly tradable token that provides access to the platform and functions as a staking mechanism, and Sparkz, a stable, internal unit of account pegged to local currency and used exclusively for transacting energy [41]. This structure separates speculative investment in POWR from the day-to-day energy settlement function of Sparkz, a design intended to mitigate volatility and support regulatory acceptance.

Technically, Power Ledger operates on both public and consortium blockchain layers. POWR is hosted on Ethereum, while Sparkz transactions are recorded on a private EcoChain ledger using Proof of Stake consensus protocols, with interoperability ensured through escrow arrangements [42]. Smart metres, which collect consumption and generation data in intervals of one to 30 minutes, play a crucial role in the system. They record the data, which is then registered on-chain. The platform's applications include xGrid for residential P2P trading, uGrid for microgrid and embedded network management, and PowerPort for electric vehicle charging markets [43, 44]. In addition, Power Ledger has piloted solutions for wholesale market settlements, renewable energy certificates, and carbon credit trading.

The company has undertaken trials in Australia, New Zealand, India, Thailand, and the United States, reflecting its ambition to position blockchain as an enabling infrastructure for distributed energy resources [45]. With a market capitalisation exceeding \$100 million, Power Ledger is also one of the most visible energy tokens in global digital asset markets [46]. Nevertheless, challenges remain. These include the platform's reliance on favourable regulation, its limited penetration beyond solar and wind, uncertainties around taxation of P2P energy transactions, and the need for further research to maximise the platform's efficiency [41]. These challenges underscore the fragility of blockchain-based energy solutions and the need for continuous innovation and adaptation.

Power Ledger's suggestion that P2P tokenised trading can replace subsidies is a beacon of hope for the renewable energy sector [46]. By making excess solar energy self-sustaining through direct market exchange, Power Ledger is paving the way for a more sustainable and efficient energy market. However, it is crucial to note that the pricing mechanics of energy tokens need to be studied carefully, as their success (and risks) will significantly influence climate policy, energy regulation, and green finance (**Table 1**).

Dimension	WePower	Power Ledger
Year & Origin	2017, Lithuania	2016, Australia
Core Purpose	Tokenisation of renewable energy production & direct trading between renewable energy producers and corporate and individual buyers.	Peer-to-peer (P2P) renewable energy trading & environmental commodities trading.
Token Types and Features	Smart Energy Tokens (SETs): 1 kWh per token, functioning as self-executing PPAs and fractional ownership of projects. WPR utility tokens are tradable.	Dual token system: POWR, a publicly tradable token that provides access to the platform and functions as a staking mechanism. Sparkz, a stable, internal unit of account pegged to local currency and used exclusively for transacting energy
Key Technical Features	WePower uploaded 24 terawatt-hours of historical consumption and production data, amounting to 26,000 hours, onto a blockchain infrastructure.	Operates across public (Ethereum) and private (EcoChain using Proof of Stake consensus protocols) blockchains. Smart metres feed consumption/generation data on-chain. Applications: xGrid (residential P2P), uGrid (microgrids), PowerPort (EV charging).

Dimension	WePower	Power Ledger
Market Applications	Pre-financing renewable projects. Fractional energy ownership. Direct and flexible access for corporations, SMEs, and households.	P2P trading in residential and microgrid contexts. EV charging markets. Solutions in wholesale markets, RE certificates, and carbon credits.
Geographic Reach	Estonia (pilot with Elering). Australia (Elemental marketplace with Mojo Power).	Pilots in Australia, New Zealand, India, Thailand, and the United States.
Financing & Investment	ICO raised \$40 m (2018). Tokenisation enables pre-selling future production, diversifying counterparties.	Market capitalisation exceeding \$100 m. POWR tokens are active in global digital asset markets.
Regulatory Outcomes & Challenges	Legal uncertainty over tokenised PPAs. Volatility of WPR token. Limited integration with mainstream energy finance	Regulatory acceptance enhanced by dual-token model. Reliant on favourable policies. Limited penetration beyond solar/wind. Uncertainty around P2P taxation and scalability.
Stakeholder Value	Producers: Upfront financing, risk reduction, improved bankability. Buyers: Flexible and transparent renewable energy access. Investors: New class of tradable green assets. Policymakers: Transparency, climate accountability and ESG reporting.	Producers/Prosumers: Monetise excess renewable generation. Consumers: Access to local and decentralised clean energy. Regulators: Sandbox for decentralised market design. Policy impact: P2P trading could substitute subsidies.

Table 1.
Authors' own.

7. Regulation of utility tokens in Malaysia

Under the Capital Markets & Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, utility tokens have conventionally been regarded as outside the definition of a “security.” This exclusion reflected the functional view that utility tokens are primarily designed to provide access to a product or service, rather than to generate investment returns [47]. As such, they have historically been spared the full weight of securities regulation. However, the Securities Commission Malaysia (SC) is now revisiting this position as part of its proposed reforms to the Guidelines on Recognised Markets (RMO Guidelines). The consultation raises the possibility that utility tokens, such as those used for access to digital platforms or services, may be brought within the regulatory perimeter of Digital Asset Exchanges (DAXs) [48]. Such a move would mark a significant policy shift, effectively reclassifying these utility tokens alongside securities and subjecting them to SC oversight.

The implications would be substantial. For issuers, listing and offering processes require prior SC consent, as well as compliance with disclosure and governance requirements, thereby raising costs and barriers to entry. For exchanges, additional compliance responsibilities would reshape market operations and potentially restrict the variety of tokens available for trading, which could mean that certain types of

utility tokens, which were previously not subject to securities regulation, may no longer be available for trading on DAXs. More broadly, the reclassification of tokens would blur the traditional distinction between “utility” tokens and “security” tokens. This boundary has long guided both innovation and regulation in digital asset markets. Ultimately, the SC’s deliberation reflects a broader regulatory dilemma. While utility tokens facilitate innovation and new business models, their speculative trading in secondary markets increasingly resembles investment activity. Whether Malaysia continues to exempt them or opts to regulate them as securities will have far-reaching consequences for the growth and competitiveness of its digital asset ecosystem, potentially affecting its global standing.

As an example, Malaysia’s proposed reclassification of utility tokens as securities would significantly affect the application of the WePower model. Its Smart Energy Tokens, representing fractional ownership and revenue rights, would likely fall within the securities perimeter, requiring prior approval, disclosure, and compliance with Securities Commission rules. This raises costs for issuers and restricts token trading to licenced DAXs, undermining WePower’s vision of democratised energy access. While stricter oversight may enhance legitimacy and investor protection, it would reduce liquidity and limit participation by smaller buyers. Ultimately, WePower’s tokenisation model could shift from enabling broad market access to serving more institutional, compliance-driven energy finance architecture.

8. Regulation of utility tokens in Australia

The Australian regulatory environment has long struggled to situate utility tokens within the framework of financial services law. By design, utility tokens provide access to a platform or service rather than conferring ownership rights or entitlements to profit. In theory, they are closer to software licences than to investment instruments. Yet, as the case law and regulatory commentary suggest, the boundary between consumptive use and investment purpose is far from clear. Even “closed-loop” tokens can fall within the ambit of financial regulation if they are broadly marketed or actively traded on secondary exchanges [49]. This creates persistent uncertainty for token issuers and exchange operators, especially in the context of initial coin offerings (ICOs). Such regulatory deterrence and ambiguity has discouraged innovators from launching projects domestically, with many choosing friendlier jurisdictions. This shows that a binary choice between classifying tokens as securities or leaving them unregulated is unworkable.

The ICO of Power Ledger (POWR) in 2017 illustrates both the potential and the ambiguity. The project raised approximately AUD \$34 million to support a blockchain-enabled peer-to-peer energy trading platform [50]. POWR tokens, characterised as utility tokens, are necessary to access the platform’s functions, while a second token, Sparkz, is used to settle actual energy transactions [51]. Power Ledger’s white paper (describing the project and configuration of its token model) expressly denied any investment rights or dividends, ownership claims, or guarantees of profitability. Instead, POWR tokens were framed as functional access keys, essential to operate the platform [50]. Nonetheless, their listing on cryptocurrency exchanges through secondary markets opened the possibility of speculative trading, raising questions as to whether they should be captured under Australian financial services laws.

ASIC has acknowledged that crypto-assets are heterogeneous, but its current framework remains ill-suited to capture the hybrid nature of utility tokens [52, 53].

Regulatory design must resist the urge to retrofit utility tokens into existing frameworks, as such an approach is akin to forcing a new form into an ill-suited legal mould. Scholars contend that while current legal frameworks may not be entirely suitable, the parallels with concerns over consumer protection and market oversight suggest that relying solely on general consumer law provisions against deception and misrepresentation is insufficient [50]. The absence of tailored safeguards leaves consumers exposed to risks similar to those associated with non-cash payment facilities such as the issuer's ability to alter the terms and conditions unilaterally and information asymmetry. A similar vulnerability exists with utility tokens, as platform operators often retain the discretion to modify the rights or functionalities attached to them [50].

Yet, because utility tokens were not automatically treated as financial products, issuers operated in a grey zone where disclosure obligations are generally weaker and unregulated. However, this concern is less acute for community-driven energy projects, where participants and platform operators are within the same community with benevolent intentions. In such contexts, the incentive structure is cooperative rather than speculative, and the primary objective is the circulation of locally generated renewable energy rather than secondary-market profit-making. The communal governance model and shared interest in sustaining the project mitigate some of the asymmetries and unilateral risks that plague more commercially driven token ecosystems.

Globally, under the EU's Markets in Crypto-Assets Regulation (MiCA), utility tokens are formally recognised as a distinct category, separate from asset-referenced and electronic money tokens. Defined as tokens providing "access to goods and services that do not yet exist or are not yet in operation," they avoid classification as securities unless they embed investment features. Issuers must publish a compliant crypto-asset white paper disclosing rights, risks, and obligations, with limited exemptions for small or closed offerings [54]. MiCA's role in increasing transparency and legal certainty is a reassuring factor, strengthening investor confidence while imposing higher compliance costs.

There is a strong case that when a token's defining function is not to generate speculative returns but to facilitate the operation of a digital ecosystem, it cannot be meaningfully regulated under the same principles as securities. Applying securities law in such cases would misconstrue the token's economic role. What is required, therefore, is a regulatory model that recognises the distinction between tokens as instruments of consumption and tokens as vehicles of investment, ensuring that oversight is proportionate to the risks actually posed. For example, treating POWR as a regulated financial product would risk assimilating the token (intentionally created to access specific products and services) into securities law, an outcome that would extend regulation beyond its natural purview. The regulatory challenge, therefore, lies in developing a framework that balances innovation and consumer protection without collapsing the distinction between functional access tokens and genuine investment products.

9. Smart contracts and token governance

If token creation provides the foundation of blockchain-enabled energy markets, smart contracts constitute the architecture that sustains them. Nick Szabo introduced smart contracts through his seminal work "The Idea of Smart Contracts,"

defining smart contracts as “A set of promises, including protocols within which the parties perform on the other’s promise. The protocols are usually implemented with programs on a computer network, [...] these contracts are ‘smarter’ than their paper-based ancestors [55].” The definition embodies the elements of trustlessness, automation, self-execution, and self-enforcement. Smart contracts that run on a Distributed Ledger Technology, such as blockchain, automate agreements by executing predefined conditions and specific actions once triggered, removing the need for human intervention or intermediaries. In the context of peer-to-peer (P2P) energy trading, smart contracts do far more than record transactions: they provide governance, enforcement, and economic stability. Further, blockchain-based smart contracts leverage key attributes, such as immutability, decentralisation, transparency, and security.

At their core, smart contracts allow for the automation of energy transactions. When a prosumer generates surplus electricity and offers it for sale, the smart contract can automatically calculate the corresponding number of tokens, set a price, and transfer ownership once a buyer agrees [32]. Similarly, when a consumer purchases energy, the contract automatically deducts tokens from the buyer’s account and credits them to the sellers. This level of automation not only reduces administrative overhead but also guarantees fairness, since all participants operate under the same transparent rules encoded in the blockchain.

Smart contracts also perform governance functions critical to the viability of tokenised markets. For example, they can enforce escrow and lock-up mechanisms, ensuring that tokens are held until energy delivery is confirmed [56]. This protocol addresses a fundamental challenge in energy trading: synchronising financial settlement with physical delivery. By requiring tokens to be locked until consumption is verified, smart contracts align incentives and reduce the scope for fraud or default. Nevertheless, the scope and utility of the smart contract depend on how accurately the programming language expresses the contractual terms agreed upon by the parties.

Beyond governance, smart contracts provide market adaptability. Contracts can include dynamic pricing algorithms that adjust token values in response to real-time supply and demand conditions, a feature essential in markets dependent on intermittent renewable generation [32]. They can also encode demand response mechanisms, rewarding consumers for shifting loads to periods of peak renewable supply. In doing so, smart contracts embed not only economic rules but also environmental objectives directly into market structures.

However, the use of smart contracts in the energy sector is not without difficulties. Unlike traditional contracts, they are written in programming languages such as Solidity, which are inaccessible to most legal practitioners and consumers. This lack of comprehensibility raises concerns about accountability and the scope of shared intention (*consensus ad idem*), especially when disputes arise. Moreover, the immutability of blockchain makes correcting errors or adapting terms challenging. These issues highlight the need for legal innovation alongside technical innovation, as regulators and courts must grapple with contracts that are simultaneously legal instruments and executable code.

While smart contracts reduce energy transaction costs, enforce energy delivery, and embed complex market rules into automated protocols, they raise new legal and regulatory questions about interpretation, liability, and consumer protection. By transforming electricity into a programmable digital asset, smart contracts extend the reach of law into code—an evolution that energy regulators cannot afford to ignore. In

Malaysia, the legal enforceability of a contract rests on the classical common law elements: an offer, its acceptance, valid consideration, and the parties' intention to create legal relations [57]. The contract must also be free from vitiating factors such as fraud, misrepresentation, coercion, duress, or illegality, as these may render the agreement void. Questions of contractual capacity and genuine consent remain equally applicable in this context. Where these conditions are satisfied, a smart contract can amount to a valid and enforceable agreement under Malaysian law in the literal sense. But where purposively interpreted, the question arises whether these traditional doctrines, formulated for human interactions, can be applied without modification to agreements generated, executed, or even concluded by autonomous code.

Section 10 of the Contracts Act 1950 (CA 1950) encapsulates the principle by stating that: "All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void." The statutory definitions of offer and acceptance under Section 2(a) and (b) mirror the common law position: a "proposal" arises where one person indicates willingness to perform or refrain from an act to secure another's assent; once that assent is given, the proposal becomes a promise [57]. This functional equivalence suggests that, in theory, smart contracts can fit within the existing legal mould as it clearly indicates contractual elements and terms.

The Electronic Commerce Act 2006 (ECA 2006) extends this framework into the digital sphere by conferring legal recognition on electronic communications. Section 6 expressly provides that information is not to be denied legal validity merely because it exists in electronic form, or because the referenced data is stored outside the electronic message itself, provided it remains accessible to the counterparty [58]. The Act also defines "electronic signature" broadly, covering any symbol, character, or digital identifier adopted as a signature, thereby accommodating the automated nature of blockchain-based transactions [58]. While the ECA was designed with email, electronic records, and digital signatures in mind, the provision can be interpreted purposively to include self-executing blockchain scripts.

However, any practical enforceability of the contract also hinges on evidentiary requirements. The issue arises where the admissibility of contracts in judicial proceedings in Malaysia further depends on compliance with the Stamp Act 1949 (SA 1949). Section 52 [1] (a) SA 1949 prohibits the admission of unstamped instruments into evidence [59]. Stamping thus remains a precondition for enforceability, providing fiscal compliance as well as evidentiary admissibility, which raises a concern: can a self-executing smart contract, existing only as lines of code on a distributed ledger, be "stamped" in the conventional sense?

Similarly, in Australia, the common law principles of a valid and enforceable contract, namely offer, acceptance, consideration, and intention to create legal relations, would equally apply to smart contracts. The Electronic Transactions Act 1999 addresses electronic transactions in Australia, ensuring that they are legally enforceable and facilitating their use in business transactions. According to the Act, "a transaction is not invalid because it took place by means of one or more electronic communication," which is a key provision when recognising smart contracts in the legal sphere [60]. Signatures, information, and documents provided, produced, recorded, or retained in an electronic form have legal status. Further, "a contract formed automatically is not invalid, void, or unenforceable because there was no human review or intervention," embodying the validity of blockchain transactions and smart contracts despite the lack of intermediaries.

However, the lack of legal frameworks in the event of disputes from coding errors or unforeseen circumstances exposes participants to significant risks and limited avenues for redress. A central right for energy prosumers is to receive transparent and accessible contractual information, covering tariffs, billing methods, allocation rules, and platform fees [61]. Yet the process of transcribing legal rights, obligations, and remedies into code (and decoding them back into human-readable language) is fraught with complexity [62]. Contractual drafting relies on nuanced phrasing and interpretive flexibility, which are rarely replicable in rigid programming codes. The absence of detailed specifications in code can produce significant downstream consequences.

Even with the advancement of programming languages, the task of mastering them remains a domain of specialist knowledge. The scarcity of reliable translation tools that can convert legal language into executable code (and vice versa) underscores the complexity of the process. This complexity often leads to hesitation among businesses and individuals to adopt smart contracts. The absence of such tools not only raises costs but also increases the likelihood of errors, which can escalate into disputes. While some obligations, when expressed with sufficient precision, can be readily coded, not all contractual clauses are amenable to automation [63]. The heterogeneous nature of contracts makes it nearly impossible to foresee every contingency [63]. For instance, force majeure clauses are notoriously resistant to codification due to their dependence on unforeseeable external events. Similarly, vague legal standards such as ‘good faith’ or ‘reasonableness’ cannot be meaningfully represented in code, highlighting the limitations of smart contracts [64].

Flaws in the code and programming errors can undermine smart contract operations, eroding any advantages they promise in executing energy contracts or power purchasing agreements (PPAs). Smart contract attributes, such as immutability and irreversibility, which are typically seen as safeguards, may exacerbate problems by preventing the alteration or deletion of faulty records. Smart contracts also face vulnerabilities to bugs, malware, and intentional exploitation by malicious actors. Such threats may compromise contractual performance, with no recourse to corrective measures, leaving parties vulnerable to significant financial harm [64]. When defects or malfunctions occur, automated execution continues regardless of whether outcomes align with the parties’ intentions [65]. Drafting and coding mistakes often manifest as billing inaccuracies or transactional disruptions. Since the performance of such agreements depends on the technical competence of programmers, the persistent question remains: who bears liability when errors cause losses? Parties, therefore, need a clear understanding of the risks associated with blockchain-based automation before committing to its use.

Using smart contracts as legal instruments presents challenges for parties unfamiliar with programming. Legal enforceability depends on a clear and mutual expression of intent but coding that intent into executable form often requires reliance on programmers. Linguistic ambiguities and limited technical knowledge may prevent contracting parties from verifying whether the code faithfully represents their agreement. To mitigate this, some scholars propose developing a “term sheet” that provides programmers with explicit specifications [64]. Parties may also consider contractual arrangements with developers themselves, either by requiring a representation that the code mirrors the parties’ intent or by embedding explicit obligations on the programmer within a separate agreement [64]. These strategies aim to reduce interpretive disputes and ensure that the coded agreement reflects the underlying consensus.

The enforceability of judgements concerning smart contracts is likewise uncertain, raising questions about the adequacy of legal protection. In decentralised peer-to-peer or community energy settings, these concerns become particularly acute, as traditional enforcement mechanisms are bypassed. Traditionally, parties agree on enforcement and dispute resolution mechanisms. Smart contracts, however, assume away the need for such provisions by embedding self-enforcement into their design. Yet disputes still arise, and enforcement presupposes identification of the parties—something that is often obscured on public blockchains where only pseudonymous addresses are visible. By design, smart contracts are immutable. Once deployed, halting performance or altering terms is virtually impossible without predefined mechanisms in place. This forces parties to rely on technical infrastructure and programmer-devised features to allow for termination or modification. Coding language itself can become a source of disagreement. If contractual terms are expressed with insufficient clarity, disputes emerge over whether the programmed instructions capture the parties' true intent. The opacity of code for non-experts only compounds these interpretive challenges.

10. Conclusion

This chapter has shown that blockchain-enabled tokenisation and smart contracts represent both an innovation and a regulatory disruption in the energy sector. While projects such as WePower and Power Ledger demonstrate how tokens and decentralised platforms can democratise energy access, facilitate renewable financing, and embed sustainability into market design, they also expose gaps in existing legal and institutional frameworks. The comparative analysis of Malaysia and Australia reveals contrasting regulatory approaches: Malaysia is shifting from exclusion to potential regulation of utility tokens under Digital Asset Exchange rules, while Australia, though recognising the heterogeneity of crypto-assets, has yet to establish a framework suited to the hybrid nature of utility tokens. In both contexts, the absence of tailored safeguards leaves consumers vulnerable to risks such as weak disclosure obligations and unilateral changes by issuers. Smart contracts, meanwhile, promise efficiency and automation but introduce risks of coding flaws, immutability, and interpretive opacity that challenge enforceability and accountability. Without tailored safeguards, these tools risk undermining the very trust they seek to replace.

The lesson is clear: effective governance of blockchain-based energy systems requires regulatory frameworks that move beyond reactive compliance and instead anticipate and adapt to technological change. Striking the right balance between consumer protection, technological neutrality, and the decentralising ethos of blockchain will determine whether tokenisation becomes a catalyst for equitable energy transitions or another layer of risk. Ultimately, the success of these innovations depends less on technical capacity than on institutional willingness to create adaptive, forward-looking regulation that aligns blockchain's potential with the urgent demands of climate and energy governance.

Acknowledgements

We are deeply grateful to have mentors, teachers, family, and friends who offered unwavering support and encouragement throughout the research and writing process.

Conflict of interest

The authors declare no conflict of interest.

Author details

Karisma Karisma^{1*} and Sam Goundar²

1 Independent Researcher, Ampang, Selangor, Malaysia

2 RMIT University, Melbourne, Australia

Address all correspondence to: karisjay@outlook.com

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Haber S, Stornetta WS. Secure names for bit-strings. In: Proceedings of the 4th ACM Conference on Computer and Communications Security. Zurich, Switzerland: ACM Conference on Computer and Communications Security; 1997
- [2] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*. 2008;21260
- [3] Buterin V. Ethereum white paper. GitHub Repository. 2013;1(22-23):5-7
- [4] Lemieux VL. Blockchain and Recordkeeping. Basel, Switzerland: MDPI; 2021. p. 135
- [5] Christensen CM, Raynor M, McDonald R. 17. Disruptive innovation. *Harvard Business Review*. 2015;93(12):44-53
- [6] Zhu X, Wang D. Research on blockchain application for E-commerce, finance and energy. In: IOP Conference Series: Earth and Environmental Science. IOP Publishing; 2019
- [7] Verma P, Ram B. Application of blockchain technology in data security. *IP Indian Journal of Library Science and Information Technology*. 2024;1:51-55
- [8] Guo H, Liu X. Exploring trust dynamics in finance: The impact of blockchain technology and smart contracts. *Humanities and Social Sciences Communications*. 2025;12(1):1235
- [9] Mylrea M, Gourisetti SNG. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In: 2017 Resilience Week (RWS). Wilmington, DE, USA: IEEE; 2017
- [10] Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A survey on the adoption of Blockchain in IoT: Challenges and solutions. *Blockchain: Research and Applications*. 2021;2(2):100006
- [11] Rahimi N, Roy I, Gupta B, Bhandari P, Debnath N. Blockchain technology and its emerging applications. In: Sharma SK, Bhushan B, Khamparia A, Astya PN, Debnath NC, editors. *Blockchain Technology for Data Privacy Management*. 1st ed. Boca Raton: Taylor & Francis Group; 2021. p. 330
- [12] Woolley JL. Getting along with frenemies: Enhancing multi-competitor coopetition governance through artificial intelligence and Blockchain. *Industry and Innovation*. 2023;1-34
- [13] Bassan F, Rabitti M. From smart legal contracts to contracts on blockchain: An empirical investigation. *Computer Law & Security Review*. 2024;55:106035
- [14] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*. 2020;166:102693
- [15] Dorsala MR, Sastry V, Chapram S. Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications*. 2021;196:103246
- [16] Kim J-w. Blockchain technology and its applications: Case studies. *Journal of System and Management Sciences*. 2020;10(1):83-93
- [17] van Lier B. Blockchain technology: The autonomy and self-organisation of cyber-physical systems. In: *Business Transformation through Blockchain*.

Vol. I. Switzerland: Springer;
2018. pp. 145-167

[18] Mehta J, Ladvaiya N, Pandya V. Exploration of Blockchain architecture, applications, and integrating challenges. In: Pandian AP, Fernando X, Islam SMS, editors. *Computer Networks, Big Data and IoT*. 66: Springer; 2021. pp. 585-600

[19] Viriyasitavat W, Hoonsoopon D. Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*. 2019;13:32-39

[20] Marthews A, Tucker C. What Blockchain can and can't do: Applications to marketing and privacy. *International Journal of Research in Marketing*. 2023;40(1):49-53

[21] Pandey V, Pant M, Snasel V. Blockchain technology in food supply chains: Review and bibliometric analysis. *Technology in Society*. 2022;69:101954

[22] Singh A, Kumar G, Saha R, Conti M, Alazab M, Thomas R. A survey and taxonomy of consensus protocols for Blockchains. *Journal of Systems Architecture*. 2022;127:102503

[23] Hong H-J, Fan W, Wuthier S, Kim J, Chow CE, Zhou X, et al. Robust P2P networking connectivity estimation engine for permissionless bitcoin cryptocurrency. *Computer Networks*. 2022;219:109436

[24] Li Z, Bahramirad S, Paaso A, Yan M, Shahidehpour M. Blockchain for decentralized transactive energy management system in networked microgrids. *The Electricity Journal*. 2019;32(4):58-72

[25] Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, et al.

Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*. 2019;100:143-174

[26] Karisma K, Deane F. Empowering energy: Legal and regulatory perspectives on blockchain-enabled trading in Malaysia and Australia. *Asian Journal of Law and Society*. 2024;11(4):507-529

[27] Yahaya AS, Javaid N, Alzahrani FA, Rehman A, Ullah I, Shahid A, et al. Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism. *Sustainability*. 2020;12(8):3385

[28] Hv S. The prosumer in European energy law. In: *Scandinavian Institute of Maritime Law Yearbook*. Oslo, Norway: Nordisk institutt for sjørett; 2018

[29] Botelho DF, Dias BH, de Oliveira LW, Soares T, Rezende I, Sousa TM. Innovative business models as drivers for prosumers integration—Enablers and barriers. *Renewable and Sustainable Energy Reviews*. 2021;144:111057

[30] Jalal TS, Bodger P. National energy policies and the electricity sector in Malaysia. In: *2009 3rd International Conference on Energy and Environment (ICEE)*. Malacca, Malaysia: IEEE; 2009

[31] Seyfi M, Mehdinejad M, Mohammadi-Ivatloo B, Aghaei J. Smart contract-based peer-to-peer energy token trading for self-decisive retailers and prosumers with flexible loads. *IEEE Transactions on Industry Applications*. 2025;61(6):8430-8442

[32] Saeed N, Wen F, Afzal MZ. Decentralized peer-to-peer energy trading in microgrids: Leveraging blockchain technology and

smart contracts. *Energy Reports*. 2024;**12**:1753-1764

[33] Mhlanga D. Blockchain and Crowdfunding for Renewable Energy Projects in Africa. *Sustainable Finance and Business in Sub-Saharan Africa*: Springer; 2024. pp. 313-333

[34] Bhavana G, Anand R, Ramprabhakar J, Meena V, Jadoun VK, Benedetto F. Applications of blockchain technology in peer-to-peer energy markets and green hydrogen supply chains: A topical review. *Scientific Reports*. 2024;**14**(1):21954

[35] Pichler M, Meisel M, Goranovic A, Leonhartsberger K, Lettner G, Chasparis G, et al. Decentralized energy networks based on blockchain: Background, overview and concept discussion. In: *International Conference on Business Information Systems*. Berlin, Germany: Springer; 2018

[36] Tian Y, Wang C, Asutosh A, Woo J, Adriaens P. Blockchain-enabled tokenization for sustainable and inclusive infrastructure investment. *arXiv preprint arXiv:220804709*; 2022

[37] Aliano M, Cestari G, Madonna S. Initial coin offering as a possible way to obtain financial resources. In: *Sustainable Finance for SMEs: The Role of Capital for Sustainable and Inclusive Growth*. Switzerland: Springer; 2024. pp. 93-101

[38] Gan R, Li R. Contract Tokenization in the Renewable Energy Market. Available at SSRN 4932043; 2024

[39] Naifar N. Interactions between renewable energy tokens, oil shocks, and clean energy investments: Do COP26 policies matter? *Energy Policy*. 2025;**198**:114497

[40] Shan S, Yang S, Becerra V, Deng J, Li H. A case study of existing

peer-to-peer energy trading platforms: Calling for integrated platform features. *Sustainability*. 2023;**15**(23):16284

[41] Ilina O, Tagirova K, Barger A, Gorgadze V. SoK: How Blockchain and tokenization will transform the energy sector. In: *2023 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*. Berlin, Germany: IEEE; 2023

[42] Cali U, Kuzlu M, Pipattanasomporn M, Kempf J, Bai L. Energy systems meet with blockchain technology. In: *Digitalization of Power Markets and Systems Using Energy Informatics*. Switzerland: Springer; 2021. pp. 197-216

[43] Etukudor C, Couraud B, Robu V, Früh W-G, Flynn D, Okereke C. Automated negotiation for peer-to-peer electricity trading in local energy markets. *Energies*. 2020;**13**(4):920

[44] Küfeoglu S, Liu G, Anaya K, Pollitt M. Digitalisation and New Business Models in Energy Sector. *Cambridge Working Paper in Economics, EPRG Working Paper*, University of Cambridge; 2019

[45] Chathuranga D, Mudiyanse W, Hasan KN. Peer-to-peer energy trading: Existing algorithms, applications, platforms, challenges and opportunities. In: *2022 IEEE PES 14th Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. Melbourne, Australia: IEEE; 2022

[46] Manahov V, Li M. A note on the relationship between digital assets and the energy markets: New evidence from the most prominent crypto heists. *The European Journal of Finance*. 2025:1-37

[47] Capital Markets & Services (Prescription of Securities) (Digital Currency and Digital Token) Order; 2019

- [48] Securities Commission. Guidelines on Recognised Markets. Malaysia: Securities Commission Malaysia; 2023
- [49] Financial Integrity Hub. Financial Integrity Hub Insights: Virtual Assets & Virtual Asset Service Providers; 2025
- [50] Lai D. Should cryptocurrencies and initial coin offerings (ICOs) be regulated under Australian financial services Laws? John Marshall Global Markets Law Journal. 2019;5(1):2
- [51] Wang C, Wu T, Kong M, Deveci M, Chen Z-S, Zaidan AA. Sustainable and secure Metaverse economies: Review of the application of renewable energy cryptocurrency and tokens. IEEE Systems, Man, and Cybernetics Magazine. 2025;11(2):33-50
- [52] Australian Securities & Investments Commission. Information Sheet 225 (INFO 225) - Crypto-assets n.d. Available from: <https://www.asic.gov.au/regulatory-resources/digital-transformation/crypto-assets/>
- [53] Australian Securities & Investments Commission. Consultation Paper 343: Crypto-Assets as Underlying Assets for ETPs and Other Investment Products. Australia: Australian Securities & Investments Commission; 2021
- [54] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937; 2023
- [55] Szabo N. The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials. 1997;6(1):199
- [56] Todorean L, Antal C, Antal M, Mitrea D, Cioara T, Anghel I, et al. A lockable ERC20 token for peer to peer energy trading. In: 2021 IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE; 2021
- [57] Contracts Act; 1950
- [58] Electronic Commerce Act; 2006
- [59] Stamp Act; 1949
- [60] Electronic Transactions Act; 1999
- [61] Paiho S, Kiljander J, Sarala R, Siikavirta H, Kilkki O, Bajpai A, et al. Towards cross-commodity energy-sharing communities—a review of the market, regulatory, and technical situation. Renewable and Sustainable Energy Reviews. 2021;151:111568
- [62] Carron B, Botteron V. How smart can a contract be? In: Kraus D, Obrist T, Hari O, editors. Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law. United Kingdom: Edward Elgar Publishing; 2019
- [63] Henly C, Hartnett S, Endemann B, Tejblum B, Cohen DS. Energizing the future with Blockchain. Energy Law Journal. 2018;39:197
- [64] Compagnucci MC, Fenwick M, Haapio H. Digital technology, future lawyers and the computable contract designer of tomorrow. In: Research Handbook on Contract Design. Gloucestershire: Edward Elgar Publishing; 2021. pp. 421-444
- [65] Lee J, Khan VM. Blockchain and smart contract for peer-to-peer energy trading platform: Legal obstacles and regulatory solutions. UIC Review of Intellectual Property Law. 2020;19(4):1



Edited by Sam Goundar

Cryptocurrencies have emerged as transformative forces in the global financial ecosystem, offering innovative solutions for transactions, investments, and decentralized operations. This book, *Cryptocurrencies - Innovations, Challenges, and Future Prospects*, provides a comprehensive exploration of the cryptocurrency landscape, combining foundational concepts with cutting-edge research and practical applications. The book delves into the technological underpinnings of cryptocurrencies, including blockchain, cryptographic algorithms, and decentralized networks, while addressing key challenges such as security vulnerabilities, scalability, and regulatory compliance. It also explores the growing use cases of cryptocurrencies in payment systems, tokenization, and decentralized applications, highlighting their potential to reshape industries and foster financial inclusion. Emphasizing forward-looking trends, the book examines topics like quantum-safe encryption, interoperability, and the rise of Central Bank Digital Currencies. Ethical considerations, risks, and the global impact of cryptocurrencies on emerging markets and the digital economy are also analyzed. Designed for academics, researchers, industry professionals, and policymakers, this book aims to bridge the gap between theoretical advances and practical applications, offering insights into the future of cryptocurrencies.

Published in London, UK

© 2026 IntechOpen
© vsijan / nightcafe.studio

IntechOpen

