THE JBBA
THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®
VOLUME 6 | ISSUE 1 | ISSN PRINT: 2516-3949
MAY 2023
britishblockchainassociation.org/jbba
The British Blockchain Association®
Advocating Evidence Based Blockchain
WORLD'S FIRST PEER-REVIEWED BLOCKCHAIN JOURNAL AVAILABLE IN PRINT & ONLINE

BUILDING A DECENTRALISED METAVERSE

THE FUTURE OF BLOCKCHAIN BASED IMMERSIVE ECONOMIES

FEATURED ARTICLES

3RD BLOCKCHAIN ASSOCIATIONS FORUM (BAF) ANNUAL MEMBER SUMMIT | 20 SEPTEMBER 2023

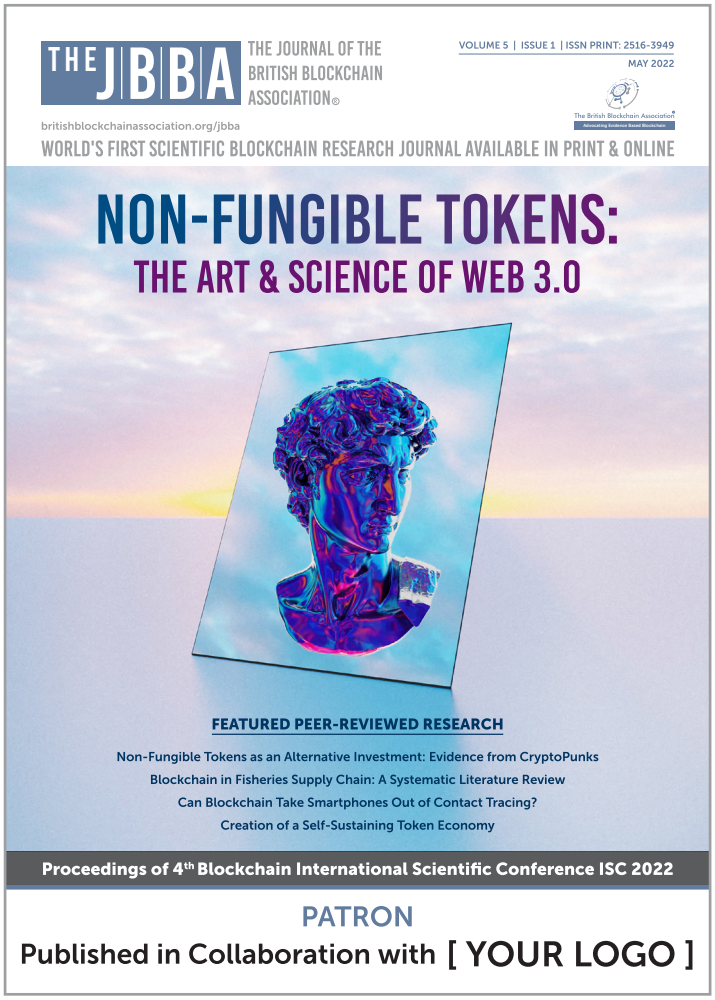
PROCEEDINGS OF 5TH BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE #ISC2023

PUBLISHED BY
CEBB | Centre for Evidence-Based Blockchain®

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

WHY BECOME A PATRON OF THE JBBA?

Your logo will appear on the COVER PAGE of the JBBA.
The journal is distributed worldwide to major Universities, Banks, Fintech Institutions, Blockchain Research Centres, Policy Makers, Influencers, Industry Leaders and Journal's Editors, Reviewers and Authors



PATRON
Published in Collaboration with [YOUR LOGO]

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

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

www.britishblockchainassociation.org | info@britishblockchainassociation.org

Follow us on:

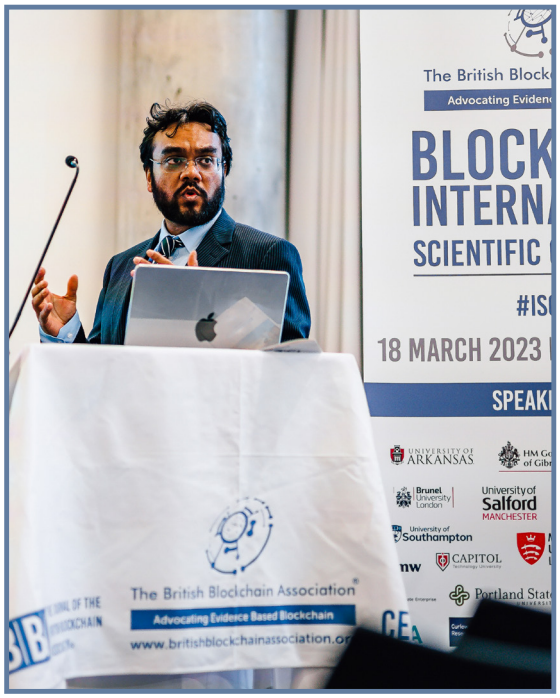
TABLE OF CONTENTS

BBA'S 5TH BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE #ISC2023


The British Blockchain Association
Advocating Evidence Based Blockchain
www.britishblockchainassociation.org

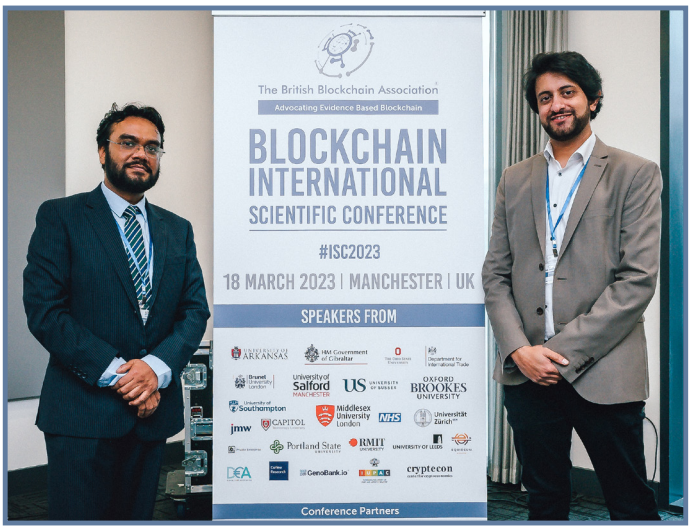

CERTIFICATE


CERTIFICATE


The British Block
Advocating Evidenc
BLOCK
INTERNA
SCIENTIFIC
#IS
18 MARCH 2023
SPEAK
The British Blockchain Association
Advocating Evidence Based Blockchain
www.britishblockchainassociation.or
University of Salford
MANCHESTER
Brunel University London
University of Southampton
CAPITOL
Portland State


BLOCKCHAIN
INTERNATIONAL
SCIENTIFIC CONFERENCE

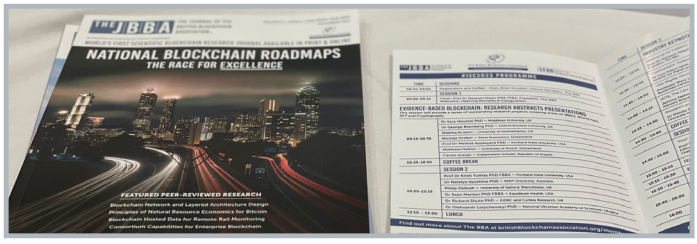

5th Blockchain International Scientific Conference ISC2023
18 March 2023, Manchester
Conference Hashtag: #ISC2023


The British Blockchain Association
Advocating Evidence Based Blockchain
BLOCKCHAIN
INTERNATIONAL
SCIENTIFIC CONFERENCE
#ISC2023
18 MARCH 2023 | MANCHESTER | UK
SPEAKERS FROM
Conference Partners


The British Blockchain Association
Advocating Evidence Based Blockchain


The British Blockchain Association
Advocating Evidence Based Blockchain
BLOCKCHAIN
INTERNATIONAL
SCIENTIFIC CONFERENCE
#ISC2023
18 MARCH 2023 | MANCHESTER
SPEAKERS FROM


The British
Advocating
BLOCKCHAIN
INTERNATIONAL
SCIENTIFIC CONFERENCE
18 MARCH 2023


NATIONAL BLOCKCHAIN ROADMAPS
THE RACE FOR EXCELLENCE
FEATURED PEER-REVIEWED RESEARCH


The British Blockchain Association
Advocating Evidence Based Blockchain


BLOCKCHAIN
INTERNATIONAL


NON-FUNGIBLE TOKENS:
THE ART & SCIENCE OF WEB 3.0


The British Blockchain Association


The British Blockchain Association
Advocating Evidence Based Blockchain
Bridging the Blockchain Research and Practice Gap
CEBB
THE JBBA
CEBB Centre for Evidence-Based Blockchain
THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION
Worlds First Peer Reviewed Blockchain Journal Available Both in Print & Online

MEMBERS & PARTNERS OF THE BBA ECOSYSTEM

EPOKA UNIVERSITY

HM Government of Gibraltar

GANT

National Blockchain Project

HELSINKI BLOCKCHAIN CENTER

SiBAN
STAKEHOLDERS IN BLOCKCHAIN TECHNOLOGY ASSOCIATION OF NIGERIA

UNIVERSITY OF ARKANSAS
Sam M. Walton College of Business

cryptecon
center for cryptoeconomics

TBA
Taiwan Blockchain Alliance
臺灣區塊鏈大聯盟

OPIS GROUP

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

BLOCKCHAIN ALLIANCE MEXICO

SANBA
South African National Blockchain Alliance

Pakistan Blockchain Institute

ASOSIASI BLOCKCHAIN INDONESIA

ALASTRIA

HELLENIC BLOCKCHAIN ASSOCIATION

RMIT UNIVERSITY

GRESHAM INTERNATIONAL

XPmarket.io

CANADIAN BLOCKCHAIN CONSORTIUM

BLOCKCHAIN NZ

WORKING IN COLLABORATION WITH:

Department for International Trade

BBC NEWS GLOBAL

British Embassy Lisbon

GCPSE Global Centre for Public Service Excellence

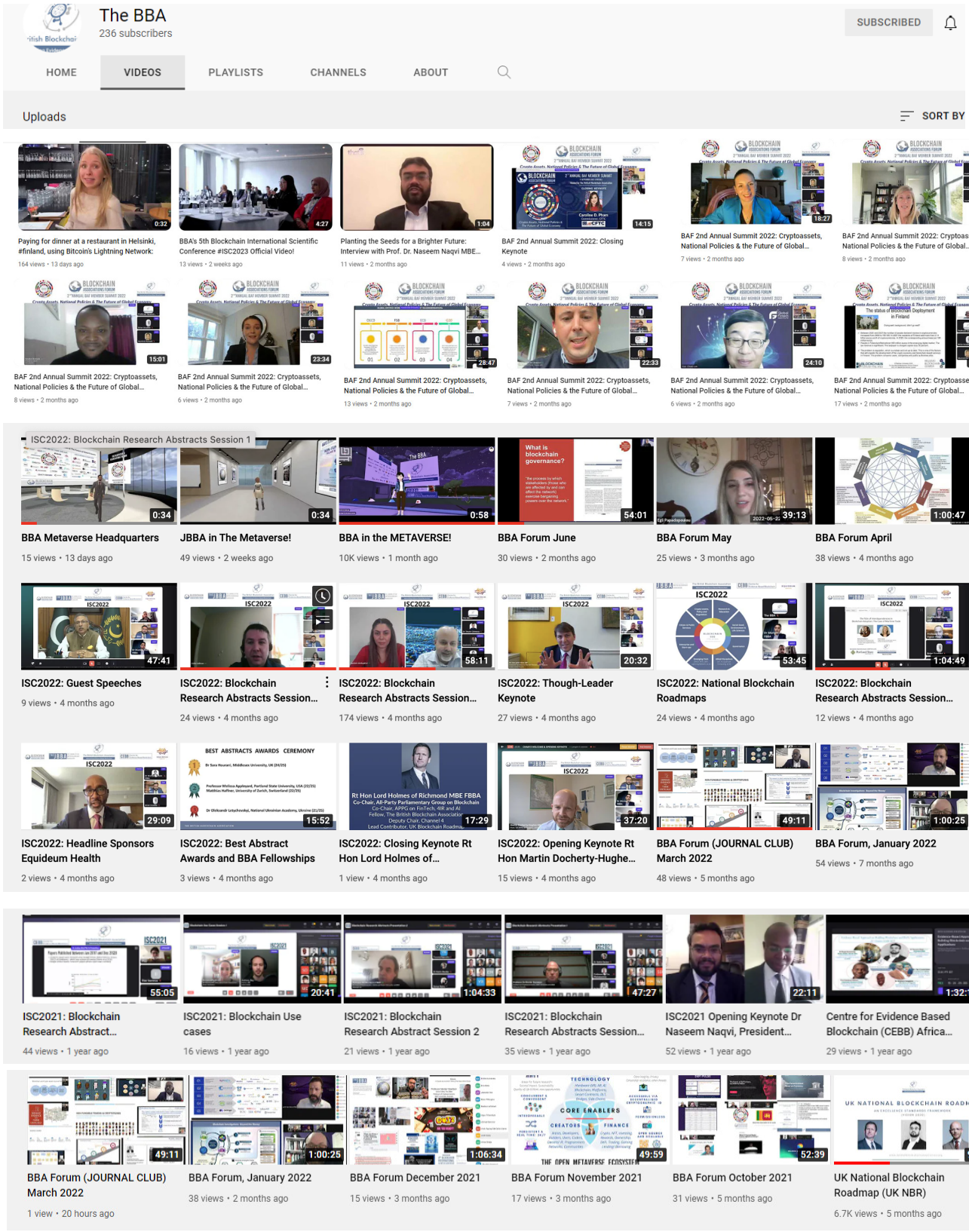
UNDP

appg BLOCKCHAIN

ARTiFACTS
Researcher Recognition. Accelerated

Join Now at britishblockchainassociation.org/membership

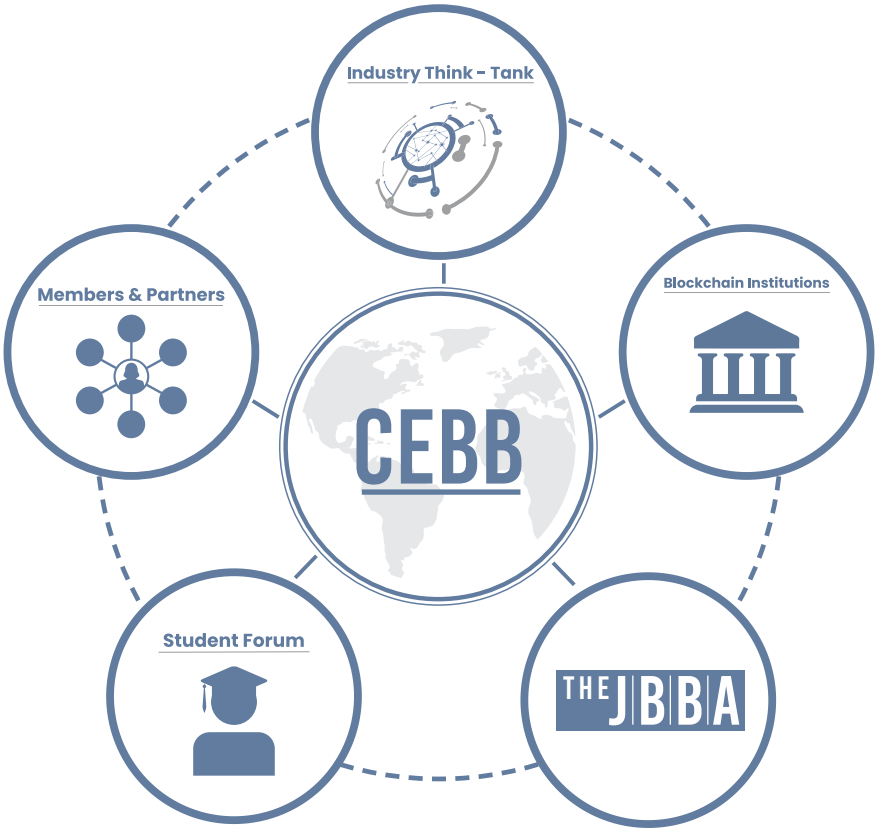
SUBSCRIBE TO OUR YOUTUBE CHANNEL



For more info, visit https://www.youtube.com/c/TheJBBA

CEBB | Centre for Evidence-Based Blockchain®

Bridging the Blockchain Research and Practice Gap



MEMBERS

GANT
HM Government of Gibraltar
Blockchain Alliance Mexico
National Blockchain Project
SiBAN
RMIT University
Equideum Health
Edinburgh Napier University
Pakistan Blockchain Institute
University of Arkansas Sam M. Walton College of Business
Ulster University
TBA Taiwan Blockchain Alliance
SANBA South African National Blockchain Alliance
uB Université de Bourgogne
The Open University
Crypto Valley
Blockchain Association Singapore
Gresham International
cryptecon center for cryptoeconomics

JOIN CEBB

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

WHAT IS CENTRE FOR EVIDENCE BASED BLOCKCHAIN?

- A neutral, decentralised, **global coalition** of leading blockchain **enterprises** and **research institutions**
- A "**Think Tank**" of thought leaders in Blockchain, conducting high-quality **industry research**
- Affordable and high-quality industry research led by eminent academics at **world's top universities**
- Setting **benchmarks** and **frameworks** to support **governments**, **businesses** and **policymakers** in making evidence-based decisions
- **Bridging Blockchain Industry and Academic gap** by providing a collective voice on the advancement of **Evidence-Based** standards in Blockchain and Distributed Ledgers
- Facilitation in conducting blockchain research projects from **inception to publication**
- A '**one-stop-portal**' coordinating blockchain enterprise research at the world's leading universities and public institutions
- Exclusive, **close-knit networking** opportunities and connection with peers to build evidence-based guidelines for stakeholder organisations
- **Collaborative initiatives** such as workshops, journal clubs, pilot projects and other initiatives
- **Evidence Assessment Frameworks** and strategies to **scientifically evaluate** blockchain projects
- Conduct a **critical appraisal** of the strengths and weaknesses of a **project implementation** at scale.
- **Project management** (both in writing and presentation) with a focus on what policy makers and regulators will be looking for when it undergoes independent review and essential steps to create an impactful, **research backed product, solution or service**
- **Executive education programmes** for senior decision makers
- **Multidisciplinary Training Workshops** (with experts from both industry and academia)
- A vibrant online **member portal operating 24/7**, providing networking opportunities with some of the best and the brightest in the field
- **Share intellectual resources**, discuss new ideas, and work collaboratively on blockchain projects to advance better science
- **Basic Science to Implementation Roadmap** – From concept to implementation and distribution

For more info, visit https://britishblockchainassociation.org/cebb
or Contact cebb@britishblockchainassociation.org

CEBB | Centre for Evidence-Based Blockchain®

Follow us on:

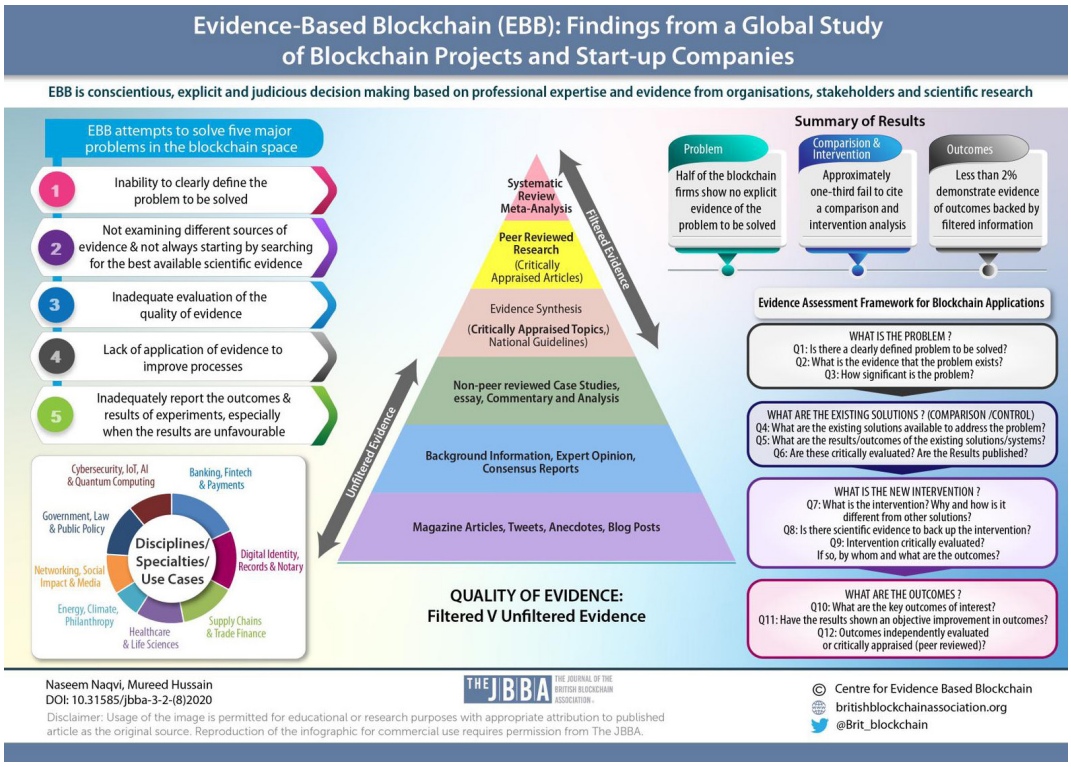
BBA METAVERSE HEADQUARTERS

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

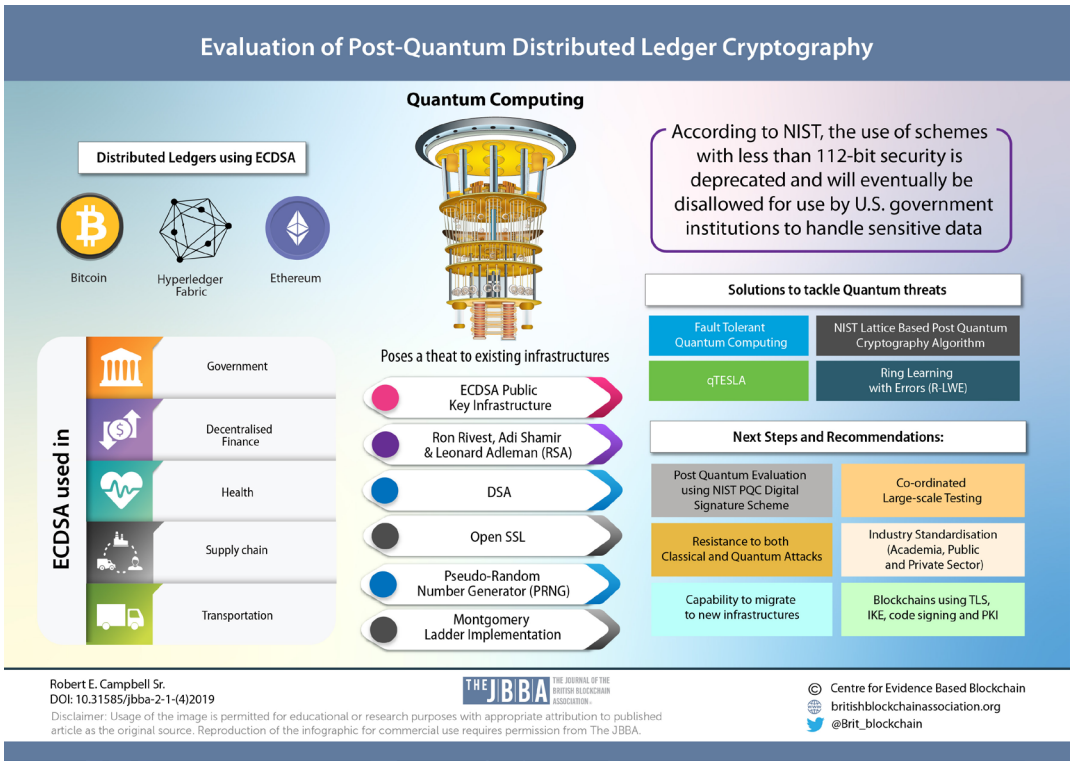
JBBA INFOGRAPHICS

PRODUCED BY

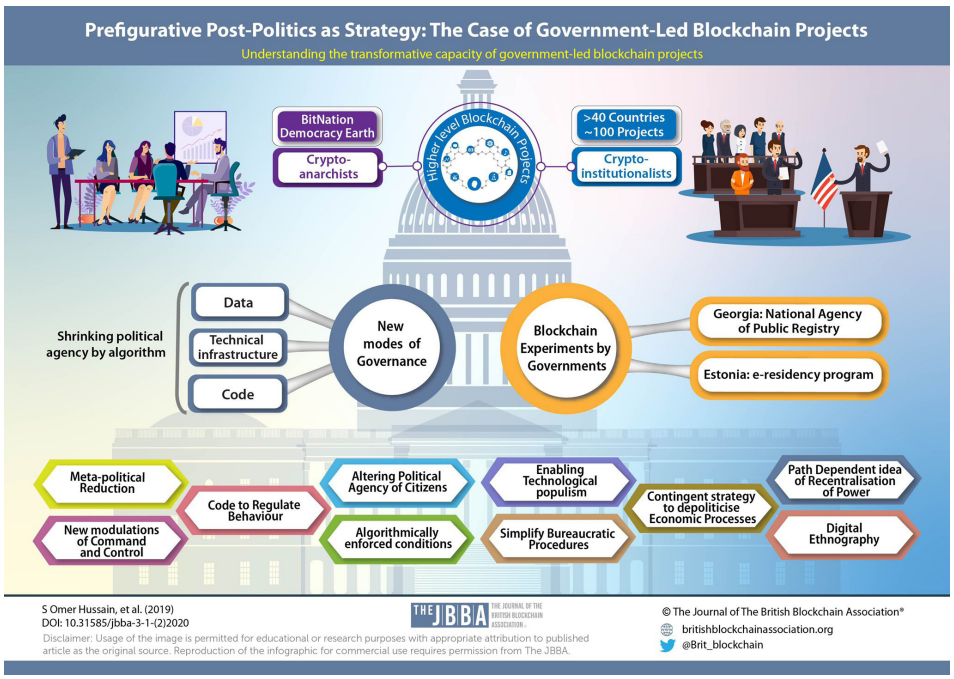
CENTRE FOR EVIDENCE BASED BLOCKCHAIN (CEBB)

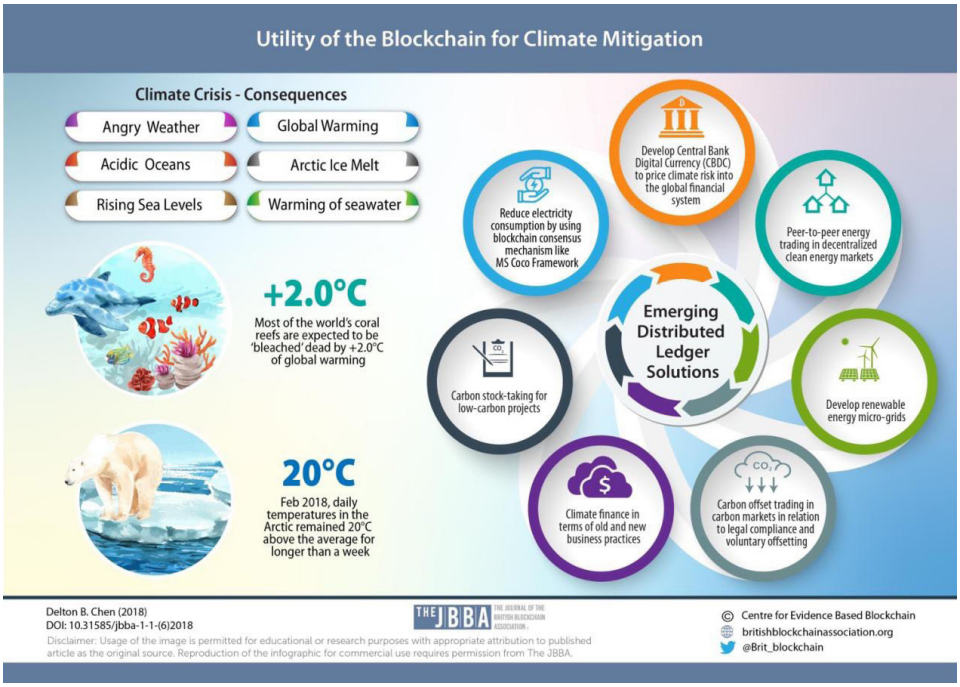


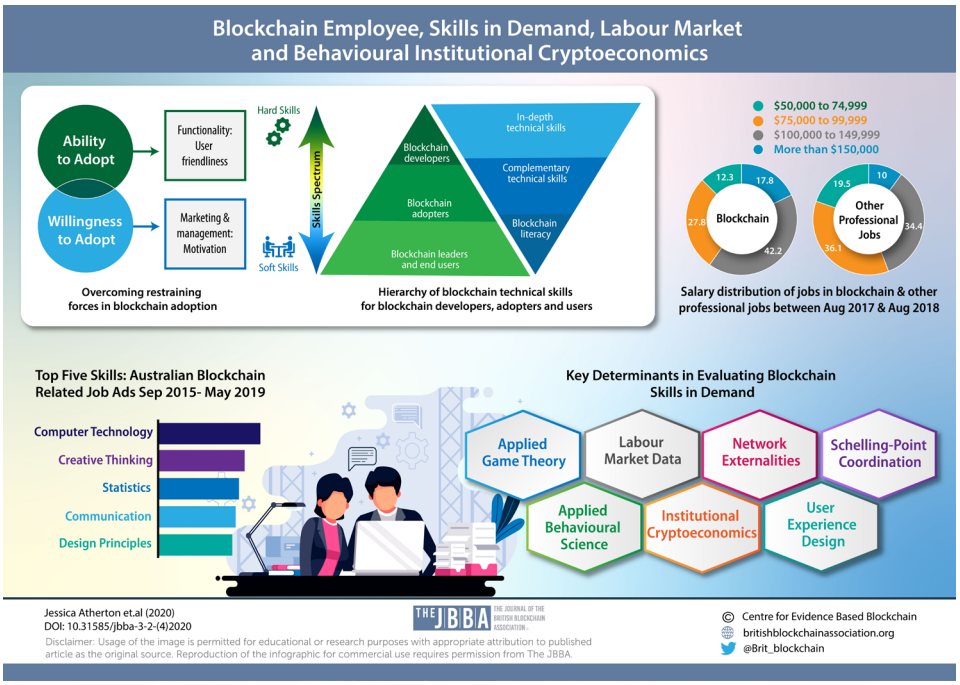
Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020



Robert E. Campbell Sr.
DOI: 10.31585/jbba-2-1-(4)2019







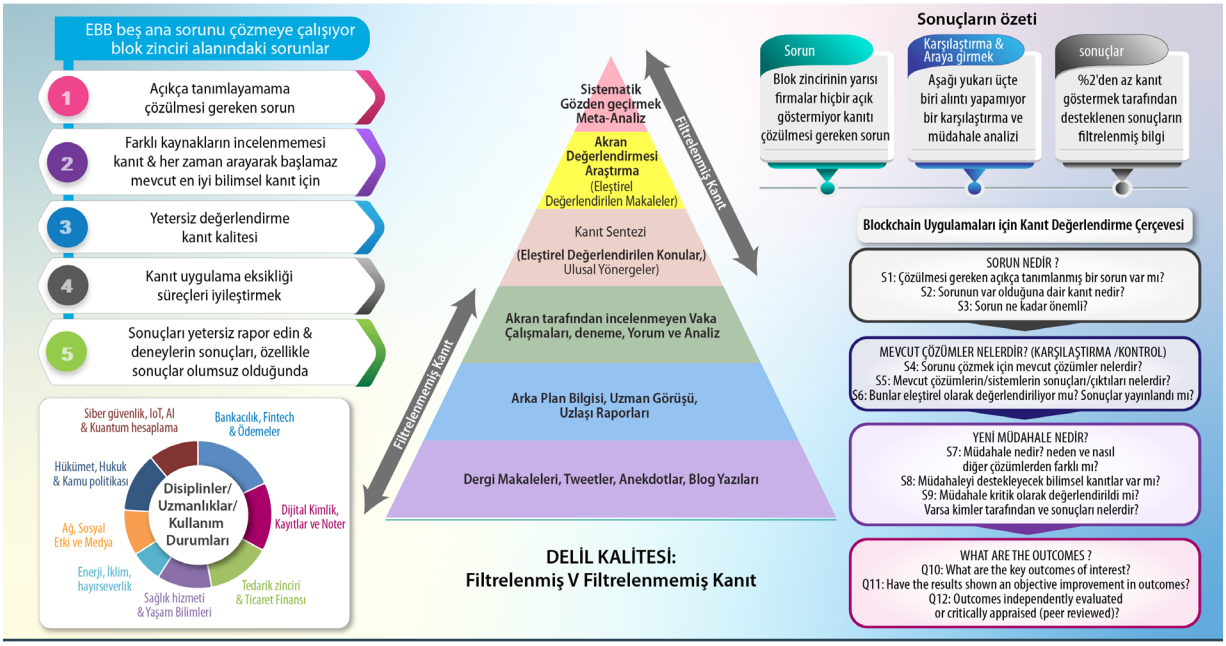
For more info, visit https://britishblockchainassociation.org/cebb

JBBA RESEARCH INFOGRAPHICS AVAILABLE IN MULTIPLE LANGUAGES

TURKISH

Kanıta Dayalı Blok Zinciri (EBB): Küresel Bir Araştırmadan Elde Edilen Bulgular Blockchain Projeleri ve Start-up Şirketleri

EBB, profesyonel uzmanlığa ve kuruluşlardan, paydaşlardan ve bilimsel araştırmalardan elde edilen kanıtlara dayalı vicdani, açık ve mantıklı karar almadır.

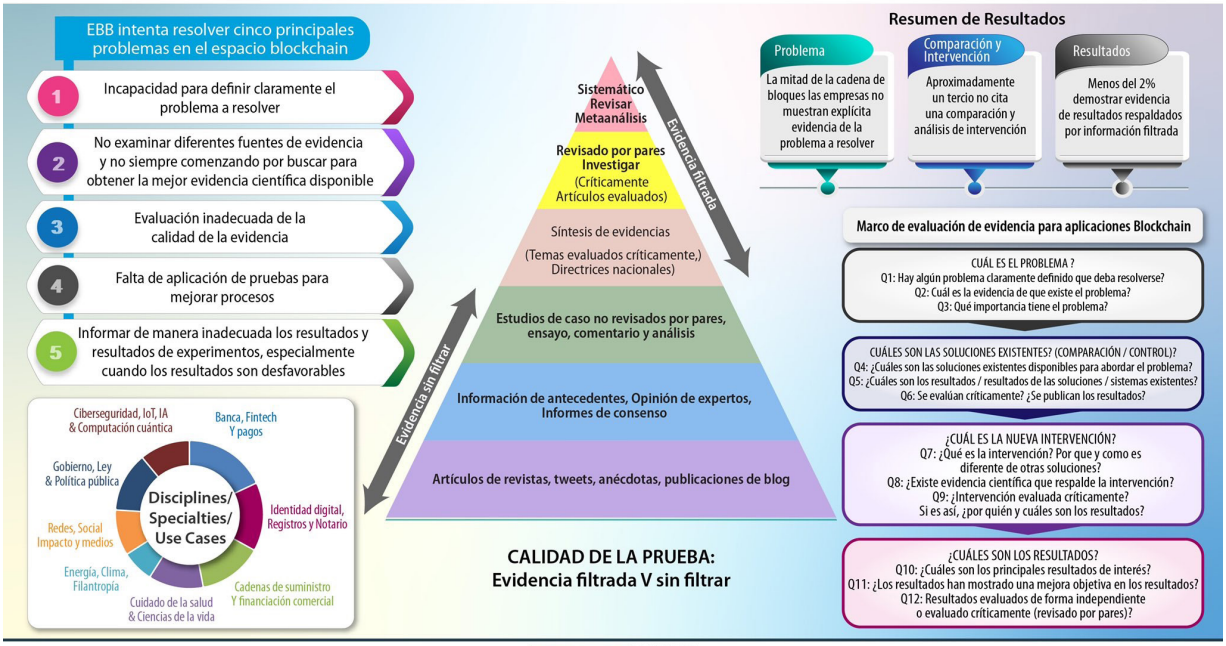


Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020

SPANISH

Blockchain basado en evidencia (EBB): hallazgos de un estudio global de proyectos de blockchain y empresas de nueva creación

EBB es una toma de decisiones concienzuda, explícita y juiciosa basada en la experiencia profesional y la evidencia de organizaciones, partes interesadas e investigación científica.

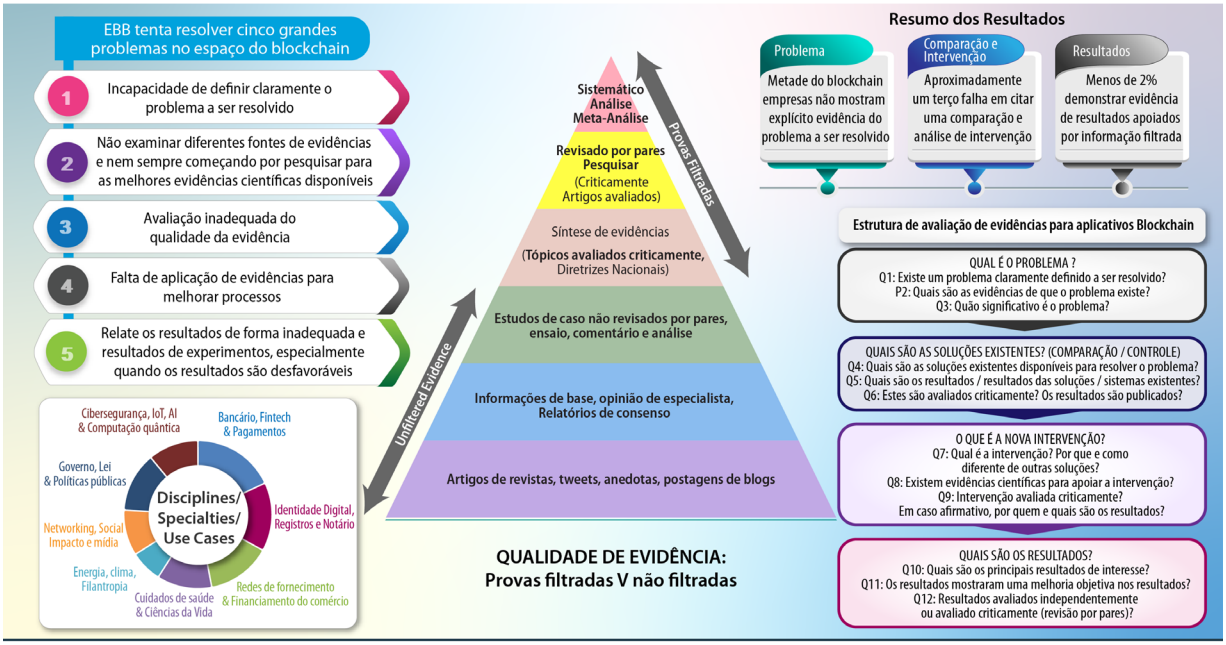


Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020

PORTUGUESE

Blockchain com base em evidências (EBB): descobertas de um estudo global de Projetos Blockchain e Empresas Start-up

EBB é uma tomada de decisão consciente, explícita e criteriosa com base na experiência profissional e evidências de organizações, partes interessadas e pesquisa científica

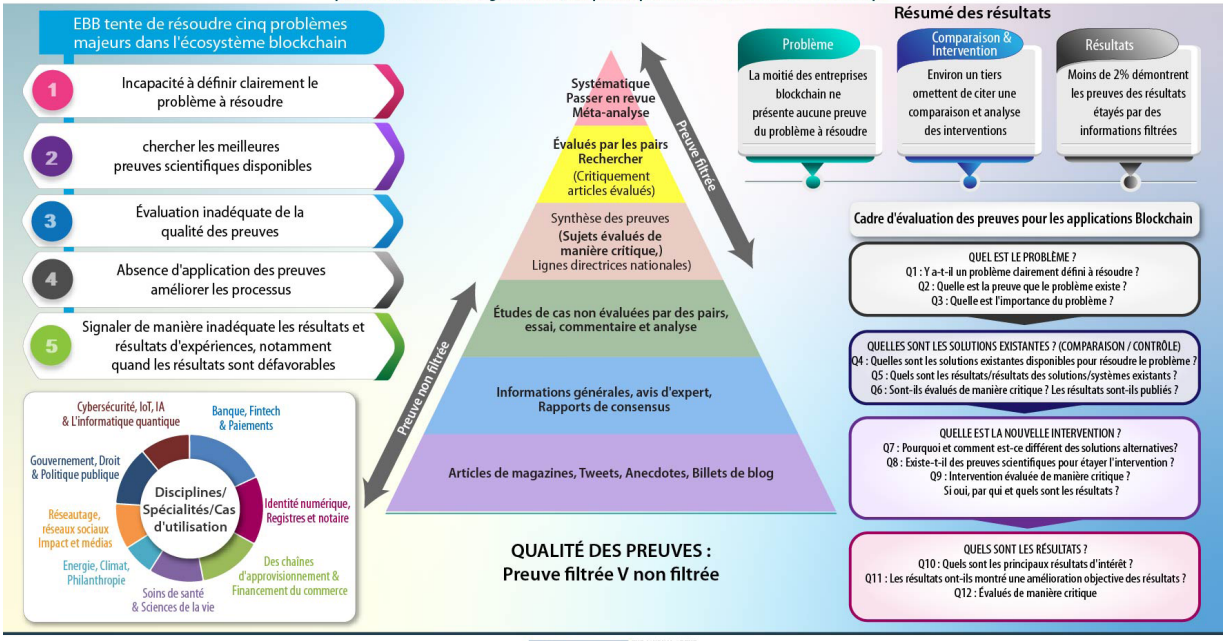


Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020

FRENCH

Blockchain fondée sur des preuves (EBB en anglais): résultats d'une étude mondiale sur des startups et projets blockchain

EBB consiste en une prise de décision informée, explicite et pertinente reposant sur l'expertise professionnelle et les preuves au niveau des organisations, des parties prenantes et de la recherche scientifique



Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020

EDITORIAL BOARD

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

THANK YOU REVIEWERS

The Editorial Board of The JBBA gratefully acknowledges and thanks the reviewers for their time and expertise. The following is the list of reviewers who contributed to the peer review process for the current Issue of The JBBA:

Professor Dr Naseem Naqvi MBE FBBA	UK
Professor Dr Markus Bick	Germany
Dr Aleksei Gudkov	Uzbekistan
Professor Dr Tim Weingaertner	Switzerland
Dr Anish Mohammed	UK
Professor Marc Pilkington FBBA	France
Professor Dr Walter Blocher	Germany
Professor Dr Mary Lacity FBBA	USA
Simon Dyson	UK
Dr Stylianos Kampakis	UK
Professor Dr David LEE, FBBA	Singapore
Professor Dr Rob Campbell FBBA	USA
Dr Mureed Hussain FBBA	UK
Professor Dr Chris Berg	Australia
Professor Dr Ping Wang	USA
Professor Dr Apostolos Kourtis	UK
Professor Dr Chen Liu	Canada
Mathias Haffner	Switzerland
Professor Dr Jeff Daniels	USA

EDITORIAL

It gives me immense pleasure to present to you the **11th issue** of the Journal of The British Blockchain Association (The JBBA, May 2023). This issue features ground-breaking research papers which delve deep into the possibilities, challenges, and opportunities presented by Blockchain and Web3 technologies.

Building an open decentralised metaverse is a massive undertaking that requires addressing many technical, social, and ethical challenges. My essay on *Metaverse for Public Good* shares insights on opportunities, threats, and challenges to building an open metaverse. In the context of a fair, democratic, and all-inclusive metaverse, decentralisation equates to achieving two important objectives:

Permissionless **A**ccess, permissionless **C**reation, and permissionless **T**ransactions - (***ACT***) to the metaverse (the freedom to read, write and own).

Interoperability – the ability to connect a blockchain based wallet that allows transfer of interoperable assets and full ownership of ***CHIDDERS:*** ***C****ommunication*, ***H****istory*, ***I****dentity*, ***D****ata*, ***D****igital* ***A****ssets*, ***E****ntitlements*, ***R****ights and* ***S****ocial Contacts.*

We find ourselves at a critical juncture in the development of Web3 Metaverse. I believe that the Metaverse will be built on a Darwinian approach where people will gradually move to the platforms that offer the most value, freedom, self-sovereignty, and autonomy. We have a unique opportunity to address the shortcomings and correct the flaws of Web2.0 internet. The creation of a decentralized metaverse presents a chance to pursue this vision, which might seem idealistic but certainly not unrealistic, and is something worth pursuing in the interest of building a more inclusive and equitable society. In the web3 metaverse, people will vote with their data and their wallet. A holistic metaverse economy will require the collaboration of various quadruple-helix stakeholders including government, enterprises, academia, and society.

As blockchain technology continues to evolve, the development and adoption of post-quantum algorithms will undoubtedly become increasingly essential. Post-quantum algorithms represent a critical step forward in blockchain security, offering enhanced resistance against the threat of quantum computing. The paper on "*A Performance Comparison of Post-Quantum Algorithms in Blockchain*" by Gan and Yokubov of Brunel University London provides a comprehensive analysis of the performance of various post-quantum algorithms in the context of blockchain. The authors examine the efficiency, security, and scalability of these algorithms and provide valuable insights into their suitability for blockchain applications.

The ability to upgrade smart contracts seamlessly and without disrupting existing functionality will become an increasingly valuable capability of DLT ecosystems. The article "*A Review of Upgradeable Smart Contract Patterns based on OpenZeppelin Technique*" by Shaima Al Amri of University of Southampton et al explores the OpenZeppelin technique for building upgradeable smart contracts. The authors provide a detailed review of the technique and its implementation, highlighting its advantages and limitations and discussing its potential applications in the context of blockchain development.

From market volatility to liquidity risks, understanding and managing the risks associated with Decentralised finance is crucial to ensuring the long-term viability and sustainability of Web3 fintech ecosystems. The research "*DeFi Lending Platform Liquidity Risk: The Example of Folks Finance*" by Hafner et al examines the liquidity risk faced by decentralized finance (DeFi) lending platforms discuss potential solutions to mitigate liquidity risk.

Finally, the conference proceedings section of this issue features selected abstracts presented at the BBA's *5th Blockchain International Scientific Conference ISC2023*. The abstracts provide valuable insights into the cutting-edge developments in the field and showcase innovative approaches to Web3 deployment.

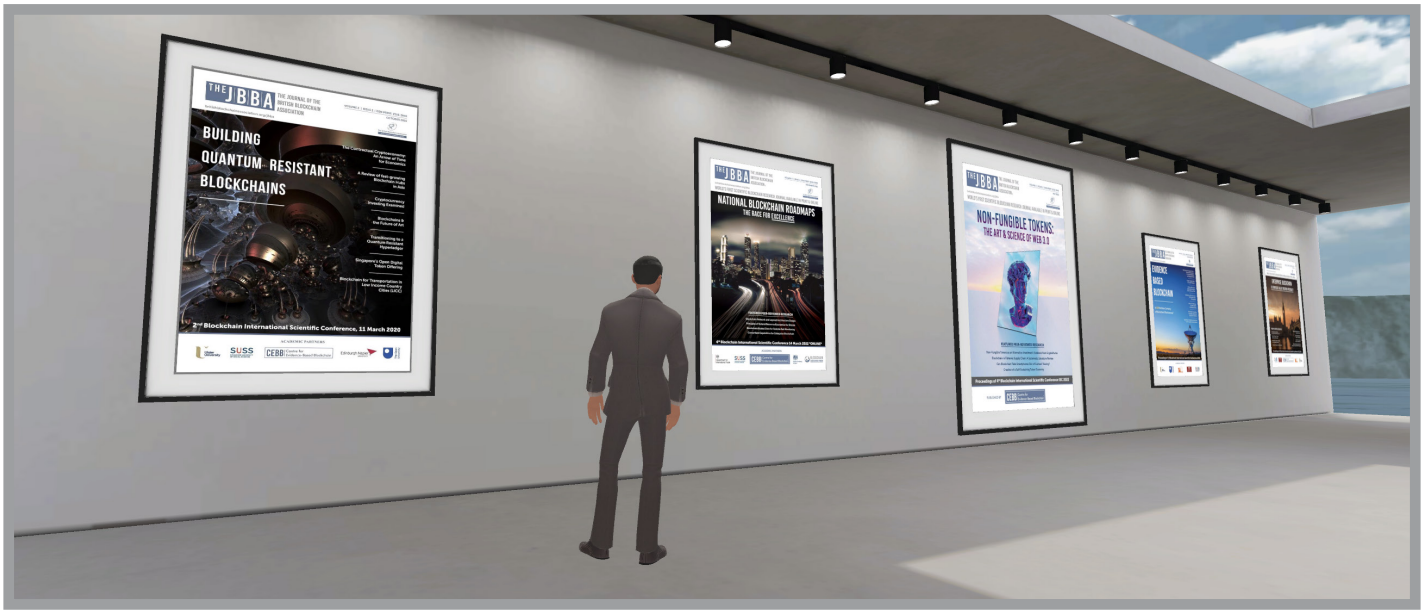
In closing, I would like to express my gratitude once more to the authors as well as the diligent peer reviewers and my fellow editors, who have invested countless hours to elevate the already exceptional quality of The JBBA. Their unwavering commitment has made the JBBA a symbol of quality and excellence. We trust that the articles presented in this issue of The JBBA will offer useful perspectives and encourage further exploration and discussion within the blockchain community. We eagerly anticipate your comments and submissions for forthcoming editions.

Until next time,

Professor Dr Naseem Naqvi MBE
Editor in Chief, The JBBA
President, The British Blockchain Association

JBBA IN THE METAVERSE

Visit us at https://britishblockchainassociation.org/jbba



WHY JBBA?

- We publish in real-time, online, as well as in **PRINT - THE HARD COPIES ARE DISTRIBUTED WORLDWIDE**
- Print copies are available at some of the largest libraries in the world including **BRITISH LIBRARY** and over **500+** more **AROUND THE GLOBE**
- Our authors and readers rate the JBBA as **OUTSTANDING**
- We create **INFOGRAPHICS** of published research papers
- We are in the **METAVERSE**
- We offer **LANGUAGE EDITING AND TRANSLATION** Services to non-native English speaking authors
- We publish **VIDEO ABSTRACTS** of research papers
- We are **ON THE BLOCKCHAIN -** ARTiFACTS Blockchain Portal
- We are **PERMANENTLY ARCHIVED** at PORTICO
- We are **ON PUBLONS** supporting Authors, Reviewers and Editors
- We are **INDEXED IN DOAJ** and **WEB of SCIENCE** (Master Journal List)
- We have a **JBBA YOUTUBE CHANNEL**
- JBBA papers are quoted by Government Officials, Policymakers, Regulators and High Profile Organisations - **CREATING A GLOBAL IMPACT**

THE JBBA
THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

Follow us on:

TESTIMONIALS FROM AUTHORS AND READERS

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

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

"I always enjoy reading the JBBA."

Professor Dr Emin Gun Sirer PhD, Cornell University, USA"

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

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

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

Professor Rob Campbell, Capitol Technology University, USA"

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

Dr Joshua Ellul PhD, Chair, Malta Digital Innovation Authority"

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

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

"This is a very professionally presented journal.

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

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

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

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

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

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

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

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

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

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

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

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

Professor Dr Eric Vermeulen, Tilburg University, The Netherlands

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

Dr Robin Renwick PhD , University college Cork, Ireland

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

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

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-1-(1)2023

A Performance Comparison of Post-Quantum Algorithms in Blockchain

Lu Gan and Bakhtiyor Yokubov
Department of Electronic and Electrical Engineering, Brunel University London, UK

Correspondence: lu.gan@brunel.ac.uk
Received: 30 July 2022 **Accepted:** 12 September 2022 **Published:** 23 September 2022

Abstract

Blockchain and other Distributed Ledger Technologies have triggered widespread research and interest. This is due to their ability to create redundant, transparent, and accountable connections in various application domains while utilising asymmetric cryptography, digital signature, and hash functions. However, the current blockchain system exhibits vulnerability to attacks, especially those staged and actualised using quantum computers leveraging Grover's and Shor's algorithms. There is a need to examine the various algorithms of digital signatures, post-quantum generations of public-key cryptography, and their performance to gain insights into the most suitable way to address the issue. In our review, we examine the performance of different post-quantum public-key generation and digital signature algorithms in blockchain and provide a performance comparison of computing time and memory usage. The research presented here includes application domains where post-quantum blockchain may be used.Disclaimer: Nothing in this paper can be interpreted as constituting financial advice. This paper was written for academic purposes only.

Keywords: *blockchain, post-quantum blockchain, distributed database, digital signature, public-key cryptography*

JEL Classifications: *C61, C88*

1. Introduction

The Distributed Ledger Technology (DLT) concept provides a distributed peer-to-peer system for value transactions with no central authority mediation. The most widely used form of DLT is blockchain, which originated with the peer-to-peer cryptocurrency Bitcoin [1].

Blockchain is expected to change many domains of our life shortly, with the help of consensus in the trustless environment. The applications of cryptocurrencies such as Bitcoin utilise the protocol of proof-of-work in blockchain as a digital signature scheme and a consensus mechanism in transaction verification.

As a result of the development of rapid quantum computers, the digital signature algorithms in blockchain systems subject them to vulnerability to a quantum adversary [2]. Most public-key cryptosystems utilise mathematical problems that are easily solved using quantum chambers using a finite abelian group. The elliptic curve digital signature algorithm (ECDSA) is used in Bitcoin and enabled by the structure of a finite abelian group. The transformation of quantum Fourier is also used in Shor's algorithm to generate exponential speed-up for the problem of discrete logarithm and integer factorisation. Grover's algorithm is used in quantum computers to speed up hashes' production while allowing for the recreation of the complete blockchain.

Various academic researchers have focused on digital signature systems in the post-quantum era to prevent quantum attacks witnessed in recent years. This has influenced the emphasis of this study in analysing how various signature algorithms can be used to create blockchain systems immune to computer attacks. There is also a comprehensive comparison between digital signatures and schemes of asymmetric encryption in the post-quantum era with respect to their performance and properties.

2. Post-Quantum Blockchain Proposals

Various authors have proposed post-quantum blockchain or modifications to existing blockchain to address the quantum threat.

In 2008, Gentry et al. introduced the first lattice-based signature technique that is probably safe in the random oracle based on the SIS issue [3]. Their core thesis is that lattices allow for natural and inherent "trapdoors" with various valuable cryptographic applications. Yin et al. [4] introduce a new transaction authentication scheme based on lattice-based cryptography that can resist quantum attacks while remaining lightweight in the blockchain system. The signature length on their schema is O(1), which is better suited for storing in a blockchain than other signature lengths. The authors of [5] proposed a safe lattice-based multi-signature system under the ring variant of the short integer solution (Ring-SIS) assumption in the random oracle model. They define a functional lattice-based multi-signature scheme (PLMS), which they extend to allow public key aggregation in a small signer group environment. Their schemes are based on the practical digital signature scheme and follow the FS-like digital signature structure. In 2019, Esgin at al. [6] provided a post-quantum RingCT protocol based on computational lattice issues such as M-SIS and M-LWE. Their initial contribution to the field is the introduction of the most minor ring signature to date, namely M-SIS and M-LWE, based on conventional lattice assumptions. The authors of Ref. [7] propose a new lattice-based signature scheme for generating sub-private and sub-public keys based on bonsai tree technology. Furthermore, the security of the proposed signature scheme is based on the short integer solution (SIS) problem.

3. Blockchain Overview

In general, blockchain can be considered a decentralised and distributed data structure. Blockchain allows non-trusted members to interact with each other in a verifiable manner without third-party authority. Bitcoin,

the first electronic peer-to-peer cryptocurrency in the blockchain context, was introduced in 2008 by Nakamoto [1]. Each block in a blockchain is identified with a cryptographic hash. Each block refers to the previous block's hash, back to the first (genesis) block, thus creating a blockchain or chain of blocks (see Figure 1).

Three types of blockchain are available based on their functioning: private, public, and consortium. In permissioned or private blockchain, only a limited number of users can participate in consensus and have the right to validate transactions. In contrast, anyone can join the network and validate permissionless or public blockchain transactions. Consortium blockchains are permissioned blockchains managed by a group of organisations rather than a single entity, as is the case with private blockchains. As a result, consortium blockchains have more decentralisation than private blockchains, resulting in higher levels of security. Bitcoin, Ethereum, Litecoin, and most cryptocurrencies are well-known implementations of public blockchains. Multichain is considered an open platform for developing and implementing private blockchains.

One of the primary benefits of blockchain technology is its ability to validate transaction trustworthiness in a decentralised environment without the use of intermediaries via consensus algorithms. The different consensus mechanisms can be used depending on the blockchain type. Proof-of-work (PoW), proof-of-stake (PoS), and Byzantine fault tolerance (BFT) are the most common examples of consensus algorithms. PoW protocols require miners to solve challenging computational tasks to create a block. PoS protocols distribute stake blocks to miners in proportion to their current wealth. BFT refers to the process of achieving consensus between two nodes communicating securely over a distributed network in the presence of malicious or misleading nodes.

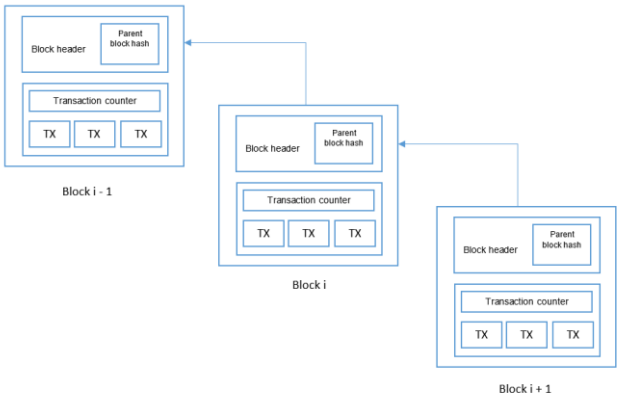


Figure 1. Block structure in a blockchain.

One of the main advantages of blockchain is smart contracts in its applications. In 1994, Nick Szabo proposed the concept of a smart contract [8]. It was described as a computerised transaction protocol that performs a contract's terms. A smart contract satisfies common conditions, minimising the need for trusted intermediaries. It can be considered a digitised form of a legal contract in simple terms. Smart contracts have the following properties: autonomy, trust, backup, and savings.

4. Blockchain Applications

Blockchain technology can be implemented in various applications, including finance, insurance, Internet of Things (IoT), healthcare, voting, supply chain, etc.

4.1 Finance

The global financial system moves trillions of dollars and serves billions of people every day. Nevertheless, the system is riddled with problems, increasing costs through fees and delays, increasing friction through redundant and onerous paperwork, and providing opportunities for fraud and crime. Blockchain technology can ease business operations while still generating a level of security and trustable records of agreements and money transfers in the banking and financial service domains.

4.2 Healthcare

Blockchain is a technology that plays a critical role in the healthcare industry, with numerous applications, such as the traceability of medicine and patients' medical data records. In the pharmaceutical industry, medicine counterfeiting is a significant issue. According to a report by the World Health Organization (WHO), counterfeit or substandard medicines make up about 50% of the global medicine market, with 25% being consumed in developed or developing countries [9]. These medicines can lead to severe problems in a patient's life rather than treating the disease. Blockchain promises to overcome the above challenge by making all the transactions immutable and timestamped. Using blockchain, it is possible to track medicine and make information tamper-proof.

One of the primary healthcare concerns is maintaining patient data integrity. Each patient needs a different treatment strategy for a common disease depending on their physical variability. Their complete medical history needs to be accessible to provide individual treatment. On the other hand, medical data are sensitive and necessitate a secure sharing platform. The current medical record-keeping system lacks both privacy and interoperability. Keeping patients' medical data safe and secure is currently one essential blockchain application. Blockchain can establish a secure and robust framework for storing patients' medical data, resulting in better service while lowering treatment costs.

Compliance requirements for healthcare blockchains depend on things like what sensitive data are stored on the blockchain, what the data usage agreements are, and where the blockchain nodes and decentralised ledgers that store this information are physically located. For example, HIPAA (Health Insurance Portability and Accountability Act of 1996) [10] rules apply when a blockchain stores PHI (Protected Health Information) about US citizens. When blockchains store sensitive information about patients who live in the European Union (EU), the GDPR (General Data Protection Regulation) [11] applies.

4.3 Internet of Things

The Internet of Things (IoT) is crucial in transforming the physical world into a massive information system. IoT can support different applications in industries, such as logistics, food industry, manufacturing, etc. IoT aspires to increase performance and efficiency, decrease machine downtime, and improve product quality. The IoT system currently faces the following challenges: heterogeneity, poor interoperability, resource limitations, and security and privacy vulnerabilities. The distributed architecture of IoT is a critical challenge. In an IoT network, each node is typically a potential point of failure that can be used to launch cyber-attacks, such as distributed denial-of-service (DDoS) [12]. Moreover, the centralised communication of IoT devices may lead to a central point of failure. Data confidentiality, integrity, and authentication need to be addressed in the IoT environment [13].

Blockchain seems to be a perfect complement to IoT, with improved interoperability, privacy, security, reliability, and scalability. Blockchain can be utilised in several domains of IoT, such as "Smart City," "Smart Home," "Smart Industry," and "Smart Grid."

4.4 Electronic Voting

Many studies have been conducted on electronic voting systems to minimise the cost of running an election while ensuring election integrity by meeting security, privacy, and compliance requirements. Replacing the traditional pen-and-paper system with a new election system can reduce

fraud while making the voting process traceable and verifiable.
DLTs, such as blockchain, provide a decentralised node for an electronic voting system with the help of an end-to-end verification process [14]. Blockchain is an appealing alternative to traditional voting systems due to decentralisation, non-repudiation, and security protection [15].

4.5 Supply Chain

A supply chain is a network that links a business and its vendors to produce and distribute particular goods to the buyer. Several companies can benefit by utilising blockchain in supply chains to store, monitor, and optimise immutable and reliable data. By storing serial numbers or other product information, such as price, location, date, and quality, on a blockchain, we can obtain a secure and transparent supply chain and eliminate counterfeit products. Moreover, we can check and trace in real-time supply chains, from raw materials to ready goods, speeding up recording and verification operations. The blockchain-based supply chain can enhance trust between involved parties and final consumers by saving all the immutable data on a blockchain.

Blockchain is ideal for establishing a chain of custody. Once written to the record, chain-of-custody transactions are immutable because they constitute a tamper-proof record. This chain of custody is also accessible to all parties on the blockchain, so parties need only read the blockchain to verify it. A chain-of-custody solution promotes the openness, efficiency, and accountability of supply chain processes that are usually unclear.

Through greater transparency and enhanced product traceability, blockchain can help reduce or even prevent fraud in the supply chain. It is extremely challenging to manipulate the blockchain, which is an immutable ledger that can only be updated and validated through network consensus. And if a product is recorded on blockchain, its origin can be easily determined because the data is on a shared, distributed ledger.

5. Post-Quantum Cryptography

According to current knowledge, Shor's and Grover's algorithms do not violate the new generation of public-key algorithms known as post-quantum cryptography. The primary objective of post-quantum cryptography is to create cryptosystems that are secure for both quantum and non-quantum computers while also being able to communicate with existing networks. In this section, the four types of post-quantum cryptosystems are studied.

5.1 Code-based cryptosystem

The algorithmic primitive in a code-based cryptosystem uses error correction codes. An asymmetric encryption mechanism, introduced in 1978 by Robert McEliece [16], was the first of these systems whose security is based on the syndrome decoding problem [17]. The public key is a random generating matrix of a randomly permuted private key version that is an arbitrary binary irreducible Goppa code. The ciphertext is a codeword with certain flaws that can only be removed by the private key owner (the Goppa code). Even though certain parameter adjustments have been necessary during the last three decades, no attack has been identified as posing a substantial danger to the system, even on a quantum computer. McEliece's system is very fast because both the encryption and decryption procedures are simple, which is beneficial for completing quick blockchain transactions. McEliece's cryptosystem, on the other hand, requires the storage and execution of large matrices that serve as public and private keys that can require between 100 kilobytes and several megabytes, and this may be a constraint for resource-constrained devices.

Harald Niederreiter developed a knapsack-type cryptosystem, a dual variant of the McEliece public key cryptosystem in 1986 [18]. Unlike the McEliece cryptosystem, Niederreiter proposed encoding the message into the error vector instead of representing it as a codeword. The dual variant uses the smaller public key size, while slowing down encryption and decryption. The security of both public key cryptosystems is equivalent.

5.2 Hash-based cryptosystem

Like any other digital signature technique, hash-based digital signature systems rely on a cryptographic hash function. The security of these methods is determined by the hash function's collision resistance rather than the difficulty of a mathematical problem. Collision-resistant hash functions might be considered a prerequisite for a digital signature method that can sign many documents with a single private key. This method dates back to the late 1970s, when Lamport developed a one-way function-based signature scheme [19]. This schema uses a one-way function and the security parameter n is a positive integer number

$$f: \{0,1\}^n \rightarrow \{0,1\}^n, \quad (1)$$

and a cryptographic hash function

$$g: \{0,1\}^* \rightarrow \{0,1\}^n \quad (2)$$

The key and signature generation of Lamport's one-time signature scheme is very efficient, but the signature size is large.

Then, hash-based signature schemes were invented by R. Merkle [20]. Variants of the extended Merkle signature method (XMSS) [21], such as XMSS-T and SPHINCS [22], are now seen to be promising hash-based signature schemes for the post-quantum period, derived from the Merkle tree scheme. Due to their performance, XMSS and SPHINCS may be impractical for blockchain applications. However, several improvements have been made, making hash-based signatures a potential alternative to RSA and elliptic curve signature systems.

5.3 Lattice-based cryptosystem

Lattice-based cryptographic constructs promise post-quantum cryptography since they provide solid security proofs based on worst-case hardness, relatively fast implementations, and considerable simplicity. Furthermore, lattice-based cryptography is resistant to quantum computers. A lattice is a set of points in an n-dimensional space with a periodic structure.

A lattice is a set of points in an n-dimensional space with a periodic structure. Given n linearly-independent vectors $v_1,\ldots,v_n \in R^n$, the lattice generated by $v_1,\ldots,v_n$ is given by an integer combination of these vectors in n-dimensional space, with $v_1,\ldots,v_n$ forming the basis of the lattice [23]

$$\Lambda(\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}) := \left\{ \sum_{i=1}^{n} \alpha_i \boldsymbol{v_i} \,|\alpha_i \in \mathbb{Z} \right\} \quad (3)$$

The assumed hardness of lattice problems, the most fundamental of which is the shortest vector problem (SVP), underpins lattice-based cryptographic constructs. We were given a lattice represented by an arbitrary basis as input, and we aimed to find the shortest nonzero vector in it. Other analogous lattice-related problems, such as the closest vector problem (CVP) or the shortest independent vectors problem (SIVP) [24], are currently inefficiently handled by quantum computers. The ones based on a short integer solution (SIS) problem [25] appear to be promising among the several lattice-based signature schemes described in the literature due to their decreased key size. According to specific performance evaluations, Bimodal Lattice Signature Scheme B (BLISS-B), which is based on the hardness of the SIS problem, has one of the top performances for lattice-

based signature cryptosystems ranked among the RSA and ECDSA [26]. On the other hand, BLISS-B is vulnerable to caching attacks that can retrieve the secret signing key after 6,000 signature generations [27]. Aside from BLISS, other lattice-based signature systems in the literature rely on the SIS problem but were designed to generate secure and efficient blockchains [28].

5.4 Multivariate-based cryptosystem

The multivariate public-key cryptosystem is based on multivariate functions over a finite field instead of single-variable NP-hard or NP-complete functions. This family is regarded as one of the key PKC families capable of withstanding even the most powerful quantum computers in the future. The public is the set of quadratic polynomials:

$$P = (p_1(w_1, \dots, w_n), \dots, p_m(w_1, \dots, w_n)), \quad (4)$$

where each p_i is a nonlinear polynomial in $\mathbf{w} = w_1, \dots, w_n$:

$$z_k = p_k(\boldsymbol{w}) := \sum_i P_{ik} w_i + \sum_i Q_{ik} w_i^2 + \sum_{i>j} R_{ijk} w_i w_j \quad (5)$$

At any given value, the evaluation of these polynomials corresponds to either the encryption or verification procedure.

The main drawback of multivariate schemes is the large public key size. Further research is needed for better decryption speed and reduced key size [29]. Currently, among the most promising multivariate-based schemes include those based on the usage of square matrices with random quadratic polynomials, Matsumoto algorithm-derived Imai's cryptosystems, and hidden field equation-based schemes (HFE) [30], [31], [32], which can generate signatures size similar to RSA- and ECC-based signatures.

6. Signature Algorithms

This section describes the ECDSA signature scheme and the NIST Round 3 finalist signature schemes Falcon, Dilithium, and Rainbow.

6.1 Elliptic Curve Digital Signature Algorithm

In 1992, Scott Vanstone proposed the ECDSA as a variant of the digital signature algorithm (DSA) that incorporates elliptic curve cryptography [33]. It is a very efficient equation that is based on public-key cryptography. ECDSA is commonly used in several security systems and is widely known in encrypted communication applications, as well as being the foundation of Bitcoin protection.

The following steps are used in ECDSA:

1) Key generation.

The key pair of an entity A is associated with EC domain parameters $D=(q,FR,a,b,G,n,h)$. The entity A must be confident that the domain specifications are correct before generating keys. The following steps are performed by each entity A:

a) Select an integer number d randomly from the range $[1,n-1]$.
b) Calculate $Q = dG$.
c) Q represents the public key, and d represents the secret key.

2) Signature generation.

An ECDSA signature is built using several domain parameters, a secret key d, and a message m. The outputs are the signature(r,s), where r and s are integer signature components, and continue as follows:

a) Select an integer k randomly from the range $[1,n-1]$.
b) Calculate $kG = (x_1,y_1)$ and $r = x_1 \mod n$. If $r=0$ then go to step 1.
c) Evaluate $k^{-1} \mod n$.
d) Convert the result from SHA-1(m) into an integer number c.
e) Calculate $s= k^{-1} (c+dr) \mod n$. If $s=0$ then go to step 1.

3) Signature verification.

B obtains a copy of A's public key and domain parameter to verify A's signature (r,s) on message m, and then performs the following steps:

a) Ensure that r and s are in the range $[1,n-1]$.
b) Convert the result from SHA-1(m) into an integer number c.
c) Calculate $w = s^{-1} \mod n$.
d) Calculate $l_1=cw \mod n$ and $l_2 = rw \mod n$.
e) Calculate $X= l_1 G+ l_2 Q$. if $X=O$, reject the signature. Else, compute $v = x_1 \mod n$ where, x_1 is an integer converted from x-coordinate x_1 of X.
f) if $v = r$, verify the signature.

6.2 Falcon Signature Algorithm

Falcon is a lattice-based signature scheme over NTRU that NIST selected as a finalist in NIST PQC contest Round 3. Falcon utilises the GPV framework with NTRU lattices as a post-quantum signature algorithm, and as a trapdoor sampler, it uses a novel technique known as fast Fourier sampling [34].

Gentry, Peikert, and Vaikuntanathan created the GPV framework in 2008 to obtain secure lattice-based signatures.

The following is a high-level description of that framework:

- The public key used to generate q-ary lattice Λ, which contains a full-rank matrix $A \in Z_q^{n \times m}$ where $m > n$;
- The private key is used to generate $\Lambda_q^{\perp}$, which contains $B \in Z_q^{m \times m}$, and is the lattice orthogonal to Λ modulo q. At the same time, the rows of A and B needs to be a pairwise orthogonal: $B \times A^t = 0$;
- The message m's signature is a short value $s \in Z_q^m$ and it should verify $sA^t = H(m)$;
- To compute a valid signature, first compute a preimage $c_0 \in Z_q^m$, which verifies $c_0 A^t = H(m)$, where c_0 is not necessarily required to be short and $m \geq n$. Then, a vector $v \in \Lambda_q^{\perp}$ close to c_0 is computed using matrix B. $s=c_0-v$ is valid signature.

Falcon, like other signature algorithms, has three phases:

1) Key pair generation.

f and g short polynomials are chosen randomly using an appropriate distribution. The matching F and G polynomials are then founded in the solution of the NTRU equation. In this case, the public key is a basis for a $2n$ dimension lattice, where n is typically 512 or 1024.

$$\begin{bmatrix} -h & I_n \\ qI_n & O_n \end{bmatrix} \quad (6)$$

The corresponding private key is another basis for the same lattice.

$$\begin{bmatrix} g & -f \\ G & -F \end{bmatrix} \quad (7)$$

$g, f, G,$ and F need to fulfil the following equations.

$$h = g/f \bmod w \bmod q \quad (8)$$

$$fG - gF = q \bmod w \quad (9)$$

2) Signature generation.

The message and a random nonce are first hashed into polynomial c modulo w. Next, a pair of short polynomials (s_1, s_2) are generated using the knowledge of the secret lattice basis (*f, g, F, G*) such that $s_1 = c\text{-}s_2$ h mod w mod q, where signature is s_2.

3) Signature verification.

After computing s_1 using the hashed message c and s_2, it should be verified that (s_1, s_2) is a short vector with the process integer computations mod q.

6.3 Dilithium Signature Algorithm

The CRYSTALS-Dilithium lattice-based signature proposed by Ref. [35] is the next finalist in the NIST.

The Dilithium signature algorithm is summarised in the steps below.

1) Key pair generation.

Initially, a matrix A with polynomial entries in the ring $Rq=(Z_q[X])/(X^n+1)$ is generated, where n is a power of 2. Then, the two private key samples s_1 and s_2 are generated randomly. Finally, the second part of the public key is calculated from $t=As_1 + s_2$, where the public key is (A,t) and the private key is (s_1, s_2).

2) Signature generation.

The potential signature is calculated as $z = y + cs_1$, where y is a vector of polynomials and the challenge c is generated using digest and a vector w1. y need to be less than the parameter γ_1. w_1 is then high-order bits of the coefficients of vector Ay, and every coefficient w in Ay can be written as $w= w_1 \cdot 2\gamma_2 + w_2$, where $|w_2| \leq \gamma_2$. Thus, w_1 is the vector, including w_1. Afterwards, the rejection sampling is used to avoid the dependency of z on the secret key and prevent the leakage of information about the secret key.

3) Signature verification.

The verification process computes w_1' and accepts if all the coefficients of z are less than γ_1-β from Az-ct and if c is the hash of the message and w_1'.

6.4 Rainbow Signature Algorithm (has been broken)

Rainbow's new multivariable polynomial signature scheme was proposed in 2005 [36]. The Rainbow signature algorithm can be defined in the below steps:

1) Key generation.

The private key consists of two randomly chosen invertible affine linear maps, L_1 on $k^{n\text{-}v1}$ and L_2 on $k^{n\text{-}v1}$, and the map F= (f_{v1+1} (x),…,f_n (x)). The number of polynomial components of F is $m = n\text{-}v_1$. The public key is the composed map $\bar{F}(x) = L_1 \circ F \circ L_2$.

2) Signature generation.

For signing a document, firstly, it needs to be considered as an element $Y' = (y_1', \ldots, y'_{1\text{-}v1})$ in $k^{n\text{-}v1}$). The signature of Y' is the inverse of L_2 from this equation.

$$L_1 \circ F \circ L_2 = \bar{F}(x) = Y' \quad (10)$$

The signature is denoted as $X' = (x'1, \ldots, x'n)$.

3) Signature verification.

The following equation needs to be checked to verify the signature.

$$\bar{F}(X') = Y' \quad (11)$$

The Rainbow signature scheme was since proven to be insecure, where the Intersection Attack and the Rectangular MinRank attack proposed by Beullen are shown to break the signature scheme in several days [37].

7. Analysis

Present-day research is focused on post-quantum blockchain. The transition from pre-quantum to post-quantum blockchain necessitates careful consideration of the steps involved. In this section, we compare performance of pre-quantum and the most promising post-quantum public-key encryption and digital signature schemes that can be utilised in blockchain nodes.

There is no comprehensive answer to the present uncertainties. For instance, varying quantum algorithms are created, bringing forth unprecedented attacks. It is also impossible to evaluate highly secretive projects, thereby presenting a significant loophole that can be used to conduct computer attacks. The performance features are inaccessible, thereby hindering their improvement. Present encryption systems are being rendered obsolete by the continuing advances in quantum computing. The most profound threat of quantum computers has been reported to be targeting the ECDSA systems relied upon by Distributed Ledger, Bitcoin, and other blockchain applications.

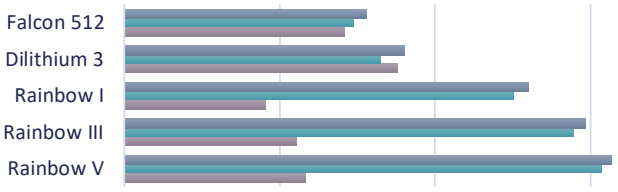
The existing public-key cryptography based on the ECDSA is evidently broken. This has subjected AES cryptography to a significant reduction in bit security due to the era of quantum computing. This study evaluated three signature techniques of post-quantum cryptography that could potentially replace the current blockchain signature scheme.

Table 1. ECDSA [38].

Software/ Scheme	Computation Assumption	Bit Security	Key Size (B)	Signature Size(B)
ECDSA (P-256)	Elliptic Curve Discrete Logarithm	128	pk: 64 sk: 96	64

The ECDSA algorithms used in the Distributed Ledger and Bitcoin technologies were examined. Table 1 represents the parameters of ECDSA that were applied as the points of comparison for the secret key, public key amount size, and security bits of the quantum as the variables that can be separately changed. The National Institute of Standards and Technology (NIST) maintains that schemes that have security lower than 112-bit are obsolete and likely to be prohibited from sensitive data handling. The

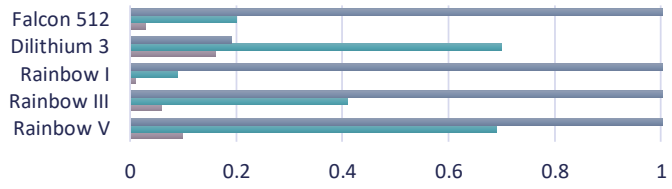
encryption and decryption speeds are crucial factors. An assessment was carried out of the PQC finalists drawn from Round 3 of the NIST for harmonisation and potential replacement in the digital signature algorithms of the blockchain.



	Rainbow V	Rainbow III	Rainbow I	Dilithium 3	Falcon 512
Private Key (B)	1,885,400	861,400	157,800	4,000	1,281
Public Key (B)	1,375,700	611,300	101,200	1,952	897
Signature (B)	212	164	66	3,293	666

Figure 2. Memory usage of post-quantum signature cryptosystems [34]–[36]. The chart is given in logarithmic scale base 10.

Figure 2 compares the post-quantum signature schemes concerning the public key, private key, and size of the signature in bytes. Among all the signatures, Dilithium is the largest. The lattice-based cryptosystems (Dilithium and Falcon) have smaller key sizes than the cryptosystem Rainbow, which is multivariate-based, deriving into large public keys with limited signatures.



	Rainbow V	Rainbow III	Rainbow I	Dilithium 3	Falcon 512
Key Gen. (ms)	121.05	54.59	8.98	0.19	7.49
Signature Gen. (ms)	0.69	0.41	0.09	0.7	0.2
Signature Ver. (ms)	0.1	0.06	0.01	0.16	0.03

Figure 3. Execution time of post-quantum signature cryptosystems [34]–[36].

The speed of the key pair generation, signature execution, and verification process of each post-quantum scheme that passed to the third round of NIST calls are given in Figure 3. All schemes were measured on an Intel(R) Core(TM) i7-1165G7 @ 2.80GHz. Dilithium 3 was the fastest for key generation, while Rainbow I offered the fastest signature generation and verification.

The lattice-based signature schemes are more promising due to their smaller key size, especially those based on the short integer solution (SIS) problem in the literature. Performance evaluations indicated that Falcon is among the best lattice-based performances in cryptosystem signing compared to the ECDSA and RSA. This has been attributed to its foundation in the hardness of the SIS problem.

Smaller keys are required in the schemes of lattice-based signatures than in the schemes based on a multivariate signature and result in slightly larger signatures. Among the studied lattice-based signatures, Falcon was found to have the shortest signature lengths and shortest key sizes. Dilithium systems were quick but had enormous signatures and key sizes. Based on the outlined analysis, most researchers have deduced that the Falcon signature scheme in blockchain is more promising.

8. Sample Implementation

The sample blockchain implementation was adapted from [39]. The Open Quantum Safe (OQS) library was used in this implementation to integrate the quantum-safe signature into the Hyperledger Fabric blockchain.

Hyperledger Fabric is a well-known and adaptable solution for creating private Distributed Ledger platforms. Fabric achieves high performance and scalability by utilising the execute–order–validate paradigm, which was first proposed to improve the performance of state machine replication [39]. Access control and identity management of Hyperledger Fabric are handled by a membership service provider (MSP) whose cryptographic interface only supports standard PKI authentication methods, such as the RSA and ECDSA classical signatures. Hyperledger Fabric is considered an industry-deployed blockchain, with 20,000 transactions per second [40].

The set of definitions used in Hyperledger Fabric blockchain are as follows:

- **Membership Service Provider (MSP)**. The membership service provider (MSP) is in charge of creating digital identities for the organisation's peers and users. For a new entity to participate in a channel, peers' identities must be configured in an existing network.
- **Fabric CA**. Fabric CA is an MSP implementation that provides a mechanism for registering users and issuing them digital certificates. Fabric CA is typically executed within a Docker container.
- **Peer (endorser)**. An endorser peer is designed to simulate transactions and prevent unstable or non-deterministic transactions from passing through the network. In the form of a transaction, a transaction proposal is sent to an endorser. Every peer who endorses it is also a committing peer.
- **Orderer**. An orderer verifies the signatures of all endorsers and uses a consensus protocol to organise the transactions into a block candidate for each set of transactions. Before returning the block candidate to peers for final validation and inclusion in the ledger, orderers sign it.
- **Transaction**. An authorised end-user performs a read/write operation on the ledger. There are three types of transactions: deploy, invoke, and query.

LibOQS [41] is used to implement post-quantum cryptographic signature algorithms in Hyperledger Fabric. LibOQS is an open-source C library used for quantum-resistant cryptographic algorithms and prototype integration into protocols and applications such as OpenSSL. Because LibOQS is written in C and Hyperledger Fabric is written in Go, a CGO wrapper has been written around LibOQS.

Implementation is carried out by a network with one orderer, one client, and two peers. The client sends all the transactions to a single peer, and the second peer plays the role of the endorser.

The chaincode from [40] was used as a simple balance account that allows for sending values between accounts. The standard cryptographic set-up only uses the ECDSA defined over the NIST curve P-256 and provides 128-bit classical security. This was then compared with the hybrid schemes that combined the ECDSA with post-quantum schemes.

Table 2 estimates how much time each signature scheme spent on hashing and LibOQS functions for each block compared to the scheme's public key plus signature size.

Even though qTesla is no longer in the running for NIST, it decided to assess its performance because it was specifically mentioned in recent work on post-quantum Hyperledger Fabric.

Table 2. Public keys and signature sizes of the algorithms [39].

Algorithm	Size* (bytes)	Execution Time** (ms)
ECDSA	96	4
Falcon 512	1563	18
Falcon 1024	3073	28
Dilithium 2	3228	18
Dilithium 3	4173	21
Dilithium 4	5126	25
qTesla p-I	17472	37

* Size of public key and signature.
** Rounded execution time of LibOQS library and hashing that includes key generation, signature generation, signature verification, and hashing times.

9. Conclusion

Recent developments in quantum computing have attracted the interest of blockchain researchers and developers, for which public-key cryptography and hash functions are important. This article examined quantum-computing attacks (based on Grover's and Shor's algorithms) on blockchain and how to use post-quantum cryptosystems to mitigate them. To this end, the most applicable post-quantum methods were studied and their application to blockchain was analysed. Moreover, comprehensive comparisons of the properties and performance of the most promising post-quantum public-key encryption and digital-signature methods were presented.

The largeness of the key sizes was identified as the most significant disadvantage presented by the current signature schemes of the post-quantum era, thereby discouraging their adoption. Many studies are being conducted to refine it into a viable option for key size reduction and facilitating more efficient implementations. Alternatives providing reduced key sizes compared to the present ECDSA algorithms should be encouraged.

References:

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, vol. 15, no. 4, pp. 580–596, 2020.

[2] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," Ledger, vol. 3, pp. 1–21, 2018.

[3] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," Proc. Annu. ACM Symp. Theory Comput., pp. 197–206, 2008.

[4] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," IEEE Access, vol. 6, pp. 5393–5401, 2017.

[5] C. Ma and M. Jiang, "Practical Lattice-Based Multisignature Schemes for Blockchains," IEEE Access, vol. 7, pp. 179765–179778, 2019.

*[6] M. F. Esgin, R. K. Zhao, R. Steinfeld, and J. K. Liu, "MatRiCT : Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol *," 2019.*

[7] C. Y. Li, X. B. Chen, Y. L. Chen, Y. Y. Hou, and J. Li, "A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network," IEEE Access, vol. 7, pp. 2026–2033, 2019.

[8] N. Szabo, "Smart Contracts," 1994. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[9] B. Glass, "Counterfeit drugs and medical devices in developing countries," Res. Rep. Trop. Med., p. 11, 2014.

[10] U. D. of Health and H. Services, "Summary of the HIPAA Security Rule," 2018. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[11] "GDPR." [Online]. Available: https://gdpr.eu/.

[12] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, and I. Fellow, "DDoS in the IoT," Computer (Long. Beach. Calif)., vol. 50, no. 7, pp. 80–84, 2017.

[13] S. Sicari, A. Rizzardi, C. Cappiello, D. Miorandi, and A. Coen-Porisini, "Toward data governance in the internet of things," Stud. Comput. Intell., vol. 715, no. May 2018, pp. 59–74, 2018.

[14] A. Ometov et al., "An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends," IEEE Access, vol. 8, pp. 103994–104015, 2020.

[15] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," IEEE Access, vol. 7, pp. 115304–115316, 2019.

[16] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," The Deep Space Network Progress Report, vol. 42, no. 44. pp. 114–116, 1978.

[17] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 384–386, 1978.

[18] "Knapsack-Type Cryptosystems," vol. 15, pp. 159–165, 1986.

[19] L. Lamport, "Constructing Digital Signatures from a One-Way Function," SRI Int. Comput. Sci. Lab., vol. 94025, no. October, pp. 1–8, 1979.

[20] R. C. Merkle, "Advances in Cryptology — CRYPTO' 89 Proceedings," vol. 435, no. June, pp. 175–185, 1990.

[21] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS - A practical forward secure signature scheme based on minimal security assumptions," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7071 LNCS, no. November, pp. 117–129, 2011.

[22] D. J. Bernstein et al., "SPHINCS : practical stateless hash-based signatures," vol. 284833, pp. 1–30.

[23] O. Regev, "Lattice-based Cryptography."

[24] J. Bl, "Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima," no. August, 2007.

[25] M. Ajtai and S. Jose, "Generating Hard Instances of Lattice Problems," pp. 1–29.

[26] M. Sjöberg, "Post-quantum algorithms for digital signing in Public Key Infrastructures Post-quantum algorithms for digital signing in Public Key Infrastructures," 2017.

[27] L. G. Bruinderink, H. Andreas, T. Lange, and Y. Yarom, "Flush, Gauss, and Reload – A Cache Attack on the BLISS Lattice-Based Signature Scheme," no. 645622, pp. 1–31, 2016.

[28] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," IEEE Access, vol. 6, no. Part Ii, pp. 27205–27213, 2018.

[29] A. Petzoldt, S. Bulygin, and J. Buchmann, "Selecting Parameters for the Rainbow Signature Scheme - Extended Version -."

[30] J. Ding, A. Petzoldt, and L. Wang, "LNCS 8772 - The Cubic Simple Matrix Encryption Scheme," no. May, 2019.

[31] J. Ding, "A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation," no. March 2004, 2015.

[32] J. Ding and D. Schmidt, "Cryptanalysis of HFEv and internal perturbation of HFE."

[33] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, 2001.

[34] P.-A. Fouque et al., "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specifications v1.2," pp. 1–65, 2020.

[35] L. Ducas et al., "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 0, no. 0, pp. 238–268, 2018.

[36] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," Lect. Notes Comput. Sci., vol. 3531, no. December 2014, pp. 164–175, 2005.

[37] W. Beullens, "Improved Cryptanalysis of UOV and Rainbow," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12696 LNCS, pp. 348–373, 2021.

[38] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," J. Br. Blockchain Assoc., vol. 2, no. 1, pp. 1–8, 2019.

[39] A. Holcomb, G. Pereira, B. Das, and M. Mosca, "PQFabric: A permissioned blockchain secure from both classical and quantum attacks," IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2021, 2021.
[40] C. Gorenflo and S. Lee, "FastFabric : Scaling Hyperledger Fabric to 20,000 Transactions per Second."
*[41] D. Stebila, "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project *," pp. 1–22, 2017.*

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Lu Gan and Bakhtiyor Yokubov prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-1-(3)2023

A Review of Upgradeable Smart Contract Patterns based on OpenZeppelin Technique

Shaima AL Amri, Leonardo Aniello, Vladimiro Sassone
School of Electronics and Computer Science, University of Southampton, UK

Correspondence: saaa1n18@soton.ac.uk/shaima.alamri@hotmail.com
Received: 30 December 2022 **Accepted:** 30 January 2023 **Published:** 20 March 2023

Abstract

The Ethereum blockchain is one of the main public platforms to run smart contracts and enable decentralised applications. Since data stored in a blockchain is considered immutable, smart contracts deployed in Ethereum are regarded as tamper-proof and therefore offer strong protection against attacks aiming at tinkering with the execution flow of an application. Yet, like any other software, a smart contract needs to be maintained over time to fix bugs or add new features. Deploying every updated version as a brand-new smart contract in Ethereum leads to problems such as migrating the contract state from the old version and enabling clients to point to the new version in a timely fashion. The OpenZeppelin framework addresses this limitation by providing libraries that enable the deployment of upgradeable smart contracts. This is achieved by relying on proxies that act as intermediaries between clients and smart contracts, allowing the latter to be updated transparently. In this paper, we present the upgradeable smart contract patterns supported by OpenZeppelin and compare them in terms of security, cost, and performance. To show this paradigm's prevalence in Ethereum, we also analyse the usage of OpenZeppelin Upgradeable smart contracts over the last four years.

Keywords: *Smart Contract, Immutability, Proxy, Upgradeable, Patterns, OpenZeppelin*

JEL Classifications: *C80 and C89*

1. Introduction

The upgraded smart contract (USC), designed with the OpenZeppelin technique, is used to reserve the contract state and redirect calls to the implementation contract (IC). In addition, it upgrades the IC address when it requires a new version. In this technique's design, the proxy stores the state of the IC and maps any new version to the same state [12]. The upgraded technique is not preventing the known attacks against smart contracts. The purpose of designing the USC is to ensure the state cannot be lost and will be mapped to a new version of IC.

OpenZeppelin is a widely used library for writing secure smart contracts, and it provides several patterns for implementing upgradability [6]. These patterns include TransparentProxy, ERC1967, UUPSUpgradeable, and Beacon [6]. The research reviews the OpenZeppelin Upgradeable patterns to understand how they vary based on gas consumption, security, and performance.

The OpenZeppelin technique of upgrading smart contracts was invented in 2017. This technique motivates us to analyse the verified smart contract in Etherscan and check whether this technique has grown within the last four years.

The paper is organised as follows. Section 2 introduces Ethereum and smart contracts, followed by the OpenZeppelin Upgradeable technique. Section 3 presents the research methods, while Section 4 presents the analysis of upgraded patterns and compares them based on gas consumption, security, and performance. Section 5 shows the analysis result of the usage of upgradeable patterns over the last four years. Finally, Section 6 summarises our review and outlines our future direction.

2. Background

2.1 Ethereum and Smart Contract

Ethereum platform is one of the public blockchain platforms introduced by Vitalik Buterin [1] to override the limitations of Bitcoin's scripting language. Unlike Bitcoins, Ethereum innovated to support all loops as it is full of Turing completeness [10]. Moreover, the Ethereum platform is the most popular for deploying contract-based applications in several contexts, including financial services, insurance, education, healthcare, and cryptocurrencies.

A smart contract is designed to verify and enforce legal contract negotiation. Once it is deployed in the blockchain, no one can change the code [2]. It is executed and verified by Ethereum Virtual Machine Environment (EVM), built within all decentralised nodes in the Ethereum blockchain. The immutability characteristic of the smart contract made it a trusted application.

2.2 OpenZeppelin Upgradeable Technique

OpenZeppelin is a popular open-source framework for building secure, modular, and reusable smart contracts on the Ethereum platform [11]. The most important approach is implementing upgradeable smart contracts on the Ethereum platform. Their approach utilises a proxy, allowing developers to deploy a contract as an intermediary between a user and the implementation contract [12]. The proxy will store the state of the implementation contract to reserve the state when upgrading the IC to a new version. The upgrade process is done by invoking the **UpgradeTo( )** function by the EOA, but if the IC had the same function, this would cause a problem known as function clashing [7]. This issue can occur because each function in a smart contract is identified by four-byte at the bytecode level [7] and can not be tracked by the Solidity compiler because we have

two different contracts: proxy and IC. To solve this issue, OpenZeppelin has designed a Transparent Proxy pattern [6] with a specific ProxyAdmin contract which plays the admin role. In addition, the invocation of any function will be delegated to the suitable contract according to the caller's address [7]. The ProxyAdmin will be the only one that have the right to invoke the UpgradeTo( ) function of the proxy.

3. Methodology

The methodology proposed in this research to analyse the upgradeable patterns involves the following steps:

1. Data Collection: We obtained the smart contract address and creation timestamp from the Kaggle [4] dataset, which contains live data of the Ethereum blockchain. Then, the data was categorised based on the creation timestamp from 2019 to 2022.
2. Source Code Crawling: We crawled source codes using the tool provided by [5] and edited them according to our needs by using the contract addresses from the previous step as input for our script. We were able to crawl different contracts categorised by years.
3. Data Analysis: We classified the dataset according to OpenZeppelin Upgradeable patterns (e.g., TransparentProxy, UUPSUpgradeable, ERC1967, and Beacon). We used Python panda's library to classify and calculate summary statistics for each category. The result of this step will be discussed and is present in Section 5.

4. Analysis of OpenZeppelin Upgradeable Patterns

4.1 Upgraded Patterns

The upgradability of a smart contract is done by creating a new version of the deployed contract. The new version is designed to overcome the issues which exist in the old version or by adding new features according to the business needs. The state of the old version will be mapped to the new version. However, the upgradability cannot prevent the smart contract from potential adversaries such as a reentrancy attack.

The OpenZeppelin technique has proposed different patterns. Each pattern is linked with a different contract to achieve its purpose. The Proxy contract is represented as the central core of the upgradeable contract with all patterns because it is the core of implementing the delegation functionality [6]. The remaining patterns are designed with different functionalities.

4.1.1 Transparent Proxy

The Transparent Proxy contract is designed to avoid the function clashing and ensure that only the admin can call the upgrade function. The following contracts are the main contracts for implementing this pattern. Figure 1 presents the deploying Tx of this pattern, where it clearly shows how the three contracts are created and attached to it is code and storage. The storage of TransparentUpgradeable Proxy is responsible for managing the state of itself and IC [6]. Moreover, the storage of the IC will be useless as IC is responsible for executing the delegated function and sending the output back to the TransparentUpgradeable contract.

- **TransparentUpgradeableProxy** is designed to manage the calls from the end-user to the IC by checking the caller's identity[8]. In case the caller is the admin, his call will only be delegated to the IC for execution if the caller is an external account.
- ProxyAdmin is designed as an admin of TransparentUpgradeableProxy. It only has the right to access the admin functions, which are used for upgrading the proxy or changing the contract owner [8]. For that, the ProxyAdmin is always assigned to a dedicated account.

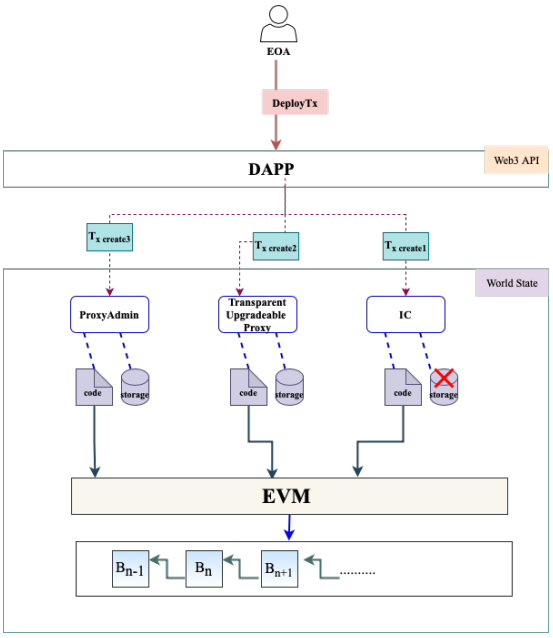


Figure 1. Process of deploying the TransparentProxy pattern

In case the external accounts invoke a function in IC, the **TransaparentUpgradeable Proxy** checks whether this call is to the admin or IC. The proxy will be delegated the request to the IC if it is valid. The proxy will update the state of IC contract once the request is executed successfully and the output is forwarded to the external accounts. **Figure 2** illustrates how the proxy manged the IC state. The proxy tracks the state of IC because all invocation to IC is only done through the proxy.

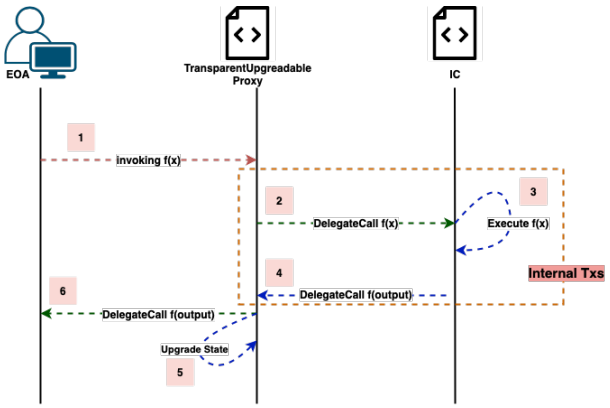


Figure 2. Invoking process of IC functions

Upgrading the IC to a new version requires deploying the new version first and upgrading the address in proxy storage via ProxyAdmin contract. It is clearly shown in **Figure 3** how the upgrade function is executed by the TransparentUpgradeable Proxy once the ProxyAdmin validates the identity of the caller.

4.1.2 ERC1967

ERC1967Proxy is designed based on EIP1967 [2], which is proposed to overcome any clashes that might occur with the storage layout of IC address. This proxy is not upgradeable by default. It is inherited into the Proxy contract, which was designed as the core for delegating the functions. The function responsible for declaring the storage slot of the IC address showed in Snapshot 1. The function is defined as a constructer because it will be executed once the contract is deployed. In

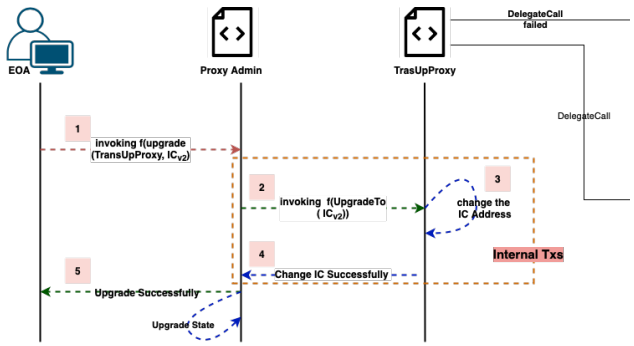


Figure 3. The Upgrade process of Upgrade function

addition, the variable of IC address can be changed. Figure 4 illustrates the contract created by deploying the ERC1967 pattern. It shows how the **ERC1967Proxy** is inherited within the proxy as one contract because it helps the proxy guarantee that the **ERC1967Upgrade** is designed along with ERC1967Proxy to "provide the getters and events which emit the upgrade functions of EIP1967 slots" [2].

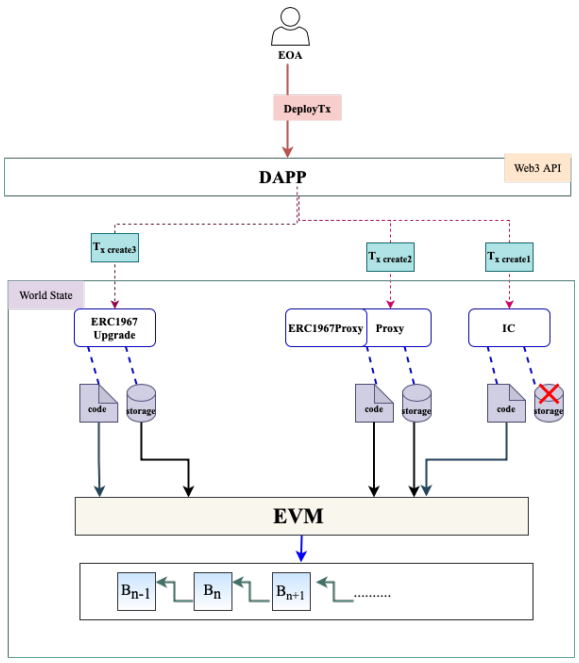


Figure 4. Process of deploying the ERC1967 pattern

The message invocation process using this pattern is similar to the previous pattern in Section 4.1.1. In this pattern, the proxy will delegate the message to IC. Then IC executes the targeted function and returns the output to a proxy. Finally, the proxy will delegate the output to the end-user and update the state of IC.

```
constructor(address  logic, bytes memory _data)
payable { assert(_IMPLEMENTATION_SLOT ==
bytes32(uint256(keccak256("eip1967.proxy.implemen
tation")) - 1));

_upgradeToAndCall(_logic, _data, false);}
```

Snapshot 1. The function of identifying the storage slot of IC address

In the case of invoking the upgrade function, the transactions will be executed differently. The owner initiates the invocation after creating the new contract version and getting IC address. The IC address will be upgraded by the ERC1967Upgrade, where it executes the **_getImplemntation(old_ICaddress)** function followed by calling the **_UpgradeTo(newIC_address)** [6]. The execution of those functions is emitting the old address to the new address, as shown in Figure 5.

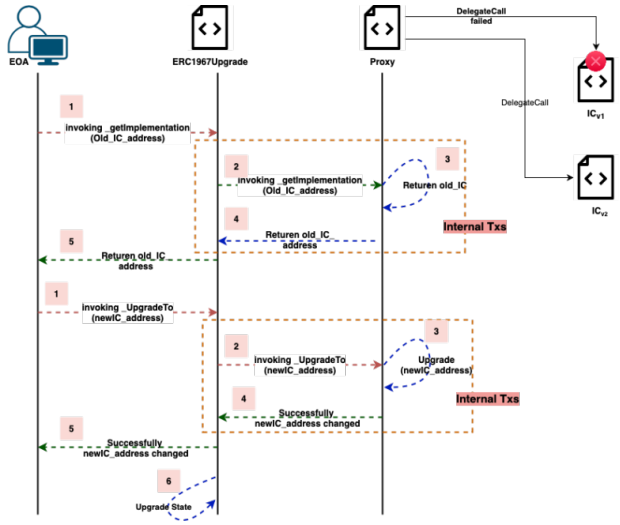


Figure 5. The process of Upgrade using ERC1967 pattern

4.1.3 Beacon

This pattern is designed to call the upgrade function of different **ICs** through multiple proxies. It consists of three contracts, as detailed below.

- BeaconProxy is implemented as a proxy designed to retrieve the IC addresses for each call initialised by the UpgradeableBeacon contract [6].
- IBeacon is designed as the interface of BeaconProxy, as it is responsible for storing the IC addresses. The BeaconProxy calls the implementation() function [6] and checks whether the return value is a contract or not. Then the return address will be used to delegate the call of the target.
- UpgradeableBeacon acts as an admin who has the right to upgrade the BeaconProxy. The upgrade process is done by calling the IBeacon contract, which holds all IC addresses, and the linked proxies will be upgraded automatically [6].

Figure 6 illustrates the deployment process of Beacon patterns, where four different contracts are created. This pattern is similar to ERC1967 during the upgrade process. Figure 5 as the upgrade IC address to the new version is done through in the IBeacon contract as the BeaconProxy is retrieving the address of IC from IBeacon. However, the interaction between this contract and the end-user is different. In the case of invoking a function in IC while using the Beacon pattern, the call goes through two transactions before being executed by the IC. First, the BeaconProxy will receive the call and retrieve the IC address from the IBeacon to delegate the call. Then, once the BeaconProxy gets the IC address it will delegate the call to the IC for executing the function, as shown in Figure 7.

4.1.4 UUPSUpgradeable

This pattern is considered an upgradability mechanism built within the IC contract. It is implemented by using ERC1967Proxy [6]. In this pattern, the data and contract logic are designed as one contract, as illustrated in Figure 8. The invocation of any function is done directly between the end-user and the contract. However, the upgrade process to a new version will be authorised first by executing the function **_authorisedUpgrade(Owner Address)** [6].

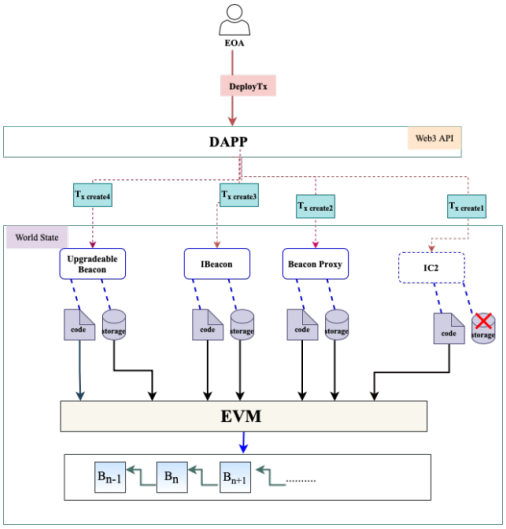


Figure 6. Process of deploying the Beacon pattern

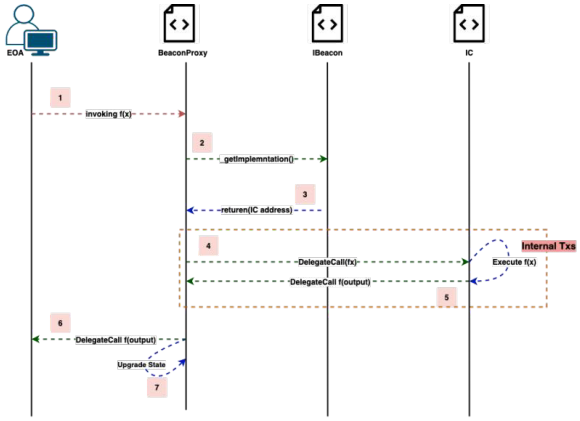


Figure 7. Process of interaction with the Beacon pattern

All OpenZeppelin Upgradeable patterns are designed to preserve the immutability of a contract by holding the implementation contract state within a proxy contract. This technique allows the implementation contract to be upgraded without losing the contract state. Some patterns, such as the **TransparentProxy** pattern, are designed to prevent authorisation issues by allowing a fixed admin to upgrade the implementation contract. These patterns can be used to ensure the contract remains upgradeable and secure. For example, the proxy contract can be deployed using the **TransparentProxy** pattern, which allows the admin to upgrade the implementation contract as needed. In addition, using the **ERC1967** by some patterns is also helpful in avoiding the proxy selector clashing issue.

4.2 Comparison of Upgradeable Patterns

4.2.1 Gas Consumption (gc)

The contract transactions executed within the EVM and the cost gas consumption (C_gc) for this operation are calculated according to the transaction type. The gas price is changed rapidly according to the network usage, where the amount of consumed gas is a fixed value identified within Appendix G[3]. The (gc) of the initial transaction of creating a smart contract is 1.28M gwei if the gas price is 40 Wei, where the estimated gas consumed is 32000 units of gas. The research aims to determine the (gc) for different types of transactions of different upgradeable patterns.

- **(gc) of Deployment T_x**

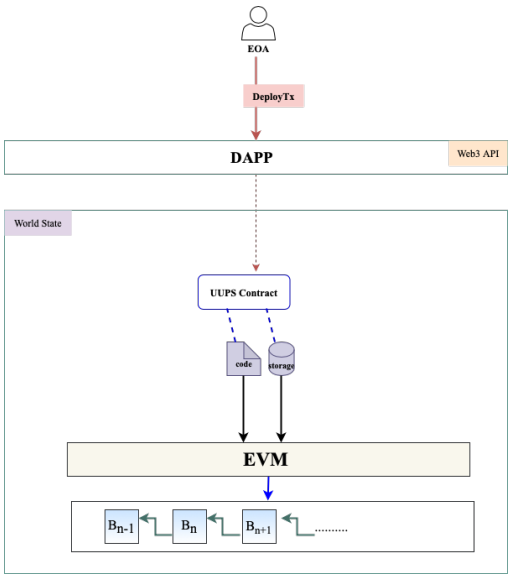


Figure 8. Process of deploying the UUPSUpgradeable pattern

Since the deployment of an upgradeable contract creates more than two SCs, then the **(gc)** depends on the number of transactions that created new contracts.

For example, in the case of implementing the **TransparentProxy** pattern, three SCs will be created according to Figure 1, and the gas consumption for three create transactions is 32,000*3. Therefore, Equation (1) can be used to calculate the **(gc)** of the creation transaction where (n) is present in the number of contracts created during the deployment process.

It is identified from Figure 8 that deploying the UUPSUpgradeable patterns is cheaper than the other patterns.

$$32{,}000 * n, n \in \mathbb{N} \; and \; n \geq 2 \qquad (1)$$

- **(gc) of Normal T_x**

The *CALL and DELEGATECALL* are categorised as normal T_x because any *IC* functions are invoked through these transaction types. We assume the end-user has invoked the IC function, which will be delegated to *IC* through *Px* as a *DELEGATECALL* transaction. The (gc) of the entire process from the end-user to *IC* is calculated as four different transactions. According to Appendix G[3] gas consumption of every transaction costs 21,000, then the total gas consumption is calculated as in Equation (2). The CALL and DELEGATE CALL have the same value of (gc) because they are treated as a transaction.

$$gc_{call} + gc_{delegatecall} + \cdots \qquad (2)$$

All upgradeable patterns have the same number of transactions except UUPSUpgradeable as the proxy and IC combined as one smart contract. For that, it has less (gc) compared with the remaining patterns.

- **(gc) of Upgrade T_x**

The upgrade T_x is a ***CALL*** transaction because the upgrade is the name of the function built within the ***ProxyAdmin*** contract. The EOA invokes this function through ***ProxyAdmin*** to upgrade the IC address. The (gc) is determined by calculating the ***CREATE*** transaction of the new version with the ***CALL*** transaction of upgrading *IC* address. Figure 5 illustrates the number of transactions that can be called to execute the upgrade function.

$$gc_{call} + gc_{CREATE} \qquad (3)$$

The gas consumption for different contract transactions can vary depending on the transaction type and the contract code's complexity.

For example, the deployment transactions consume a fixed amount of gas because this transaction only involves creating the contract and does not execute any of its functions. On the other hand, invoking a function in ***IC*** requires multiple transactions to be executed and complete the call. It includes an average transaction to initiate the call, internal transactions to execute the function, and a final transaction to return the result. Therefore, the gas consumption for these transactions can be more expensive than the deployment transaction.

Additionally, performing the upgrade to an IC, the owner must initiate a transaction to update the proxy contract by changing the address of the old version to the new version. This transaction consumes gas, as does the deployment transaction to deploy the new implementation contract. Therefore, the total gas consumption for an upgrade depends on the complexity of the new implementation contract and the number of transactions required to complete the upgrade.

4.2.2 Performance

In our research, we have conducted a qualitative analysis method to evaluate the performance of different patterns and perform the comparison between them. The evaluation estimates the number of transaction rounds required to execute the target function within the proxy patterns or IC. The comparison will be based on transaction types as it will cover in the following sections.

• Performance of Deployment T_x

The regular **deploymentT_x** of deploying contract requires one transaction, called creation Tx. In the case of deploying the different patterns, such as **ERC1967** pattern, it also required three rounds of transactions, as it initialised three different creation transactions. It is responsible for creating the **ERC1967Proxy, ERC1967Upgrade,** and **IC**. On the other hand, deploying the **Beacon** pattern required three rounds of creation transactions, as shown in Figure 6. Moreover, deploying the UUPSUpgradeable contract required two rounds of creation transactions as the UUPSUpgradeable is built-in with the IC and needs ERC1967Proxy to avoid the proxy selector clashing issue.

The performance of this type of transaction can be estimated by counting the number of rounds required to create each contract pattern successfully. However, each created contract is created in an individual block because once the IC is created, the address will be stored within the proxy pattern and used later as input to delegate the end-user invocation. For that, by using our analysis method, we assume that UUPSUpgradeable patterns have high performance as it requires only two rounds of creation transactions during the deployment process.

• Performance of Normal T_x

The **normal T_x** is the call initiated by the end-user to IC to execute the targeted function. In the case of executing a function of IC via proxy, it required six transactions. Those transactions represent different types of calls, starting with the call from the end-user to IC through the proxy. Then, once the IC receives it, it will be executed and delegated to the end-user. Finally, the proxy completes the final transaction to update the contract state once the process is done successfully. The internal transactions consist of three transactions which are linked with the original transaction. Once the output from internal transactions is delegated to the end-user, the six transactions will be added to the same block with the same hash value. Figure 5 shows the number of transactions performed to execute a function in the **ERC1967** pattern.

As the proxy plays an essential part in all patterns, we estimate that ERC1967 and Transparent Proxy patterns have the same number of transactions to execute the targeted function. Therefore, the UUPSUpgradeable pattern has the best performance as the execution of the function is done within the same contract.

Our method focuses on the number of transactions initiated to be executed. Other metrics can be considered experimentally to know which patterns perform better than others. We aim to evaluate the performance experimentally by measuring throughput, latency, and code complexity which can give us an accurate result.

• Performance of Upgrade T_x

Upgraded smart contracts involve the contract owner changing the address of IC from the old version to the new version. Figure 5 represents the upgrade process of the ERC1967 pattern, as the number of transactions performed is equal to the number of transactions performed by the Beacon pattern. We assume that both patterns perform similarly during the upgrade process.

In the case upgrade process done by the TransparentProxy, the owner calls the upgrade function similarly as the end-user invokes a function from IC. For that, we assumed that the number of transactions required for upgrade Tx is similar to normal Tx. Therefore, we assume that UUPSUpgradeable is best performed, followed by the TransparentProxy pattern, and the remaining patterns are performed slower.

4.2.3 Security

The design of an upgradeable contract does not prevent the known attack of smart contracts, such as reentrancy, because the main idea of an upgradeable contract is to ensure the immutability concept of blockchain by reserving the contract state.

In this section, the research aims to discover the security vulnerabilities that affect upgradeable patterns. First, we have used some datasets from Section 3. Then, we use the Slither [1] tool to analyse the source codes of different upgradeable patterns. Figure 9 shows the result of different affected vulnerabilities and their impacts on each pattern.

It shows that 20% of the detected vulnerabilities in **Beacon** and **TransparentProxy** patterns have an informational impact. However, the vulnerabilities categorised as informational will not affect the safety of upgradability because they do not affect the upgrade functions. On the other hand, the **ERC1967** pattern is affected by 60% of detected vulnerabilities equally divided between the informational, low, and medium impacts. For that, the code complexity of upgradeable patterns could be one of the main metrics that might **ERC1967** pattern to be the most affected, with 20% of vulnerabilities with medium impact.

There is no result related to **UUPSUpgradeable** patterns in Figure 9. For that, we need to use another analysis tool in future to verify the results.

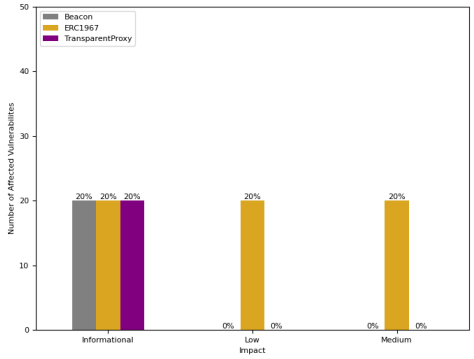


Figure 9. The number of affected vulnerabilities based on OpenZeppelin patterns

Therefore, the good practice to keep the contract safe and secure is developing the following mechanisms besides the upgradeable contract [9].

- **Ownable**
  This contract module provides an access control mechanism and ensures the authorisation of upgradeable contracts [9]. It is linked with upgradeable contracts, such as Transparent, Beacon, and UUPSUpgradeable contracts. The EOA who deploys this contract will be the owner by default unless he transfers the ownership to another owner by invoking the **transferOwnership( )** function, which is only reachable by the owner. If the ProxyAdmin account needs to be changed, it will be done with the Ownable contract's function.
- **ReentrancyGuard**
  This contract module is designed to prevent reentrant calls to the contract function [9]. It is built with the **nonReentrant( )** modifier, which fails any call execution with a reentrancy pattern.

5. Analyse the Usage of OpenZeppelin Upgradeable Smart Contracts Over the Last Four Years

In this section, we analyse the use of OpenZeppelin Upgradeable smart contracts over the last four years. The analysis starts by using the dataset which been created from Section 3.3.

5.1 Result Analysis

Figure 10 compares the number of upgradeable patterns and how they evolved over the last four years. For example, the **TransparentProxy** pattern's value increased significantly from 2019 to 2022, with a value of 5116 in 2019 and a value of 53,898 in 2022. These changes represent a growth of more than 90%. Similarly, the value of the **UUPSUpgradeable** pattern increased from 122 in 2019 to 13,134 in 2022.

On the other hand, the value of the **ERC1967** pattern remained relatively constant from 2019 to 2021 but increased significantly in 2022. However, the value of the **Beacon** pattern also increased steadily from 2019 to 2022, with a value of 9 in 2019 to 229 in 2022.

Overall, the data show that the Transparent and UUPSUpgradeable patterns are the most upgradeable and are used between 2019 and 2022. The comparisons discussed earlier in this paper could be related. It was clear that Transparent patterns have been invented to overcome the issue discussed in Section 2.2. In addition, the UUPSUpgradeable pattern has better performance and is cheaper. The values of the ERC1967 and Beacon patterns have remained relatively constant or have increased steadily over the four years. This analysis provides empirical results of using upgradeable smart contract patterns based on the OpenZeppelin technique.

Conclusion and Future Work

In this paper, we reviewed the OpenZeppelin Upgradeable patterns and compared them from different aspects, such as cost, performance, and security. We performed some analyses to find the vulnerabilities that might affect upgradeable smart contract patterns.

The difference between upgradeable patterns on performance and gas consumption is performed based on three transactions: DeploymentTx, NormalTx, and UpgradeTx. However, the comparison between upgradeable patterns on performance was based on a qualitative analysis. We found that the UUPSUpgradeable pattern performs better according to the number of transactions completed per round. In the case of gas consumption, the gas consumption while using the UUPSUpgradeable pattern is cheaper than other patterns. We assume that the Beacon pattern also consumes much gas and has slow performance according to the number of transactions performed during the interaction. Finally, the result analysis shows that the use of Transparent Proxy of upgradeable patterns has grown significantly over the last four years.

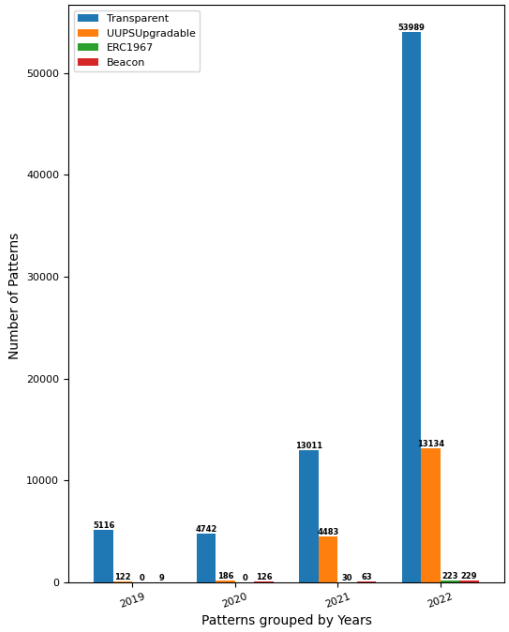


Figure 10. Number of Upgradeable patterns between 2019 and 2022

In future work, we aim to verify the vulnerabilities identified in Section 4.2.3 by creating a threat model and identifying upgradeable patterns' security requirements. In addition, we will conduct experimental evaluations of the performance of the upgradeable patterns. The experimental method will involve measuring key metrics such as throughput, latency, and code complexity and using these metrics to compare the performance of different upgradeable patterns.

References

[1] J. Feist, G. Grieco, and A. Groce, "Slither: a static analysis framework for smart contracts", in 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). IEEE, May 2019. pp. 8-15.
[2] Ethereum, "EIPS/EIP-1967.MD at master Ethereum/EIPS," GitHub, 08 Sep. 2022. [Online]. Available: https://github.com/ethereum/EIPs/blob /master/EIPS/eip-1967.md.
[3] "Yellow paper – github pages." [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf.
[4] G. BigQuery, "Ethereum blockchain," Kaggle, 04 Mar. 2019. [Online]. Available:https://www.kaggle.com/datasets/bigquery/ethereum-blockchain.
[5] W. Jie, A. S. Koe, P. Huang, and S. Zhang, "Full-stack hierarchical fusion of static features for smart contracts vulnerability detection," 2021 IEEE International Conference on Blockchain (Blockchain), 2021. Availbale: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9680540.
[6] "Proxies," OpenZeppelin Docs. [Online]. Available: https://docs.openzeppelin.com/contracts/4.x/api/proxy.
[7] "Proxy upgrade pattern," OpenZeppelin Docs. [Online]. Available: https://docs.openzeppelin.com/upgrades-plugins/1.x/proxies?utm_source=zos&utm_medium=blog&utm_campaign=proxy-pattern#the-constructor-caveat.
[8] S. Palladino, "The transparent proxy pattern," OpenZeppelin blog, 26 Apr. 2021. [Online]. Available: https://blog.openzeppelin.com/the-transparent-proxy-pattern/.
[9] "Security," OpenZeppelin Docs. [Online]. Available: https://docs.openzeppelin.com/contracts/4.x/api/security.

[10] M. Wohrer and U. Zdun, "Smart contracts: Security patterns in the ethereum ecosystem and solidity," in 2018 IEEE 1st Int. Work. Blockchain Oriented Softw. Eng. IWBOSE 2018 - Proc., vol. 2018-Janua. IEEE, 2018. pp. 2–8.
[11] "Proxies," OpenZeppelin Docs. [Online]. Available: https://docs.openzeppelin.com/contracts/4.x/api/proxy.
[12] S. Palladino, Aquiladev, and Josselinfeist, "Contract upgrade anti-patterns," Trail of Bits Blog, 06 Sep. 2018. [Online]. Available: https://blog.trailofbits.com/2018/09/05/contract-upgrade-anti-patterns/.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
The authors worked together to design and conduct this research and prepare the manuscript.

Funding:
University of Southampton
Ministry of Higher Education, Research Innovation Oman

Acknowledgements:
Not applicable.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-1-(5)2023

DeFi Lending Platform Liquidity Risk: The Example of Folks Finance

Matthias Hafner,[1, 2] Romain de Luze,[2] Nicolas Greber,[2] Juan Beccuti,[2, 3] Benedetto Biondi,[4] Gidon Katten,[4] Michelangelo Riccobene,[4] Alberto Arrigoni[4]

[1] *University of Zurich, Switzerland*

[2] *Center for Cryptoeconomics and Swiss Economics, Switzerland*

[3] *University of Bern, Switzerland, and Informal Systems, Canada*

[4] *Folks Finance*

Correspondence: matthias.hafner@swiss-economics.ch

Received: 03 January 2023 **Accepted:** 03 March 2023 **Published:** 02 April 2023

Abstract

Decentralised finance (DeFi) lending platforms may experience liquidity risk, which occurs when users are unable to withdraw their assets. Researchers and practitioners have found that the concentration of deposits among a small group of users is one of the main drivers of liquidity risk. Typically, lending platforms experience high concentration at the beginning of their operations. As a result, they face a significant liquidity risk that has not been investigated so far. This article closes this gap by investigating liquidity risk from the perspective of a new lending platform, describing the use case of Folks Finance. First, we describe the liquidity risk the lending protocol faces using platform economics. Second, we theoretically assess the efficacy of different liquidity risk measurements. Third, we investigate how a reward mechanism can reduce liquidity risk. We show that the liquidity risk is more pronounced for a new lending platform than for an incumbent protocol. In addition, we find that the Herfindahl–Hirschman index (HHI) outperforms other liquidity risk measurements. Finally, we show that if rewards are sufficient but not too large, a programme that incentivises depositors to lock their assets can reduce liquidity risk and increase liquidity bootstrapping. Several conclusions are drawn from the case study: First, new lending platforms should be particularly cautious regarding liquidity risk. Second, lending protocols should use HHI instead of other concentration measurements when calibrating their parameters. Third, rewards can be used to bootstrap liquidity and incentivise liquidity holdings but should not be overused.

Keywords: *DeFi, Lending Platform, Liquidity Pools, Platform Economics, Liquidity Risk*

JEL Classifications: *C63, D47, G10, L10*

1. Introduction

In the last years, decentralised finance (DeFi) has experienced rapid growth, attaining a peak of total value locked (TVL), which refers to the overall value of crypto assets deposited in DeFi, of about $50 billion in December 2022 [1]. Among the different types of DeFi projects, lending protocols account for a big share of DeFi's TVL. A lending protocol is a type of financial service that allows individuals and organisations to lend and borrow funds from each other without the need for a traditional financial institution, such as a bank, to facilitate the transaction.

Such protocols, and more broadly DeFi, present a range of new opportunities and can mitigate some traditional risks. This is not necessarily the case for liquidity risk. Liquidity risk can affect the ability of users to access and trade their assets. This article investigates liquidity risk for a new lending platform in the DeFi ecosystem and aims to provide insights and strategies that can help to mitigate potential vulnerabilities and challenges faced by DeFi platforms.

There exists a large literature on market liquidity and liquidity risk in the context of traditional finance. In general, liquidity refers to the ease with which an individual or entity can exchange their wealth for goods, services, or other assets [2, 3]. Multiple definitions for liquidity risk exist, but in this article we stick to the definition related to banks, where it refers to the possibility that an entity is unable to service its liabilities as they come due without incurring unacceptable losses (e.g., [3, 4, 5]). Liquidity risk depends on various factors, such as the volatility and the concentration of the assets held in custody [6]. Researchers investigated the impact of it on the economy and market prices (e.g., [7, 8]). The literature shows that liquidity risk can lead to, among other things, financial crises, which can damage financial stability, disrupt the allocation of resources, and ultimately destabilise the real economy [3]. Given the significant negative impacts that can result, understanding, measuring, and effectively managing liquidity risk is of critical importance.

In a DeFi lending protocol, users can lend and borrow assets directly from one another without the need for a traditional financial intermediary, such as a bank. In this system, liquidity risk refers to the risk that a protocol will not have enough assets available to support basic operations, including the ability of a depositor to exit the protocol [9]. This risk can arise if, for example, there is a large outflow of assets from the platform, leading to a lack of available liquidity for depositors to use to withdraw their own assets.

The literature on liquidity risk in the context of DeFi is sparse. Gudgeon et al. [10] provide a theoretical overview of interest rate mechanisms of different lending protocols and empirically assess their interest rates at different points in time. They found that deposits are often very concentrated which presents a significant liquidity risk. Sun et al. [11] investigate liquidity risks focusing on Aave, a popular lending protocol. They analyse the behaviour

of a small group of users who are both borrowers and depositors. Those users can have complex and potentially amplifying effects on the platform's liquidity risks, which may be transmitted to other liquidity providers in the market.

Empirical evidence suggests that liquidity concentration tends to be high in the initial stages of lending platforms (see also section 3.2). This presents a significant risk for these platforms that has not been investigated so far. This article closes this gap by investigating liquidity risk from the perspective of a new lending platform and proposes a solution to mitigate it.

We investigate liquidity risk by presenting the use case Folks Finance, a DeFi lending platform on the Algorand blockchain. We do this in two parts. First, we describe Folks Finance as a lending protocol and the associated liquidity risk using platform economics. In line with the literature, we find that concentration is a major driver of liquidity risk. Second, we discuss the practical implementation of a reward system to mitigate liquidity risk. More specifically, we theoretically assess the efficacy of different liquidity risk measurements and investigate how a reward mechanism for locking the assets for a fixed period can reduce liquidity risk. We find that the Herfindahl–Hirschman index (HHI) outperforms other liquidity risk measurements. Finally, we show that a programme that incentives depositors to lock their assets can reduce liquidity risk and increase liquidity bootstrapping.

The article is structured as follows. In section 2, an overview of the relevant components of Folks Finance is presented. In section 3, we describe how DeFi lending platforms work from an economic point of view and describe the risks they face. In section 4, we analyse different possibilities of measuring concentration of liquidity in a pool. In section 5, we present a solution to mitigate liquidity risk. In section 6, we conclude.

2. Lending Platform Model: The Example of Folks Finance

Lending platforms are DeFi platforms that allow individuals to lend and borrow money from each other without the need for a traditional intermediary such as a bank. In this section, we show how participants on a lending platform interact by presenting the use case of Folks Finance, a lending protocol in the Algorand ecosystem.

Lending platforms typically have two main participant types: borrowers and depositors (also called lenders). Borrowers are individuals or organisations who take loans and increase or repay existing loans. For any loan, the borrowers must provide collateral. Depositors are individuals or organisations who provide assets or withdraw them. As explained later, in Folks Finance depositors can additionally lock their assets. The platform acts as a facilitator, connecting borrowers and depositors and managing the loan process. Depending on the complexity of a platform, more participants can interact. That is the case of Folks Finance.

Figure 1 illustrates the various users of Folks Finance and how they interact with each other.

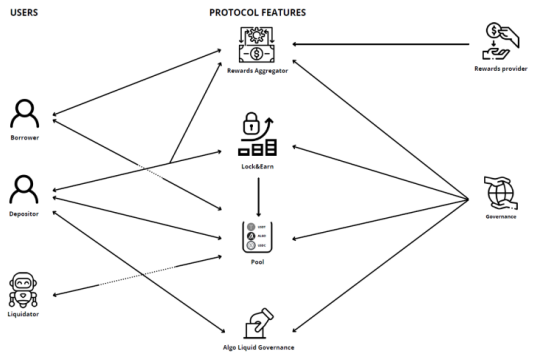


Figure 1. Interactions between Folks Finance's users

Besides borrowers and depositors, the other actors involved on Folks Finance are liquidators, reward providers, and governance. Liquidators buy the collateral and liquidate positions when the borrow balance value falls below an under-collateralisation threshold. Reward providers are entities that provide rewards for Lock & Earn. Governance may execute parameter updates and other related actions.

The different operations and participants are described in more detail in Folks Finance's official documentation [12].

3. Lending Platform Economics and Associated Risks

Folks Finance and other lending protocols are multi-sided platforms, acting as intermediaries between interdependent groups (in particular, lenders and borrowers). To understand the challenges that new lending platforms face, it is necessary to understand their economic models. In this section, we introduce the platform economics of lending platforms and discuss the liquidity risks that they face.

3.1 Platform Economics of Lending Protocols

There is a wide range of markets where users benefit from choices made by other users. Such users differ in needs or interests (e.g., buyers and sellers, borrowers and depositors). Platforms are intermediaries that make the interaction between such heterogeneous users possible [13].

A platform business model has a key economic characteristic. The distinct groups expose themselves to so-called cross-network effects. The effects are positive if the platform becomes more attractive/valuable for one group when the other user group grows and negative in the opposite case. The main challenge for a platform with cross-network effects is to bring all user groups on board. Notably, the platform must determine its pricing strategy, which is crucial for influencing various groups to join. This usually results in platforms charging different prices to user groups [13, 14].

As discussed in the previous section, lending platforms facilitate the interactions between depositors and borrowers of crypto assets. Borrowers and depositors exert positive cross-network effects on each other. Depositors exert positive cross-network effects on borrowers since a larger pool size increases the likelihood that a borrower can borrow the type and amount of asset they choose. Borrowers have a positive effect on depositors because an increasing amount borrowed from the pool raises the efficiency of the deposited assets. Under reasonable protocol designs, increased efficiency results in higher returns for depositors.

Lending protocols use a dynamic pricing strategy to control cross-network effects. To optimally match demand from borrowers and depositors, platforms adjust interest rates algorithmically to attract participants from the two groups using the following principles: (1) If the total assets deposits are high, but only a small amount is borrowed, the interest rate is reduced to attract borrowers. (2) If the total amount of loans is high compared to the deposits in the pool, the interest rate is high. In practice, lending platforms set the interest rate i based on the so-called utilisation ratio U, which describes how much of the available assets in a pool (deposited amount) are borrowed:

$$U = \frac{Borrowing\ Amount}{Deposit\ Amount}$$

Lending platforms set the interest rate using a positive transformation of this utilisation ratio:

$$i = f(U)$$

An example of such a function is presented in Figure 2.

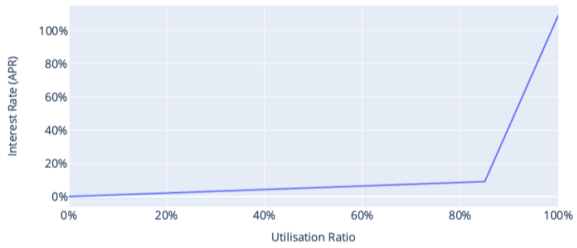


Figure 2. Folks Finance's USDC interest rate as a function of the utilisation ratio

Figure 2 presents the interest rate of USDC on Folks Finance as a function of the utilisation ratio at the time of writing. The blue line represents borrowers' interest rate (y-axis), which increases with the utilisation ratio (x-axis). The interest rate function balances demand from borrowers and depositors. If groups are unbalanced, the protocol will dynamically adjust the interest rate. Assume, for example, a utilisation ratio of 10%, meaning that only 10% of the deposited USDC is borrowed. Then the function will set an interest rate of 1% (see Figure 2). The low interest rate will attract borrowers (low cost of borrowing) and deter depositors (low reward for lending assets) and thus result in a more balanced state.

Note that in Figure 2 the slope of the interest rate curve becomes sharply steeper above a certain threshold (utilisation ratio 85%). This kink is used to manage liquidity risk, which we discuss in more detail in the next section.

3.2 Liquidity Risk

The utilisation ratio – the percentage of available assets borrowed at any given time – is a key factor determining a lending protocol's success. Lending protocols aim to maintain a utilisation ratio that is close to but below 100% to maximise profits and minimise risk (cf. the kink in Figure 2). The main reason for targeting a utilisation ratio below 100% is to manage liquidity risk. If all assets were borrowed (utilisation ratio 100%), depositors would not be able to withdraw their assets. Such a situation represents an undesired liquidity shortage.

The optimal target for the utilisation ratio depends on the probability of a liquidity shortage: For a given asset or market condition, the higher the liquidity risk, the lower the target ratio to mitigate the risk. To find the optimal target ratio, it is therefore necessary to analyse the conditions under which liquidity risk is high.

One of the significant liquidity risk drivers in DeFi is the concentration of deposited amounts. Concentration is high if only a few depositors make up most of the protocol's assets. In a concentrated protocol state, a large depositor withdrawing assets is likely to cause liquidity issues because a relatively larger amount of the pool is now in the hands of the borrowers and not freely available for withdrawals. In contrast, pools with many small depositors are less likely to cause liquidity issues because the withdrawal of assets by any one depositor has less impact on the overall market (see also section 4.2). In other words, liquidity shortage is less likely in these pools because the risk is spread out among many different depositors rather than being concentrated in a few large ones.

Incumbent lending protocols such as Aave have proven that the problem can be solved using specific utilisation ratio targets lower than 100%. However, the problem is more pronounced at the launch of a new protocol, when only a few lenders and borrowers are participating on the platform. In this case, the concentration is usually higher. For example, Figure 3 shows the deposit shares of the top 50 USDC depositors on Aave at the time when the platform was first deployed on the Ethereum network.

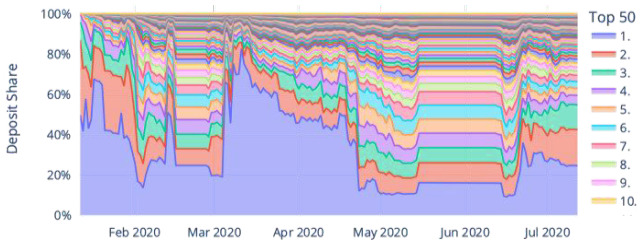


Figure 3. Deposit shares of the top 50 USDC depositors on Aave between January and June 2020 (relative to each other) [15]

Note: Deposit shares and rank (top 50) are calculated using the 50 largest depositors at specific points in time. This means that the largest depositor on a given day may be a different user than the largest depositor on another day.

Figure 3 clearly illustrates that the percentage of the largest depositors and, thus, concentration decreases over time. In the first few months of a new lending protocol, governors may, therefore, need to set a lower target ratio to compensate for the increased liquidity risk.

However, setting a low target ratio has major downsides. Low interest rates may not be attractive to depositors, who may prefer to deposit their funds on other platforms that offer higher rates. Setting a lower utilisation target ratio will make the platform less efficient than incumbent platforms. With such a strategy, in combination with network effect, it is difficult for a new lending platform to reach a critical size, and thus it is at risk of failing.

To mitigate the problem, Folks Finance proposed a reward mechanism to incentivise depositors to lock up their assets initially, thus reducing the risk of withdrawals at a critical time. This strategy allows for setting competitive interest rates without increasing liquidity risk. To implement the solution, however, several practical challenges must be solved. First, there is a need to determine how to measure concentration. Second, a reward system must be designed that incentivises users to lock assets without negatively impacting the incentive design around the utilisation ratio.

4. Risk Measurements

As explained in the previous section, liquidity concentration relates to liquidity risk. But what is the best way to measure concentration? Several existing economic indices can be considered to quantify the risk in liquidity pools on a lending platform: the concentration ratio, the HHI, and the Gini index. The concentration ratio and HHI are commonly used to measure the market concentration in whole industries [16]. The HHI can additionally be used to measure the distribution of wealth between households [17]. The Gini index can be used to measure concentration as well as inequality on blockchains [6, 18].

4.1 Measuring Concentration

Concentration Ratio. The concentration ratio is used to measure market concentration in industries. Because it is a straightforward representation of the size of major actors in an industry, the concentration ratio is an obvious choice to represent the size of significant actors in liquidity pools. To calculate the index, the liquidity shares for the m largest depositors are added together,

$$CR_m = \sum_{i=1}^{m} s_i$$

with $s_1 \geq s_2 \geq \cdots \geq s_n$,

for a total of n depositors. For example, CR_4 denotes the combined liquidity share of the four largest depositors. This results in an index

between 0 and 1. The higher the index, the more liquidity the largest m depositors hold.

Herfindahl–Hirschman index. Instead of including only the largest depositors in the pool, the HHI considers the whole distribution. The HHI is calculated by squaring each depositor's market share and adding these squared values together,

$$HHI = \sum_{i=1}^{n} s_i^2$$

with $s_1 \geq s_2 \geq \cdots \geq s_n$ and n depositors.

The resulting index again ranges from 0 to 1, with a higher value indicating a more concentrated liquidity pool.

Gini index. The Gini index measures concentration and economic inequality by comparing the distribution of wealth among members in a pool. It too ranges from 0 to 1, with 0 indicating perfect equality (everyone has the same amount) and 1 indicating perfect inequality (one person has everything and the rest nothing). A higher Gini index indicates a greater degree of inequality in the distribution of wealth or income. The formula is as follows:

$$G = \frac{2\sum_{i=1}^{n} i \times s_{n+1-i}}{n\sum_{i=1}^{n} s_i} - \frac{n+1}{n}$$

with $s_1 \geq s_2 \geq \cdots \geq s_n$.

4.2 Efficacy of the Indices

We turn now to examining the suitability of the CR, HHI, and Gini index for assessing liquidity risk on a lending platform. To do so, it is necessary to consider their ability to adequately reflect the risk associated with the distribution of deposit shares and the number of deposits.

Liquidity risk relates to the probability of a significant withdrawal from the liquidity pool. The CR cannot capture the liquidity risk of an entire distribution because it does not account for variations between depositors – it simply reflects the *combined* share of the largest depositors.

To illustrate, consider a market where the concentration ratio of the five largest liquidity holders is 50%, i.e., □CR□_5=0.5. It is unclear whether one liquidity holder is providing 40% of the pool and the remaining four holders are providing the remaining 10%, or all five holders are providing 10% of the pool. The liquidity risk associated with these two scenarios is quite different, yet the CR would be the same in both cases. Therefore, we conclude that CR is not suited for liquidity risk assessment and focus on the other two measurements that consider details of the contribution.

Concerning the number of depositors, the HHI outperforms the Gini index. As stated, liquidity risk is related to the ability to withdraw a certain share from the liquidity pool. It is therefore crucial to know if the liquidity pool consists of a few large or many small deposits. In other words, the number of deposits matters. While the HHI takes into account the number of deposits, the Gini index does not. To illustrate, assume all deposits are the same size. If there are N liquidity holders with identical shares, the HHI is 1/N. As the number of users increases, this index converges to 0, the minimum value. On the other hand, if a single holder provides 100% of the pool, the HHI is 1, the maximum. Thus, the HHI reflects liquidity risk adequately. The exact opposite holds for the Gini index, however. If deposit size does not vary, the Gini index remains the same independent of the number of deposits. Furthermore, additional depositors with very small deposits can have a large impact on the index, whereas this is not the case with the HHI.

Given these considerations, in what follows we use HHI as the preferred measure of liquidity risk.

5. Risk Mitigation with Lock & Earn Using HHI

To protect liquidity pools – especially at their early stages – against risks stemming from high market concentration, Folks Finance has developed a scheme called "Lock & Earn".

5.1 Lock & Earn

To ensure the constant and wide availability of funds in the protocol, Folks Finance differentiates ordinary depositors from those who participate in Lock & Earn (L&E), considering the latter as long-term depositors by tying up their liquidity for a fixed term. This mechanism differentiates them from ordinary depositors, who can withdraw their assets at any time. This system has been specifically designed to create a pillow pool of assets that will allow low-cost loans to launch a new pool and increase the security of redeemable assets.

L&E participants agree to keep the liquidity inside the protocol for a long time to stabilise it. In return, they receive folks-reward tokens. This incentive increases their annual percentage rate relative to ordinary depositors.
The value of the incentive is set by Folk Finance governors. Considering the liquidity needs of the different pools, the incentives can be updated and adjusted based on governance choices.

5.2 The Impact of L&E and Reward Calibration

It can be shown analytically that L&E increases liquidity bootstrapping and reduces liquidity risk. Assume we have a liquidity pool that has not yet introduced L&E. The depositors earn an interest rate $i_d(U)$ which depends on the utilisation ratio U. The outside option for the depositors is r>0, i.e., the return they could get elsewhere. Because depositors value their ability to withdraw assets at any moment (as renouncing liquidity entails a risk), the total reward for L&E needs to be higher, i.e., $i_l > i_d$.

Proposition: The introduction of L&E always helps bootstrapping more liquidity.

Proof:
We consider a mass of potential depositors with different valuations of the outside option r and the value of being liquid in the next period ϕ, distributed according to the continuous function $f(r,\phi)$. Assume that an equilibrium exists for the utilisation ratio U^* and corresponding equilibrium depositor and borrower interest rates i^*_d and i^*_d. Without L&E, only depositors with $i^*_d > r$ make deposits. The introduction of L&E leads to two changes:

1. *Some potential depositors with $i^*_d > r$ and $i_l > r + \phi$ who did not participate before deposit with L&E.*
2. *All depositors with $i_l - i^*_d > \phi$ and $i_l - r - \phi > 0$ now deposit with L&E instead of normally.*

The resulting total deposits (deposits + L&E) are larger than before if $i_l > i_d$. The change in the number of total depositors affects the utilisation ratio and, in turn, the interest rates, which deviate from the equilibrium. There are two cases to consider:

1. *If only the borrowers react to the change in interest rates, they borrow additional assets until the interest rates return to their previous levels.*
2. *If only the depositors react to the change in interest rates, some will reduce their deposits in favour of making L&E deposits, while others will decrease their deposits in favour of not participating. This gradual return to the equilibrium leads to the same total amount of deposits as before, but with a fraction now participating in the L&E programme.*

Any combination of borrower and depositor reactions will result in a scenario between these two extremes, with total deposits being slightly larger than before.

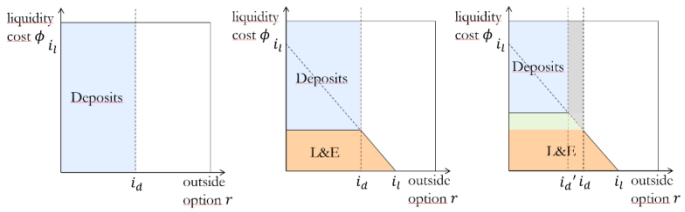


Figure 4. Illustration of the proof

Figure 4 illustrates the proof using the distribution $f(r,\phi)=U(r)\times U(\phi)$. Without L&E, only normal deposits are made by depositors with an interest rate higher than their outside option (left). If L&E is introduced, new potential depositors are gained, and a fraction of existing depositors with low liquidity costs also switch to L&E (middle). After the change in the utilisation ratio, the depositors' interest rates also change. Depending on whether borrowers or depositors react more to this change, the grey area consists of depositors or non-depositors, and the green area consists of depositors or L&E depositors (right).

As the total number of deposits (including L&E) increases, the relative size of each individual depositor (who is not participating in the L&E programme) in the pool decreases. This results in a lower concentration of the pool, which reduces liquidity risk. Figure 4 shows that boosting liquidity through the L&E programme comes at the cost of losing some normal depositors. The size of L&E (and thus the difference between i_l and i^*_d) is a trade-off between safety and cost. If the rewards are sufficient but not too large, the L&E programme can increase liquidity and reduce liquidity risk at a low cost. This raises the question: How to determine optimal L&E level?

5.3 Computation of Optimal L&E Level

L&E is expensive for a lending platform. Therefore, finding a suitable trade-off between the protocol's security and expenses is essential. To determine the safety of a liquidity pool, it must be calculated how much liquidity is at risk. This is strongly dependent on the concentration in the liquidity pool. The higher the concentration, the more the platform's safety is exposed to individual liquidity providers.

In the first step, we assume that a certain fraction, α, of the liquidity pool is at risk of being withdrawn in a short period of time. This value will be determined later using HHI discussed in section 5.4. We also assume that a total value of D (in USDC) has been deposited in the pool by depositors and a total of B (in USDC) has been borrowed. Therefore, the initial utilisation ratio is $U=B/D$. If a fraction α of the pool is withdrawn, the utilisation ratio will immediately become $U=B/(1-\alpha)D$.

The minimum amount of L&E the lending platform provides for long-term deposits can now be calculated. Depending on the risk aversion of the lending platform, the governance sets a maximum utilisation ratio, $U_{max}>0$. The higher U_{max} is set, the less risk-averse the platform is and the lower the cost it incurs on interest payments for L&E. L&E (referred to as L for short) is now determined by

$$\frac{B}{(1-\alpha)D+L} \leq U_{max}.$$

This formula calculates the amount of additional L&E that is required to ensure that the utilisation rate does not exceed U_{max}. Solving for L yields

$$L \geq \frac{B}{U_{max}} - (1-\alpha)D,$$

where α is the fraction of deposits at risk and U_{max} is the exogenously set maximum utilisation ratio. This allows us to calculate the minimum amount

$$L = \frac{B}{U_{max}} - (1-\alpha)D,$$

that will ensure that the utilisation rate, U, is less than or equal to U_{max}. If the interest rate payments for L&E i_l are high enough, the full amount L can be brought into the pool (see the graphic illustration in Figure 4).
If the amount of L&E in the pool has already been determined, a different formula is used. In this case, the formula uses total deposits, which includes the existing L&E and normal deposits, instead of just deposits D. The purpose of this formula is to calculate the remaining amount of L&E needed rather than determining the overall required amount of L&E.

5.4 Implementation of L&E at Folks Finance

Folks Finance introduced L&E to mitigate liquidity risk and for liquidity bootstrapping. To balance the trade-off between safety and cost, an index based on s_1 and HHI was chosen for the calculation of liquidity at risk α. Specifically, Folks Finance has taken the size of the largest depositor (s_1) and multiplied it by a scalar which represents the remaining concentration,

$$\alpha = s_1 \times f(HHI)$$

$$\text{with } f(HHI) = f(x) = \begin{cases} 1, HHI < 0.15, \\ 1.25, 0.15 \leq HHI < 0.25, \\ 1.5, HHI \geq 0.25. \end{cases}$$

The choice of α for the liquidity at risk index is based on a balance between security and cost savings. It considers the effect of the largest depositor's withdrawing assets quickly on the concentration of the remaining depositors. The resulting formula for L&E is

$$L_{Folks} = \max\left(\frac{B}{U_{max}} - \left(1 - s_1 \times f(HHI)\right)D, 0\right).$$

5.5 Numerical Example

For this example, we used data from three deposit distributions on USDC on Aave in early 2020. The data for this example was downloaded from Flipside on 21 February 2022 [16]. We calculated s_1, the HHI, and the relative amount of L&E compared to deposits $(\Delta L=L/D)$ for three different expected utilisation ratios $(U=B/D)$ at three different timestamps. The maximum utilisation ratio used for this calculation is U_{max}=0.99. The resulting L&E ratios for the three days and scenarios are shown in Table 1.

Table 1. Calculation of L&E level

	HHI	s_1	$\Delta L\|_{U=0.65}$	$\Delta L\|_{U=0.75}$	$\Delta L\|_{U=0.85}$
1.2.2020	0.16	26%	0	8%	18%
1.4.2020	0.22	44%	21%	31%	41%
1.6.2020	0.06	15%	0	0	1%

Table 2 shows the utilisation ratios with and without the introduction of L&E on the platform, assuming that the largest depositor withdraws their fund immediately on that day.

Table 2. Resulting utilisation ratio if the largest depositor withdraws his assets.

Utilisation ratio if s_1 withdraws	U for $\Delta L\|_{U=0.65}$		U for $\Delta L\|_{U=0.75}$		U for $\Delta L\|_{U=0.85}$	
	L&E	No L&E	L&E	No L&E	L&E	No L&E
1.2.2020	0.87	0.87	0.91	1.01	0.92	1.14
1.4.2020	0.85	1.17	0.86	1.35	0.87	1.53
1.6.2020	0.76	0.76	0.88	0.88	0.99	1.00

Note: The table shows the scenario with and without L&E.

With the liquidity risk mitigation introduced, the utilisation ratio is less likely to reach critical levels and does not reach 100% if the largest depositor withdraws, assuming the L&E depositors did not deposit before.

6. Conclusion

This article investigates the liquidity risk faced by new DeFi lending platforms, using the example of Folks Finance. It is found that liquidity risk is particularly pronounced for new lending platforms and can be effectively measured using the HHI. The article also shows that a reward mechanism, when properly implemented, can reduce liquidity risk and increase liquidity bootstrapping for a new lending platform. The findings suggest that new DeFi lending platforms (a) should be cautious about liquidity risk, (b) should consider using HHI for risk measurement, and (c) should consider implementing a reward programme to incentivise liquidity holdings.

References:

[1] DefiLlama 2022. Accessed on: December 23, 2022. [Online]. Available: https://www.defillama.com

[2] A. Crockett, "Market liquidity and financial stability", Financial Stability Review, vol. 11, pp.13–17, February 2008. Accessed on: December 29, 2022. [Online]. Available: https://ideas.repec.org/a/bfr/fisrev/2008113.html

[3] K. Nikolaou, "Liquidity (risk) concepts: definitions and interactions", European Central Bank Working Paper Series 1008, February 2009. Accessed on: December 29, 2022. [Online]. Available: http://dx.doi.org/10.2139/ssrn.1333568

[4] BIS: Bank for International Settlement BIS Basel Committee on Banking Supervision, "Principles for Sound Liquidity Risk Management and Supervision", Bank Asset and Liability Management, pp. 143–146, September 2018. Available: https://doi.org/10.1002/9781119444497.app1

[5] IMF: International Monetary Fund IMF, "Global Financial Stability Report 2008", April 2008. ISBN 9781589067202. Available: https://doi.org/10.5089/9781589067202.082

[6] CEBS: Committee of European Banking Supervisors, "Guidelines on the management of concentration risk under the supervisory review process (GL31)", European Banking Authority, 2010. Accessed on: December 20, 2022. [Online]. Available: https://www.eba.europa.eu/regulation-and-policy/supervisory-review/guidelines-on-the-management-of-concentration-risk-under-the-supervisory-review-process

[7] V. V. Acharya and L. H. Pedersen, "Asset pricing with liquidity risk", Journal of Financial Economics, vol. 77, no. 2, pp. 375-410, August 2005. Available: https://doi.org/10.1016/j.jfineco.2004.06.007

[8] L. Pástor and R. F. Stambaugh, "Liquidity Risk and Expected Stock Returns", Journal of Political Economy, vol. 111, no. 3, pp. 642-685, 2003. Available: http://dx.doi.org/10.1086/374184

[9] Aave 2022: Aave documentation. Accessed on: December 23, 2022. [Online]. Available: https://docs.aave.com/risk/liquidity-risk/introduction

[10] L. Gudgeon, S. M. Werner, D. Perez, and W. J. Knottenbelt. "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency", ACM Conference on Advances in Financial Technologies, pp 92-112, 2020. Available: https://doi.org/10.1145/3419614.3423254

[11] X. Sun, C. Stasinakis, and G. Sermpinis. "Liquidity Risks in Lending Protocols: Evidence from Aave Protocol", SSRN, October 2022. Accessed on: December 23, 2022. [Online]. Available: https://dx.doi.org/10.2139/ssrn.3985105

[12] Folks Finance Docs 2022. Accessed on: June 17, 2022. [Online]. Available: https://docs.folks.finance/

[13] P. Belleflamme and M. Peitz, "The Economics of Platforms", Cambridge University Press, 2021.

[14] J.-C. Rochet and J. Tirole, "Platform Competition in Two-Sided Markets", Journal of the European Economics Association, vol. 1, no. 4, pp. 990-1029, June 2003. Available: https://doi.org/10.1162/154247603322493212

[15] M. Armstrong, "Competition in Two-Sided Markets." The RAND Journal of Economics, vol. 37, no. 3, pp. 668–91, Autumn 2006. Available: https://doi.org/10.1111/j.1756-2171.2006.tb00037.x

[16] Flipside. Accessed on: February 21, 2022. [Online]. Available: https://flipsidecrypto.xyz/

[17] P. Belleflamme and M. Peitz. Industrial Organization: Markets and Strategies. Cambridge University Press, 2010. ISBN 9780521862998. Available: https://books.google.ch/books?id=nmUcldoQ

[18] S. A. Rhoades. "The Herfindahl-Hirschman Index", Federal Reserve Bulletin, vol. 79, no. 3, pp. 188-189, March 1993. Accessed on: December 10, 2022. [Online]. Available: https://fraser.stlouisfed.org/files/docs/publications/FRB/pages/1990-1994/33101_1990-1994.pdf

Competing Interests:
All authors are affiliated with the use case presented in this manuscript.

Ethical approval:
Not applicable.

Author's contribution:
MH coordinated the manuscript, drafted sections on economics and liquidity risk, and edited all sections. RD conducted analysis on liquidity risk, conducted and drafted the literature review, and edited various sections. NG drafted the sections on risk measurements and risk mitigation with L&E using HHI. JS provided input on platform economics. BB, GK, MR, and AA provided inputs on the L&E mechanism and drafted the section on lending platforms.

Funding:
This research was self-funded by the Center for Cryptoeconomics and Folks Finance.

Acknowledgements:
Not applicable.

THE JBBA

ESSAY

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/ jbba-6-1-(6)2023

Metaverse for Public Good: Embracing the Societal Impact of Metaverse Economies

Naseem Naqvi MBE
Centre for Evidence-Based Blockchain, The British Blockchain Association, UK

Correspondence: metaverse@britishblockchainassociation.org
Received: 20 March 2023 **Accepted:** 4 April 2023 **Published:** 7 April 2023

Abstract

The metaverse is internet's next tectonic shift. Currently, there are approximately 400 million monthly users of the collection of worlds that make up the metaverse [1], with projected growth to 5 billion users worldwide by the end of the decade This is expected to drive a total addressable metaverse market of $8–13 trillion by 2030 [2]. According to Statista, 15% of the world's digital economy has already shifted to the metaverse [3], and many "world's first" metaverse initiatives have been launched over the past two years [4] [figure 28]. The potential applications of a metaverse for public services are vast, including remote governance, service delivery, virtual public spaces, enhanced transparency and accountability, increased social connectedness, improved access to information and education, new job opportunities, innovative forms of entertainment and creativity, and improved accessibility, to name a few. This article explores the practical applications of the metaverse for citizens and some multidisciplinary use cases from around the world. We also examine the national metaverse strategies and opportunities as well as challenges of the metaverse ecosystems, including its potential impact on society and public services. Finally, we propose some recommendations for policymakers and governments to construct forward-thinking metaverse economies.

Keywords: *Metaverse, Blockchain, Web3, Decentralisation, Public Services, Citizens, Government, Economy*

JEL Classifications: *A30, M37, M38, G23, G24, L26*

1. Introduction

The metaverse ushers in a new era of digital reality and human-computer interaction by enhancing the integration of the physical and virtual worlds. In 2021, the British Blockchain Association released a summary of an open metaverse economy [figure 43] which outlined three crucial facilitators: technology, creators, and finance. Additionally, the summary detailed seven essential features, including persistency, a user-centric economy, open source, accessibility, and interoperability, et al [63]. The term "metaverse" refers broadly to an extended reality experience that brings together a range of emerging technologies, such as virtual reality, augmented reality, artificial intelligence, blockchain, Internet of things (IoT), 5G, spatial computing, cryptographic assets, and others, in a persistent environment where users can interact with each other and the digital content using 3-D rendered digital twins or avatars. These fundamental elements for constructing metaverse experiences have been in existence for several years [5]. Merriam Webster dictionary defines the metaverse as "*a persistent virtual environment that allows access to and interoperability of multiple individual virtual realities*" [6].

The notion of a metaverse (or "the" metaverse to describe all-encompassing metaverse ecosystems) has gained substantial attention in recent years, primarily due to technological advancements that have enabled the creation of increasingly immersive virtual experiences [7]. The metaverse has significant potential applications in government and public services, including but not limited to remote governance, public service delivery, virtual public spaces, enhanced government transparency and accountability, increased social connectedness, improved access to information and education, new job opportunities, improved accessibility for people with disabilities, and new forms of entertainment and creativity, to name a few.

At the same time, it is crucial to proactively recognise and address the potential challenges associated with the metaverse. These challenges may include issues related to privacy, legality, security, identity, ownership, accessibility, cost, and availability of metaverse-related technologies [8]. By addressing these concerns, we can ensure that the benefits of the metaverse can be realised, while minimising any negative impacts that may arise from its adoption. Public and private sector enterprises are utilising the metaverse and its related technologies to foster growth, enhance productivity, and improve their ability to govern effectively. By leveraging the metaverse, they can make their administrative processes more efficient and provide better services to their communities.

In this article, we have examined some of the examples of public-sector and community-based use cases and practical implementations of the metaverse from around the globe [9]. We explore the real-world applications of the metaverse by highlighting national metaverse strategies and analyses the opportunities and challenges of the metaverse economy, including its potential impact on society and public services. Finally, based on our findings, we will propose recommendations for policymakers and governments to construct forward-thinking digital economies that can effectively harness the potential of the metaverse. By taking a comprehensive approach to understanding the practical implications of the metaverse, we can unlock its full potential to foster growth, enhance productivity, and improve the lives of citizens around the world.

Preserving a Nation in the Metaverse: *The Case of Tuvalu*

"Our land, our ocean, our culture are the most precious assets of our people and to keep them safe from harm, no matter what happens in the physical world, we will move them to the cloud," said Simon Kofe, Tuvalu's foreign affairs minister at the 2022 United Nations Climate Change Conference (COP27) [10]. Tuvalu is

a small country in the middle of South Pacific which is facing an existential threat due to rise in sea levels.

Figure 1: Tuvalu's Foreign Minister Kofe at COP27

As Mr. Kofe virtually addressed world leaders [figure 1], the camera zoomed out to reveal Kofe standing in Teafualiku, the smallest islet in Tuvalu. "*Islets like this one won't survive rapid temperature increases and rising sea levels*," he said, "*so we'll re-create them virtually - piece by piece, we'll preserve our country, provide solace to our people, and remind our children and our grandchildren what our home once was*" [11].

Tuvalu's official website now features a real-time, live update counter that tracks the progress of everything from digital twins of government buildings to public documents, to sights and sounds of local birds being uploaded and preserved in the metaverse [Figure 2].

Preserving heritage in the metaverse provides an opportunity to safeguard cultural and historical assets against threats such as climate change, natural disasters, and human activity. The case of the dodo, a bird native to Mauritius which became extinct due to human activity 200 years ago, serves as a cautionary tale about the importance of preserving such assets in a format that can withstand the test of time. By utilising the metaverse to digitally recreate and preserve cultural heritage, future generations can experience and learn from their past in a way that was previously impossible. Additionally, the metaverse allows for the creation of interactive and immersive social experiences that can provide a deeper understanding and appreciation of a nation's cultural heritage. Tuvalu's innovative approach to preserving their nation's heritage serves as a powerful example of how the metaverse can be utilised to ensure that cultural heritage is not lost, but instead continues to thrive and evolve.

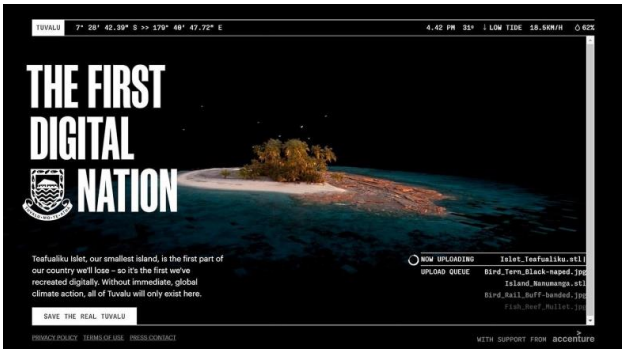


Figure 2: Tuvalu's official website showing real-time live updates of nation's heritage being uploaded on the metaverse: https://www.tuvalu.tv/

Public Service Delivery and Remote Governance: "*The Metaverse Seoul*"

One of the potential applications of metaverse in government and public services is remote governance. A metaverse could allow government officials and citizens to interact with each other in an interactive, immersive, 3-D virtual environment, making it possible for public services to be delivered remotely, inclusively, and efficiently [12]. This could be particularly beneficial for people who live in regions where access to public spaces is limited. It can also provide a safe and inclusive environment for socialisation and community building for people who live in rural or remote areas, or for those with mobility issues. From a government's perspective, the metaverse could be used to provide services across the "BIG 7" – Business, Education, Governance, Healthcare, Entertainment, Creative Industries, and Science & Technology. Metaverse could provide a virtual platform for citizens to interact with each other, participate in public events, and engage in discussions about public policy and governance.

As a component of its "Digital New Deal" political strategy, South Korea has been increasing its efforts in the realm of metaverse initiatives [13]. In February of 2022, the country revealed intentions to allocate roughly $200 million in financing for metaverse projects, distributing grants to universities and businesses to aid in the advancement of their technologies. [14]. Seoul was the first city to outline metaverse ambitions in November 2021 and in January 2022 announced that it would invest KRW 223 billion in metaverse technologies, as part of its digital transformation strategy.

Figure 3: Metaverse Seoul, South Korea: Mayor's office in the metaverse

The Metaverse Seoul offers a platform for government officials to share information and engage with citizens in a transparent and accountable manner [figure 3]. This is done through virtual town halls, public forums, and other interactive events, allowing citizens to meet their councillors and mayors, and hold their elected officials accountable for their actions [15].

The Mayor of Seoul has been meeting citizens in the metaverse, where people can lodge complaints and visit the virtual replica of the city [figure 4]. By 2026, the South Korean capital aims to have a metaverse environment for all administrative services, including economy, education, culture, and tourism. The South Korean government is believed to be investing around $34 million in this project [16]. The Metaverse Seoul will also include services such as a fintech lab, a corporate support center, Seoul's top 10 tourist attractions, a youth mentoring counselling room and tax services.

Figure 4: Metaverse Seoul (opengov.seoul.go.kr)

The "Cognitive Cities," Digital Twins, and the NMOs: *The Case of "The Line"*

Saudi Arab is building the world's first metaverse "cognitive city" – XVRS [figure 5], where people can travel and "live" in the metaverse, while the city is being physically built [17]. Therefore, unlike the digital twin of a physical city like Seoul, Saudi Arab is building a physical twin of the city that exists in the metaverse – also called NMOs or "Native Metaverse Organisations." This innovative approach to building a smart futuristic city in the metaverse will make it possible for people from anywhere in the world to visit NEOM virtually, before making investment decisions about buying a physical real estate in The Line.

Figure 5: XVRS: Metaverse Cognitive City The Line, Saudi Arabia

Public–Private Collaboration: *The Case of Shanghai's Metaverse Pilot*

At the end of 2021 Shanghai announced a 5-year plan to leverage the metaverse for public and private stakeholders [18]. Furthermore, the Chinese government also announced its ambition to grow the local metaverse industry to a whopping $52 billion by 2025, while adding 10 globally leading enterprises and an additional 100 more new metaverse companies to the metaverse ecosystem [19]. This news was accompanied by the announcement of a new $1.5 billion fund to support metaverse development [20].

In the Shanghai Metaverse Pilot Programme, some of the services for citizens are already up and running, such as the "Metaverse Diagnose System" at Shanghai Eye Hospital, an affiliate of Fudan University, enabling doctors to use 3D remote diagnosis equipment to treat patients. China is also building the metaverse infrastructure for Urban planning, work and education, tourism, and entertainment, fintech and payments, healthcare, government and public services, businesses, and creative industries, to name a few [21].

According to the plan [figure 6], Lin-gang, a Special Development Area and pilot zone for the city's artificial intelligence industry, the region will strive to develop the overall scale of the extended reality and metaverse industry to see revenue exceed 10 billion yuan within three to five years. Focusing on key metaverse components, technologies, terminal equipment, content supply, software, and other areas, it will build a number of public service platforms covering the whole metaverse industrial ecosystem for citizens [22].

Virtual Public Spaces: *Celebrating Days of National Significance in the metaverse*

A metaverse could provide a virtual platform for citizens to interact with each other, participate in public events, and engage in discussions about public policy and governance. This could be especially beneficial for people who are unable to physically attend public events, or for those who live in regions where access to public spaces is limited.

From 22 to 24 September 2022, Saudi Arabia celebrated its 92nd National

Figure 6: Shanghai's XR Conference 2023, discussing China's 3-year Metaverse Plan

Day [figure 7] in the metaverse [23]. The three-day celebration took place in Decentraland [24]. From traditional NFT (non-fungible token) outfits to an open-air museum, the immersive experience paid homage to Saudi Arabia's culture and history. Event attendees were able to explore Saudi Arabia's civilisation, tradition, art, and history [figure 8]. Furthermore, the visitors were able to buy wearable NFTs inspired by Saudi national attire, as well as Proof of Attendance Protocol NFTs (POAPs).

Figure 7: Saudi Arabia's National Day in the metaverse

During the period of UK's national mourning following the death of Her Majesty the Queen, a tribute was paid to her at the BBA's metaverse headquarters [25]. A minute's silence was also observed at in the honour of The Queen [figure 9].

Figure 8: BBA president, Prof Naseem Naqvi, in his digital avatar, visiting Saudi Arabia's National Day in the Decentraland Metaverse

Metaverse Economic Zones – The "MEZs": *The Case of Japan*

Japan has recently launched the Metaverse Economic Zones or "MEZ"s, which are a consortium of technology giants coming together to build a metaverse for citizens [26]. These include major Japanese technology, manufacturing, and finance firms collaborating to create the infrastructure

Figure 9: Official national mourning, The Queen, BBA's Metaverse Headquarters, 10 September 2022

for an open metaverse towards Japan's national Web3 strategy [figure 10]. The Metaverse Economic Zones features "Auto-learning Avatars," which collect users' information to provide a personalised metaverse experience, as well as "Multi-Magic Passport" that will enable identification and payment methods to facilitate interoperability within the metaverse space for the users. This is particularly relevant since most centralised metaverses such as Roblox or Minecraft, a user is unable to transport its digital assets, payments, history, data, and identity to the other platforms since the platforms are not interoperable and do not talk to each other [27].

In November 2022, Japan's Digital Ministry announced plans to create a decentralized autonomous organization (DAO) to help government agencies enter Web3 [28].

National Metaverse Strategy: *The Case of Dubai*

The UAE has set its sights beyond just competing in the metaverse arena and instead aims to be the dominant player in the region. This goal is evidenced by their published 5-year metaverse roadmap [figure 11] and plans to generate 40,000 virtual jobs, contributing approximately $4 billion USD to the economy [29].

Figure 10: Metaverse Economic Zones, MEZs, Japan

Dubai's metaverse strategy includes attracting 1,000 metaverse-related companies in the sector by 2030. A new metaverse accelerator has also been launched in Dubai, a city that is also home to a growing number of blockchain venture funds with active investing interest in the metaverse [30].

In May of 2022, Dubai's Virtual Assets Regulatory Authority (VARA) became the first government regulatory authority to enter the metaverse [figure 12] when it launched its headquarters (VARA Hq) in the Sandbox [31].

In recent times, devising metaverse policies to stimulate economic growth at a national level has become increasingly paramount [figure 13]. Various

Figure 12: UAE announcing the launch of Metaverse VARA Headquarters

countries have developed their own distinct metaverse strategies [32] with different goals and scopes. These strategies have been shaped by various socioeconomic and political factors, resulting in different patterns and approaches to metaverse development, as highlighted in table below:

Country	Key elements of the metaverse strategy	Sample projects/goals
China	• The country has a strategic approach: "use the virtual to enhance the real, use the virtual to strengthen the real." • CICIR analyzed the metaverse's national security challenges. • The country is reported to be studying a registration system for metaverse users. • Shanghai: the metaverse as among the four "frontiers for exploration."	• The country is developing a teaching center with immersive technology to foster CCP values. • Shanghai: US$1.5 billion investment. Goal: to develop 10 leading companies and 100 small-sized firms and launch 100 products and services by 2025.
Saudi Arabia	• The metaverse is a key part of Vision 2030. • The country launched the National Gaming and Esports Strategy.	• The US$500 billion futuristic megacity NEOM will have its own metaverse. • Gaming and esports market: US$6.8 billion by 2030, 39,000 jobs.
South Korea	• The country launched K-metaverse 2022. • 2022: investment of US$185 million in metaverse-related projects.	• The country plans to select 70 K-metaverse companies and provide them with customized supports. • 2021: Seoul announced a five-year plan to build the city's digital twin; a beta test run of its first stage was in August 2022.
The UAE	• The country plans to measure economic success using gross metaverse product • The country plans to focus on tourism, education, government services, retail and real estate. • The country plans to launch a task force to evaluate opportunities for exporting culture. • Dubai: aims to make the city among the world's top-10 metaverse economies. Goal: attract more than 1,000 blockchain and metaverse companies and support more than 40,000 virtual jobs by 2030.	• The Ministry of Economy: plans to have its headquarters in the metaverse. • Dubai city's digital twin will be in the metaverse. • Sharjah: has plans for the "Virtual Transaction Centre—Metaverse."

CICIR: China Institute of Contemporary International Relations; CCP: Chinese Communist Party.

Figure 13: National Metaverse Strategies Computing's Economics, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10042106)

Government Communication through the Metaverse:
Emmanuel Macron of France and Mayor of Orlando of USA

Government leaders have started delivering their speeches in the metaverse. In 2022, French President Emmanuel Macron delivered his presidential speech in Decentraland [33] addressing the business communities, and to quote him:

"*We are reindustrializing the nation – The metamorphosis is always scary, but formidable. the innovations will make the great revolutions of tomorrow!*" [figure 14]

Figure 14: President of France in the metaverse

In December 2022, the Mayor of Orlando Florida in USA became the first US politician to deliver a speech [figure 15] in the metaverse [34]. Here is what he had to say:

"*Consider this your personal invitation from the mayor of Orlando. We want to share what we're building here in the Metaverse - There are currently some 2,500 open IT and tech jobs in Orlando, and we want you in Orlando.*"

Education, Learning, and Training in the Metaverse:

Universities have started incorporating metaverse in their curriculum. This includes both teaching about the metaverse (offering courses, research) [35] as well as hosting lectures inside a metaverse environment [36] [figure 16]. Japan built a metaverse-based educational environment to encourage students who cannot afford to attend in-person lectures. Toda, Japan's city in the Saitama prefecture, is solving the problem of growing absenteeism by utilising metaverse tools [37]. Students far away from school can attend class daily and explore their campus from their comfort zone. To enable metaverse schooling and fulfil attendance sheets via participating in the virtual classrooms, candidates must first obtain approval from their respective institutions.

Figure 15: Mayor of Orlando in the metaverse

Figure 16: Kwangwoon University Metaverse platform, South Korea

Improving accessibility to knowledge and information is another benefit of the metaverse. It can provide citizens with access to a wealth of information and educational resources [figure 17]. Virtual libraries, museums, and universities can be established, allowing people to learn and explore from anywhere in the world [38]. This can be especially beneficial for people who live in regions where access to educational resources is limited.

Learning in the metaverse offers some unique advantages in the field of research and education. The experience is immersive and kinetic environment such that students can roam and interact with objects, and with each other. This can be used to experience the history of World War 1 in the battlefield, studying human body by becoming a red blood cell in the arteries, be with the molecules to experience the chemical reaction, or experience how it feels like to be with a dinosaur [39] [figure 18].

Figure 17: JBBA Blockchain Research Infographics gallery in the metaverse

Figure 18: Metaverse for Learning and Education

The British Blockchain Association is assisting universities and businesses to take their first step into the metaverse [figure 19]. The learning offered is practical and hands-on, involving visits to various types of metaverses (decentralised, centralised, and hybrid). Participants gain knowledge on NFT-gating, avatar management, the history and future of metaverse economies, and other relevant materials. These masterclasses have been meticulously curated to provide a comprehensive and all-encompassing learning experience for delegates. In addition, a Proof of Attendance (POAP) NFT certificate is issued on the blockchain [figure 20] to serve as a permanent, immutable record of the learning achievement [40]. The students have rated these masterclasses "outstanding." The monthly member networking forums of the BBA have also moved to the metaverse [figure 21 and 22].

Figure 19: BBA Metaverse Headquarters, hosting Epoka University

Improved Emergency Response

To enhance emergency response efforts, metaverse has the potential to facilitate coordination and efficiency. The use of virtual simulations can help to train emergency responders [figure 23]. Additionally, virtual command centres could be established to manage real-time response

efforts. By integrating data from multiple sources such as aircraft, sensors, maps, and databases, an augmented-reality layer of information can be displayed over live drone camera feeds. This provides first responders with the ability to identify roads and powerlines obscured by fire or floodwater, track their own vehicles and personnel, and even tag individuals who may be in danger or suspected criminals [41].

Figure 20: POAP NFTs in the Metaverse for Attendees

Figure 21: The British Blockchain Association's Member Forum at the BBA's Metaverse Headquarters

Figure 22: The British Blockchain Association's Metaverse Headquarters in Spatial: https://bit.ly/3Ya1kSS

Figure 23: Metaverse for emergency response system

Faith and Religious Practices in the Metaverse

In the metaverse, virtual 3-D synagogues and churches have been established [figure 24], offering visitors the opportunity to learn about different faiths, their histories, and collect NFTs related to various religious items. An example of this can be seen in the Decentraland Metaverse [42], where a virtual synagogue has been constructed (Figure 24)

Figure 24: Prof Naqvi at a Synagogue in the metaverse

Increased Social Connectedness

In a metaverse, citizens can have access to a persistent virtual environment where they can interact with each other regardless of their location. This is particularly advantageous for individuals residing in remote areas or those who have difficulty accessing public spaces in person. Within the metaverse, individuals can participate in virtual events, attend concerts, and socialise with friends and family, all within a secure and inclusive environment.

As an example, Harvard Business School hosted an alumni reunion [43] within the metaverse. This event brought together Harvard alumni from 28 different countries, providing them with an opportunity to connect virtually, without the need for air travel [Figure 25]. By utilising the metaverse, such gatherings can reduce the carbon footprint of air travel, while also overcoming other challenges such as visa requirements, costs, COVID-19 restrictions, work absences, and jet lag.

Legal Proceedings in the Metaverse

Colombian courts have conducted a pioneering legal hearing using metaverse technology [44]. Magistrate María Victoria Quiñones Triana of the Magdalena court approved the use of Horizon Worlds technology

Figure 25: Harvard University Alumni Reunion

provided by Meta and virtual avatars to represent participants in the proceedings [figure 26]. According to Magistrate Triana, "*the metaverse is a technological tool that can facilitate access to the administration of justice. The use of information technology in the development of judicial proceedings has the essential purpose of facilitating and expediting these processes.*"

Figure 26: Colombian Court Hearing in the Metaverse

Weddings in the Metaverse

Marriage ceremonies and weddings have taken place in the metaverse, with one of the first legal metaverse weddings occurring in February 2022. The nuptials of Candice and Ryan Hurley were held in the Decentraland metaverse, officiated by Arizona Supreme Court Justice Clint Bolick and facilitated by the Rose Law Group [figure 27]. The virtual ceremony took place at a modified property in Decentraland, designed to resemble a mountain town wedding venue, with the bride's and groom's avatars and thousands of attendees in attendance. Instead of traditional wedding favours, the couple gifted NFTs featuring their dog, Pepper, to guests. Following this milestone event, numerous official weddings have taken place in the metaverse [45–47].

Figure 27: Candice and Ryan Hurley's wedding in the metaverse

Figure 28: World's First Metaverse Initiatives

Sports in the Metaverse

In February 2023, the Islamabad United cricket team from the Pakistan Super League became the first cricket team to join the metaverse. They created a virtual stadium that was built to scale in Decentraland, and it had a twin stadium that was available on Android. Through interactive experiences and challenges, fans could get closer to the cricket action and their favourite team players [figure 29]. Visitors could also explore and interact with different areas within the stadium, including the locker room, players' lounge, and fans conference room. Those who participated and completed challenges were rewarded with official Islamabad United digital kits, club memorabilia, digital assets, and offers from sponsors. This experience provided a unique and exciting way for fans to engage with their favourite cricket team and players [48].

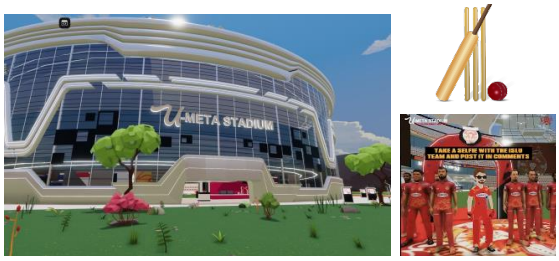


Figure 29: Islamabad United Pakistan Super League Cricket Stadium in Decentraland Metaverse

Travelling and Tourism in the Metaverse

The travel and tourism industry has the potential to be revolutionised by the metaverse. Metaverse technologies are already starting to reshape the industry, from enhancing boarding experiences to immersive virtual reality travel and from extended reality employee training to augmented reality guided tours [49], [50] [figure 30 and 31].

Figure 30: QVERSE: Qatar Airways Lounge in the metaverse

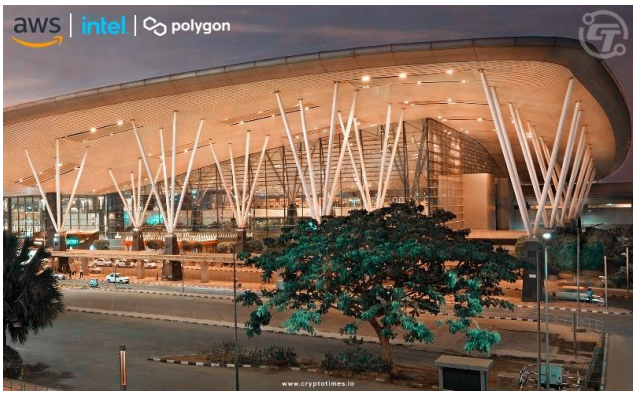


Figure 31: Bangalore International Airport (BIAL) in the Metaverse

Banking in the Metaverse

Banks are beginning to explore the potential of the metaverse. According to a 2022 survey by Accenture [51] 67% of global banking executives believe that the metaverse will have a positive impact on their organisations [figure 32]. Additionally, 47% of bankers believe that customers will use AR/VR as an alternative channel for transactions by 2030, while 38% believe it will be a breakthrough or transformational. The survey also found that 92% of respondents agreed that future digital platforms need to offer unified experiences that enable interoperability of customers' data across different platforms and spaces. JP Morgan and HSBC were among the first banks to launch their metaverse headquarters in 2022, followed by Union Bank of India, Bank of Poland, Sygnum, and others.

Figure 32: Accenture's guide to banking in the metaverse

Commercial Bank International has recently launched its metaverse branch – the first UAE bank to launch a branch in Decentraland. With 24/7 accessibility, minimal carbon footprint compared to a brick & mortar branch, both trad-fi and de-fi services (crypto and fiat) products & services tailor-made to be used within the metaverse economies, metaverse enables persistent, real-time, inclusive, and open access to traditional and crypto finance, and the possibilities are endless [figure 33].

PKO Bank Polski has launched its headquarters in the metaverse [52] [figure 34].

JP Morgan was one of the first banks in the world to launch its metaverse headquarters in the Decentraland [53] [figure 35].

Law Enforcement in the Metaverse:

Law enforcement agencies are recognising the potential of the metaverse, and INTERPOL has recently established its headquarters within this virtual environment to train and educate its staff worldwide [54] [figure 36].

Figure 34: Bank Polski in the Metaverse

Figure 35: JP Morgan in Decentraland Metaverse

Figure 36: INTERPOL's office in the metaverse

World Economic Forum in the metaverse:

The World Economic Forum (WEF) has recently announced its foray into the metaverse by partnering with Microsoft and Accenture to launch the Global Collaboration Village metaverse [figure 37]. This initiative aims to create a virtual space where individuals and organisations can participate in collaborative activities throughout the year, rather than just during a few days each year at Davos. The project is expected to offer a unique experience, leveraging metaverse technologies to promote cross-border collaboration, networking, and knowledge sharing [55].

Enhanced Job Opportunities

A metaverse can provide citizens with new job opportunities in fields such as virtual event planning, digital content creation, and virtual architecture.

This can be especially beneficial for people who live in regions with limited job opportunities, or for those who are unable to work in traditional office environments [56].

Some of the job opportunities that would exist solely in the metaverse:

Figure 37: World Economic Forum in the Metaverse

1. Metaverse avatar clothing designers
2. Metaverse architects, coders, and designers
3. Metaverse event directors
4. Metaverse safety managers and moderators
5. Metaverse research scientists
6. Metaverse marketing specialists
7. Metaverse virtual tour guides
8. Metaverse virtual real-estate agents

Improved Accessibility for People with Disabilities

A metaverse has the potential to serve as a comprehensive platform for individuals with disabilities to engage with each other and avail public services. By designing virtual environments to be inclusive and accessible to persons with disabilities, the barriers to their participation in social and economic activities can be eradicated. The metaverse can also usher in a new era of job opportunities for individuals with disabilities, previously beyond their reach. Additionally, virtual medical consultations and telemedicine services offered within the metaverse could offer disabled individuals the convenience of accessing healthcare services from the comfort of their own homes [57] [figure 38].

The metaverse has the potential to revolutionise the delivery of education to disabled individuals and late-life learners, by providing a wider range of high-quality educational pathways. Immersive technologies allow for the delivery of higher education in an engaging manner, without requiring physical attendance. This mode of delivery eliminates some of the obstacles that prevent many individuals from accessing education, such as having to move away from home or travel to a physical campus. A recent Microsoft survey of 31,102 participants across generations revealed that only 16% did not anticipate carrying out at least some of their job duties as "metawork" in the near future, indicating a growing trend towards virtual work and the potential for the metaverse to transform the workforce.

Figure 38: Source: Five ways the metaverse could be revolutionary for people with disabilities (Brunel University, London)

New Forms of Entertainment and Creativity:

From Justin Bieber to Ariana Grande to Travis Scott, most mainstream artists have now performed in the metaverse. In April 2020, during the pandemic-induced lockdowns, Travis Scott's performance in Fortnite's metaverse attracted nearly 28 million viewers [figure 39] highlighting the potential of the metaverse as a platform for mass-entertainment [58].

Figure 39: Travis Scott in Fortnite Metaverse

Several fashion and sports brands such as Gucci, Luis Vuitton, Dolce Gabbana, Nike, Prada, Zara, Ralph Lauren, Givenchy, Dior, and others have forayed into the metaverse. Decentraland recently hosted the 2023 Metaverse Fashion Week, allowing participants from around the globe to explore and network with others through their avatars [59].

A metaverse also provides a platform for citizens to express their creativity and participate in new forms of entertainment. Virtual games, virtual reality movies and experiences, and virtual concerts [figure 40] can be enjoyed by people of all ages and interests. However, it is important to consider the potential challenges associated with a metaverse. Issues related to privacy, security, and accessibility must be addressed to ensure that all citizens can safely and comfortably participate in virtual environments. Additionally, the cost of accessing a metaverse and the availability of technology must also be considered, to ensure that all citizens have equal access to its benefits.

Figure 40: Metaverse Fashion Week, Decentraland Metaverse

Art in the Metaverse

Many art galleries from around the world have established their presence in the metaverse [figure 41]. Sotheby's, the world's largest brokers of fine and decorative art, and collectibles have opened their digital twin in the Decentraland metaverse [60], [61].

Many art galleries have opened up in the metaverse, showcasing culture, heritage, tradition, and history from around the globe [figure 42].

Figure 41: Prof Naseem Naqvi at Sotheby's in the metaverse

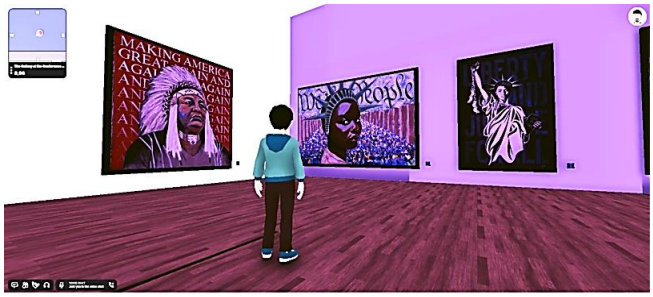


Figure 42: Prof Naseem Naqvi at an art gallery in the Decentraland metaverse

Challenges and Limitations

The emergence of metaverse-centric economies holds immense potential for growth and innovation, as organisations strive to create novel products and services for their consumers. However, this shift also brings along several challenges [62] including the need for new hardware and software infrastructures, privacy and security concerns, and the possibility of monopolies to emerge in the metaverse.

While the benefits of the metaverse for public services are considerable, it is crucial to consider the various challenges and limitations that must be addressed when developing extended reality applications. This includes accessibility concerns and providing equal access to the Metaverse for all citizens, regardless of their socioeconomic status. It is also important to approach the development of the Metaverse in a responsible and ethical manner, considering its potential long-term impact on society and the environment.

Access

While the metaverse has the potential to enhance access to public services, it is important to recognise that not everyone has access to the technology needed to participate in the Metaverse, such as high-speed internet (latency and bandwidth), cost of VR and/or AR devices, and access to education and training resources. The cost of such technologies and the lack of necessary knowledge and awareness for end-users are additional challenges that must be addressed to ensure equitable access to the metaverse.

Interoperability

Interoperability is a critical aspect of the metaverse. Supporters of decentralised metaverse (Web3 metaverse) argue that open source decentralised metaverses such as Decentraland or Sandbox can enable better interoperability and self-sovereignty compared to centralised metaverses such as Roblox or Fortnite. One of the key advantages of Web3 metaverses is that their underlying infrastructure is built on public blockchains such as Ethereum. This enables efficient management of **C**ommunication, **H**istory, **I**dentity, **D**ata, **D**igital **A**ssets, **E**ntitlements, **R**ights, and **social** contacts (***CHIDDERS***) across various platforms. This is in contrast to centralised metaverses such as Roblox or Fortnite, where interoperability between different platforms is limited, and data management is often fragmented. With Web3 metaverses, there is a unified system for managing and sharing data, digital assets, and identity information, which can improve the efficiency and effectiveness of communication and interactions within the metaverse.

Furthermore, the use of public blockchains provides a transparent and secure platform for managing *CHIDDERS*, ensuring that user data and digital assets are protected and that users have control over their information using private keys and self-sovereign identities. This enhances trust and confidence in the metaverse, making it more attractive to users. Overall, the use of public blockchains in Web3 metaverses enables efficient and secure management of *CHIDDERS*, providing a strong foundation for the development of a decentralised and interoperable metaverse ecosystems.

Privacy and Security

Metaverse can be vulnerable to cyberattacks and data breaches, and this poses a significant risk to the privacy and security of citizens using the metaverse for public services. Hackers may try to exploit vulnerabilities in the underlying technology or infrastructure of the metaverse, or they may use social engineering tactics to trick users into revealing sensitive information. A cyberattack or data breach in the metaverse could have serious consequences. It could compromise the personal data of users, such as their identity, communication, assets, financial information, and other sensitive data. It could also disrupt public services that rely on the metaverse, potentially causing widespread disruption and harm.

To address these risks, it is important to implement strong cybersecurity measures and protocols in the metaverse. This includes using encryption or zero-knowledge proofs to protect data in transit and at rest, implementing multi-factor authentication, regularly patching, and updating software and systems, and providing user education and awareness training to prevent social engineering attacks.

Additionally, it is important to have robust incident response plans in place in case of a cyberattack or data breach. This includes having the capability to detect and respond to security incidents quickly using digital forensic toolboxes and communicating with users about any potential impacts or risks.

Digital Divide

The metaverse is a digital environment, which means that it may not be accessible to everyone, particularly those who do not have the skills or resources to navigate digital platforms. This could create a digital divide between those who have access to the metaverse and those who do not.

Infrastructure

The metaverse may require sufficiently advanced technological infrastructures, including high-speed internet, powerful computing systems, and sophisticated software. This could be a barrier to implementation, particularly in countries or areas with poor access to internet.

User Adoption

The success of the metaverse for public services will depend on user adoption. It is important to consider how citizens will engage with the metaverse and what factors might incentivise, motivate, or discourage them from using it.

Cost

The development and maintenance of the metaverse infrastructure could be expensive, which could be a barrier to implementation for some governments or organisations.

Ethics and Regulation

The metaverse raises significant ethical and regulatory questions,

particularly around issues such as digital identity, data ownership, and digital citizenship. It is important to develop clear ethical and regulatory frameworks to ensure that the metaverse is used in a responsible and accountable way.

Training and Education

One of the key challenges associated with establishing metaverse-centric economies is the need for adequate training and education of all stakeholders.

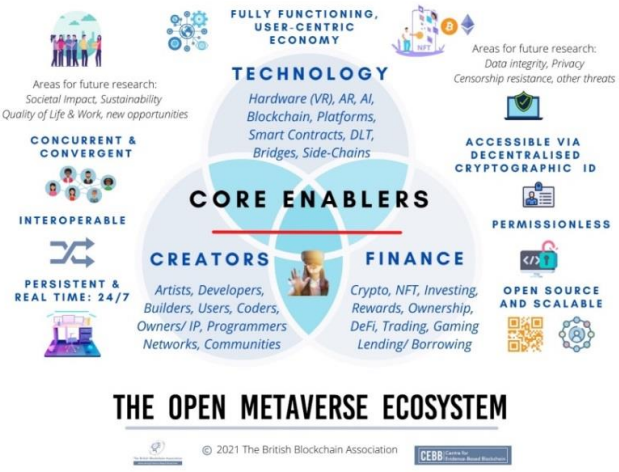


Figure 43: The Open Metaverse, The BBA, 2021[63]

Recommendations

Foster Quadruple Helix Metaverse Ecosystems and Public–Private Partnerships

In order for the metaverse to bring benefits to both citizens and society, close collaboration between the government, academia, and enterprises is necessary as they are the other three players in the "Quadruple Helix."

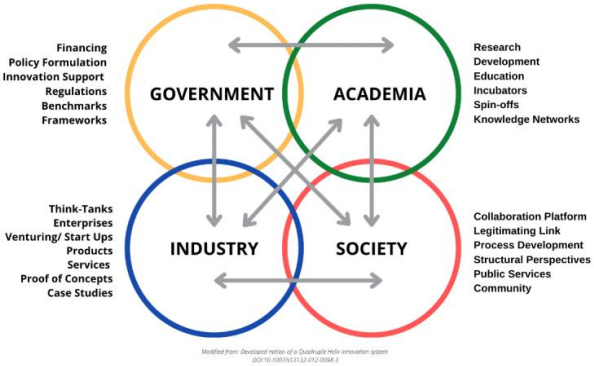


Figure 44: Quadruple Helix Innovation Ecosystems

Devise a National Metaverse Roadmap

All governments should begin to work towards their national metaverse roadmap. A roadmap may take the form of a series of recommendations or a blueprint to devise a 5–10-year national metaverse strategy. When devising such framework, it is paramount to have a futuristic but pragmatic vision of the metaverse. This may be achieved by garnering collaboration with other countries that have already demonstrated practical impact of metaverse applications and use their outcomes to build bespoke standards and benchmarks.

Establish and Nurture Metaverse Economic Zones

Governments and public services should allow metaverse economic zones and metaverse "sandboxes" to build evidence base for metaverse economies, as well as an impetus for future research. The case of Japan can be used as a prototype example.

Appraise the Effectiveness of Metaverse Programmes

As with any public service, it is important to evaluate the effectiveness of metaverse-based services. Metrics such as user satisfaction, accessibility, and efficiency should be tracked and analysed to ensure that the service is meeting its intended goals.

Set Up a National Steering Committee to Spearhead Metaverse Development

Government and public services should take proactive steps to establish a multidisciplinary metaverse think-tank for the advancement of metaverse. This think-tank should utilise emerging evidence to devise consensus among stakeholders and identify any barriers to metaverse adoption.

Identify and Support Metaverse Centres of Excellence

Government should build a national repository of organisations and thought leaders in the metaverse space. All metaverse centres of excellence should be adequately supported, and their work acknowledged.

Incorporate Metaverse in the Postgraduate Curriculum at Colleges and Universities

More than two dozen universities in the world are now offering courses on applied metaverse and the list is growing. Students of today are the CEOs and CTOs of the Web3 metaverse ecosystems of tomorrow. Hence, it is vital that necessary steps should be taken to include metaverse taster sessions, diplomas, master's, and doctorate programmes at all major universities to train a metaverse-savvy future digital workforce.

Evaluate the Social Impact of Metaverse Applications

It is prudent that all metaverse experiments and use cases are regularly evaluated over time to ensure they are safe, effective, and remain credible and fit-for-purpose. Government must ensure that all metaverse funding is evidence-based and achieves the desired impact on end-users. This data should be incorporated into national budgeting processes.

Devise Interoperable Standards and Frameworks

For a thriving metaverse economy, it is crucial to establish open, fair, decentralised, interoperable, and user-friendly standards. The British Blockchain Association is leading the charge in these discussions, collaborating with other standards-setting organisations, and participating in forums like the Metaverse Standards Forum, among others. While regulation is necessary and inevitable, we must strive for fewer bureaucratic obstacles and more opportunities for experimentation and exploration in the metaverse. Overly restrictive policies could stifle innovation and hinder the introduction of new ideas, services, and innovative products.

Explore Use Cases and Initiate Pilot Programmes

Our suggestion is to establish pilot programmes and build systems that explore potential metaverse use cases. We recommend creating a public repository that catalogues all successful metaverse pilot programmes, providing consumers with the opportunity to explore them. Public service employees can leverage the metaverse to conduct virtual meetings, training sessions, and conferences, resulting in cost and time savings, as well as facilitating more frequent and efficient collaboration. Additionally, the metaverse can be utilised to offer virtual public services, such as providing information on government amenities, e-voting, land registration processes, e-residency applications, access to government-held citizen documents, applying for driving licences, seeking real-time virtual assistance from government employees, making it easier for citizens to access theses services thereby increasing end-user satisfaction.

Incorporate Accessibility Features into Project Planning

The metaverse can be designed to include accessibility features such as VR and AR devices specially designed for disabled groups, text-to-speech, closed captioning, and alternative accessibility infrastructure for disabled citizens. This can make it easier for people with disabilities to access metaverse-based public services.

Foster Collaboration between Native Metaverse Organisations (NMOs)

The NMOs can facilitate interoperable collaboration between multidisciplinary metaverse stakeholders including government agencies, enterprises, academia, and society. By providing shared virtual workspaces, these interactions can help to break down physical barriers and silos, improve communication and coordination between agencies, and provide a venue for persistent, dynamic, immersive, and real-time cooperation.

Consider Data Privacy and Cybersecurity Aspects of Metaverse Ecosystems

Like any technology, it is crucial to prioritise data privacy and security when utilising the metaverse for public good. It is essential to implement sufficient safeguards and protocols to ensure the protection of citizens' personal information, assets, identity, and communication.

Involve Citizens in the Design Process

The metaverse offers an opportunity to involve citizens in the design of public services. Citizen feedback can be collected through virtual town halls, shared public spaces, and at dedicated community events. The feedback mechanisms must be put in place to allow for a user-centred and user-driven approach to service delivery in the metaverse, as evidenced by auto-learning avatars in Japan's Metaverse Economic Zones.

Conclusion

The promise of the metaverse for public good presents a new frontier to build socially responsible virtual economies. Metaverse offers a unique opportunity to create a more equitable and accessible web, and a tool for economic development and social progress. With careful planning and development, the metaverse has the potential to revolutionise the way public services are delivered, making them more efficient and effective for citizens. Careful consideration must be given to the potential challenges and risks associated with the metaverse, to ensure that the metaverse is built on evidence-based frameworks, and is safe, secure, and accessible to all. With thoughtful development, metaverse has the potential to transform the way users will interact and participate in a digital economy. By harnessing the power of metaverse for public good and community building, by incorporating accessibility features, and by involving all stakeholders in the design process, the metaverse can help to create more efficient, effective, and user centric Web3 economies.

References

[1] Metaverse Market Statistics: Users, Revenue, and Forecasts. (2022, January 12). Metaverse Ventures. [Online]. Available: https://metav.rs/blog/metaverse-market-statistics-2022-2023/ (accessed: Apr. 07, 2023).

[2] Huawei Technologies Co., Ltd. (2022, July). Metaverse: A Trillion Dollar Opportunity. [Online]. Available: https://www.huawei.com/en/huaweitech/publication/202207/metaverse-trillion-dollar-opportunity (accessed: Apr. 07, 2023).

[3] World Economic Forum. (2023, February 7). Chart: Metaverse Market Growth in the Digital Economy. [Online]. Available: https://www.weforum.org/agenda/2023/02/chart-metaverse-market-growth-digital-economy/ (accessed: Apr. 07, 2023).

[4] The BBA. (2023, March). First in the Metaverse. [Online]. Available: https://britishblockchainassociation.org/wp-content/uploads/2023/03/First-in-Metaverse-2023.png (accessed: Apr. 07, 2023).

[5] E. Shein, "7 Top Technologies for Metaverse Development," CIO, 18-Nov-2022. [Online]. Available: https://www.techtarget.com/searchcio/tip/7-top-technologies-for-metaverse-development. (accessed: Apr. 07, 2023).

[6] "Metaverse Definition & Meaning - Merriam-Webster." https://www.merriam-webster.com/dictionary/metaverse (accessed: Apr. 07, 2023).

[7] "The Metaverse | World Economic Forum." https://www.weforum.org/topics/the-metaverse (accessed: Apr. 07, 2023).

[8] "The State of the Metaverse 2023 | Challenges & Opportunities." https://influencermarketinghub.com/state-of-the-metaverse/ (accessed: Apr. 07, 2023).

[9] "Technology Research and Insights | Zinnov." https://media.zinnov.com/wp-content/uploads/2022/12/metaverse-in-the-public-sector-a-focused-analysis-report.pdf (accessed: Apr. 07, 2023).

[10]https://globetrender.com/2022/12/15/tuvalu-digital-nation-metaverse/ (accessed: Apr. 07, 2023).

[11] The Guardian. (2022, November 17). First digital nation Tuvalu turns to metaverse as rising seas threaten existence. [Video]. Retrieved from https://www.theguardian.com/world/video/2022/nov/17/first-digital-nation-tuvalu-turns-to-metaverse-as-rising-seas-threaten-existence-video (accessed: Apr. 07, 2023).

[12] "Governmemt Enters the Metaverse | Accenture." https://www.accenture.com/us-en/insightsnew/us-federal-government/technology-vision-2022 (accessed: Apr. 07, 2023).

[13] Ministry of Science & ICT, Korea's Digital New Deal 2.0 Action Plan 2022: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=626&searchOpt=ALL&searchTxt= (accessed: Apr. 07, 2023).

[14] "The global metaverse hub: Why South Korea is investing $200M in its metaverse ecosystem." CoinGeek. https://coingeek.com/the-global-metaverse-hub-why-south-korea-is-investing-200m-in-its-metaverse-ecosystem/ (accessed: Apr. 07, 2023).

[15] "South Korea launches metaverse replica of Seoul." Forkast. https://forkast.news/headlines/south-korea-metaverse-capital-city-seoul/ (accessed: Apr. 07, 2023).

[16]T. Maresca, UPI. https://www.upi.com/Top_News/World-News/2023/01/16/Seoul-Metaverse-virtual-platform-launched/6531673859297/. (accessed: Apr. 07, 2023).

[17] WIRED. https://wired.me/technology/saudi-arabias-new-metaverse-will-help-design-500bn-city-irl/ (accessed: Apr. 07, 2023).

[18] CNBC. https://www.cnbc.com/2021/12/31/shanghai-releases-five-year-plans-for-metaverse-development.html(accessed: Apr. 07, 2023).

[19] O. Knight. "Shanghai Plans to Cultivate $52B Metaverse Industry by 2025." CoinDesk: https://www.coindesk.com/business/2022/07/12/shanghai-plans-to-cultivate-52b-metaverse-industry-by-2025/ (accessed Apr. 7, 2023).

[20] "Shanghai to pursue metaverse development as part of China's economic recovery efforts." South China Morning Post. https://www.scmp.com/tech/policy/article/3184781/shanghai-ramp-support-metaverse-development-low-carbon-projects-smart (accessed Apr. 7, 2023).

[21] "Shanghai starts metaverse services at 20 urban spots as part of pilot program - Global Times." Global Times. https://www.globaltimes.cn/page/202301/1283918.shtml (accessed Apr. 7, 2023).

[22] "Analysis: A metaverse with Chinese characteristics is a clean and compliant metaverse." Reuters. https://www.reuters.com/markets/funds/metaverse-with-chinese-characteristics-is-clean-compliant-metaverse-2022-01-25/ (accessed Apr. 7, 2023).

[23] "Saudi National Day 2022 To Be Held In The Metaverse." Tech Magazine. https://techmgzn.com/saudi-national-day-2022-to-be-held-in-the-metaverse/ (accessed Apr. 7, 2023).

[24] Prof Dr Naseem Naqvi MBE [@DrNaseemNaqvi], Twitter, Accessed: Apr. 7, 2023. [Online]. Available: https://twitter.com/DrNaseemNaqvi/status/1573223341510787073

[25] The British Blockchain Association on LinkedIn: https://www.linkedin.com/posts/britishblockchain_queen-queenelizabeth-tribute-activity-6976209947583750145-LB2F?utm_source=share&utm_medium=member_desktop (accessed Apr. 7, 2023).

[26] "Agreement on the creation of the." Fujitsu Global. https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0227-02.html (accessed Apr. 7, 2023).

[27] "Interoperability and the Future of the Metaverse." LeewayHertz - Software Development Company. https://www.leewayhertz.com/metaverse-interoperability/ (accessed Apr. 7, 2023).

[28] J. Crawley. "Japan Digital Ministry to Create DAO for Web3 Exploration." CoinDesk: https://www.coindesk.com/policy/2022/11/03/japanese-digital-ministry-to-create-dao-for-web3-exploration/ (accessed Apr. 7, 2023).

[29] "Dubai Metaverse Strategy - The Official Portal of the UAE Government."

https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-metaverse-strategy (accessed Apr. 7, 2023).
[30] "Dubai International Financial Centre launches new metaverse platform." The National. https://www.thenationalnews.com/business/technology/2023/01/30/dubais-difc-launches-new-metaverse-platform/ (accessed Apr. 7, 2023).
[31] "Dubai World Trade Centre - The Sandbox Announces Dubai VARA - the world's first Regulator in the Metaverse." dwtc.com. https://www.dwtc.com/en/press/the-sandbox-announces-dubai-vara-the-worlds-first-regulator-in-the-metaverse-2022/ (accessed Apr. 7, 2023).
[32] "IEEE Xplore Full-Text PDF:." IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10042106 (accessed Apr. 7, 2023).
[33] "First Metaverse Presidential Speech: Macron Appearance on Decentraland." TechJuice. https://www.techjuice.pk/first-metaverse-presidential-speechmacron-apperance-on-decentraland/ (accessed Apr. 7, 2023).
[34] "A Mayoral First: Orlando." https://news.orlando.org/blog/a-mayoral-first-orlandos-buddy-dyer-gives-address-in-the-metaverse/ (accessed: Apr. 07, 2023).
[35] "16 Best Universities for Metaverse and Web3: Education, Research". https://mpost.io/16-best-universities-for-metaverse-and-web3-education-research-courses/ (accessed: Apr. 07, 2023).
[36] DECENTRALAND, Events: https://events.decentraland.org/event/?id=fbb8513c-74d6-4471-98f1-380a068fac55 (accessed: Apr. 07, 2023).
[37] "Classes in the metaverse": Japan Times. https://www.japantimes.co.jp/news/2023/01/02/national/metaverse-japan-education/ (accessed: Apr. 07, 2023).
[38] "Metaverse Library - How Does Library in Metaverse Work?" https://metaverseofthing.com/business/metaverse-library/ (accessed: Apr. 07, 2023).
[39] "A whole new world: Education meets the metaverse." https://www.brookings.edu/research/a-whole-new-world-education-meets-the-metaverse/ (accessed: Apr. 07, 2023).
[40] The British Blockchain Association on Linkedin: https://www.linkedin.com/posts/britishblockchain_epoka-university-in-the-metaverse-activity-7018979262439292929-dEP0?utm_source=share&utm_medium=member_desktop (accessed Apr. 7, 2023).
[41] "Israeli Metaverse startup saves lives on Earth and heads for Space": Times of Israel. https://www.timesofisrael.com/spotlight/israeli-metaverse-startup-saves-lives-on-earth-and-heads-for-space/ (accessed: Apr. 07, 2023).
[42] Prof Dr Naseem Naqvi MBE [@DrNaseemNaqvi], Twitter, Accessed: Apr. 7, 2023. [Online]. Available: https://twitter.com/DrNaseemNaqvi/status/1582778610695680000?s=20
[43] Business Insider: (accessed Apr. 7, 2023) https://www.businessinsider.com/harvard-students-metaverse-school-reunion-potential-use-vr-tech-2022-6?r=US&IR=T
[44] "Future of justice: Colombia makes history by hosting its first-ever .." Euro News. https://www.euronews.com/next/2023/03/01/future-of-justice-colombia-makes-history-by-hosting-its-first-ever-court-hearing-in-the-me (accessed: Apr. 07, 2023).
[45] Khaleej Times: (accessed: Apr. 07, 2023). https://www.khaleejtimes.com/uae/uaes-first-metaverse-wedding-to-take-place-this-week?amp=1
[46] K. Wright, Cointelegraph: https://cointelegraph.com/public/index.php/authors/keira-wright/amp?page=2 (accessed: Apr. 07, 2023).
[47] Technology Review: (accessed: Apr. 07, 2023). https://www.technologyreview.com/2023/03/15/1069848/taco-bell-metaverse-wedding/amp/
[48] https://propakistani.pk/2023/02/04/islamabad-united-launch-worlds-first-metaverse-in-cricket/ (accessed: Apr. 07, 2023).
[49] "Qatar Airways Steps into the Metaverse with ." Qatar Airways. https://www.qatarairways.com/press-releases/en-WW/215125-qatar-airways-steps-into-the-metaverse-with-qverse-virtual-reality-and-world-s-first-metahuman-cabin-crew (accessed: Apr. 07, 2023).
[50]"India." https://www.airport-technology.com/news/india-bial-launches-metaverse-experience/ (accessed: Apr. 07, 2023).
[51] "Prepare for the metaverse with our ultimate guide | Accenture .." ACCENTURE. https://bankingblog.accenture.com/ultimate-guide-to-banking-in-the-metaverse (accessed: Apr. 07, 2023).
[52] DECENTRALAND, Events: https://events.decentraland.org/event/?id=0c949a7a-7a0e-4a95-a8bb-4b3ca278b920
[53] "Opportunities in the metaverse | JPM." JP Morgan. https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf (accessed: Apr. 07, 2023).
[54] "INTERPOL launches first global police Metaverse." INTERPOL. https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse (accessed: Apr. 07, 2023).
[55] "A vision for a Global Collaboration Village | World Economic Forum." https://www.weforum.org/agenda/2023/01/the-global-collaboration-village-davos-2023/ (accessed: Apr. 07, 2023).
[56] "10 Jobs That Only Exist in the Metaverse." https://www.makeuseof.com/jobs-that-only-exist-in-the-metaverse/ (accessed: Apr. 07, 2023).
[57] "Five ways the metaverse could be revolutionary for people with disabilities": Brunel University. https://www.brunel.ac.uk/news-and-events/news/articles/Five-ways-the-metaverse-could-be-revolutionary-for-people-with-disabilities (accessed: Apr. 07, 2023).
[58] "Ariana Grande to Travis Scott: The Biggest Metaverse Concerts." https://www.mirrorworld.media/lil-nas-x-to-travis-scott-the-biggest-metaverse-concerts/ (accessed: Apr. 07, 2023).
[59] "Decentraland Kicks Off Metaverse Fashion Week 2023." https://www.cryptotimes.io/decentraland-kicks-off-metaverse-fashion-week-2023/ (accessed: Apr. 07, 2023).
[60] Prof Naseem Naqvi MBE on Linkedin: https://www.linkedin.com/posts/naseemnaqvi_art-art-nft-activity-7024833038190563329--hM9?utm_source=share&utm_medium=member_desktop (accessed: Apr. 07, 2023).
[61] Prof Naseem Naqvi MBE on Linkedin: https://www.linkedin.com/posts/naseemnaqvi_metaverse-nft-blockchain-activity-6962471569558224896-cHDo?utm_source=share&utm_medium=member_ios
[62] "The State of the Metaverse 2023 | Challenges & Opportunities." https://influencermarketinghub.com/state-of-the-metaverse/ (accessed: Apr. 07, 2023).
[63] "The Open Metaverse: 3, 7 & 9 | Published by The Journal of The British Blockchain Association" The JBBA. https://jbba.scholasticahq.com/post/1255-the-open-metaverse-3-7-9 (accessed: Apr. 07, 2023).

Competing Interests:
None declared.
Ethical approval:
Not applicable.
Author's contribution:
NN designed and coordinated this research and prepared the manuscript in entirety.
Funding:
None declared.
Acknowledgements:
The author would like to thank the team at the British Blockchain Association's Centre for Evidence-Based Blockchain (CEBB) for their contributions to the data collection in preparation for this article.

THE JBBA

ESSAY

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-1-(2)2023

Tokenomics Beyond 2023: Why Now more than Ever Before

Stylianos Kampakis
Centre for Blockchain Technologies, University College London UCL CBT, UK

Correspondence: stylianos.kampakis@gmail.com
Received: 30 November 2022 **Accepted:** 11 December 2022 **Published:** 16 December 2022

In 2018, I dared to ask the question on the inaugural issue of the Journal of the British Blockchain Association: Why do we need tokenomics[1]?

I was one of the very first to note the importance of token economics, but also the potential that tokenomics brings to revolutionise multiple industries and society.

The innovations behind Ethereum gave rise to the creation of token economies that can align complex incentives. Then many other projects followed. From new Layer 1 solutions, like Solana and Avalanche, to Layer 2s, like Polygon and Optimism, and interoperability blockchains like PolkaDOT and Cosmos.

This has made tokenomics ever more important. What used to be a fringe interest in 2018, has now become a recognised area of expertise.
This is why I thought it would be good to revisit the original article published in 2018. No-one questions the importance of tokenomcis. However, the answer to the question "why do we need tokenomics?", is more complicated than it was four years ago. The rise of areas such as DeFi, NFTs and the metaverse has created a multitude of new opportunities, and challenges, which tokenomics as a field needs to solve.

Tokenomics in 2018

In the original article in 2018, I had identified three types of tokens:

1. Equity tokens
2. Security tokens
3. Utility tokens

NFTs were primarily unheard of back then, and most tokens belonged in the utility token category.

In the original article I had also voiced this opinion:

"*The use of blockchain-based tokens allows the creation of new kinds of economies, completely customisable and adaptive, while at the same time ensuring security and transparency without a central authority.*

There are many possibilities, and in this article, we are going to see three different examples:

1) Improved incentivisation schemes for different agents of an ecosystem.
2) Automatic control of inflation.
3) Automatic reward/punishment of different actions within the ecosystem."

All these things are as true back then, as they are now. However, I think that this list needs to be further expanded and commented upon.

Tokenomics in 2023 and beyond
Revisiting the original discussion

In terms of the first point (improved incentive mechanisms), I think that this is something proven beyond doubt. Tokenomics is an effective mechanism for aligning incentives in ways that traditional economic models cannot. What is surprising in the blockchain space is the multitude and constant discovery of new mechanisms to achieve these objectives. Here are some great examples:

1. Automated market makers
2. Borrowing/lending protocols
3. Yield farming

In terms of inflati on, I hadn't foreseen back then is how of an important problem inflation would be in the current fiat system. Could crypto have solved this problem? At the current level of maturity and volatility, probably not. But could self-adjusting crypto-currencies be the solution to future inflation challenges? It is very likely that the answer is yes.

Artificial intelligence's role in society and the industry is becoming more and more prevalent. Newer generations will take AI as a given. Given the policy fallacies of central banks over the last decade, it's likely that automated and decentralised systems will play a larger role in the global economy. A self-adapting financial system will be more resilient than one based on human policy. The rise of CBDCs might facilitate such a transition. However, this development does not depend only on technological advancements, but also political will.

With regards to the third point (automatic reward/punishment of different actions within the ecosystem), I think the tokenomics community has mostly focused on rewards, with punishment being restricted to mechanisms such as proof-of-stake. This point ties in with the first point of tokenomics being able to create new incentive structures that would not be able to exist otherwise.

The new frontier in tokenomics

In addition to those three points, I would add some more.

A fourth point would be "tokenomics enables the unlocking of latent demand". The best example of this are NFTs in the art world. I mention the art world, because the use of NFTs in areas such as land registries and car ownership is largely a technological improvement over the currently centralised state of the art.

The explosion of the total value of the NFT space, while partially funded by speculation, clearly demonstrated there is "latent demand". The term latent demand is referring to demand for a certain good or service which was unable to express itself unless the invention of a certain technological

innovation.

If there would be one key application of tokenomics to focus on, this would be the best one. The term "latent demand" encapsulates countless use cases in the world of Web3.0. Other great examples of this concept are decentralised exchanges, since they allow trading assets 24/7, across all timezones. Another great example of this is borrowing and lending protocols. Indeed, most of DeFi can be seen as an attempt to unlock latent demand for financial services which is not satisfied by mainstream finance.

A fifth point is around interoperability. Projects like Cosmos and PolkaDOT are focused on bridging together multiple blockchains. The revised tokenomics of Cosmos demonstrate how complex incentives can be used for more than the simple transaction of value. Cosmos' new tokenomics system incentivises (amongst other things) the preservation of security. PolkaDOT's parachain slot auctions incentivise efficient allocation of resources. Both go beyond traditional tokenomics applications.

A sixth point is around interconnectedness with the physical world. The metaverse is a relatively recent development which has been partially fuelled by Facebook's transition to Meta. While the jury's still out as to whether Meta's vision will be successful, this development is a clear transition towards a trend of connecting the physical world with the digital. To that extent, it can be seen as within the same group of technologies like augmented reality. One thing that's clear is that this trend will persist in one form of another, irrespective of whether it can be successful or not.

The new risks in tokenomics

The conversation, up to this point, focused on the positives of tokenomics. However, tokenomics are much needed for another reason. As the blockchain industry grows, it faces unprecedented financial risks which can wreak financial havoc on investors.

There are two excellent examples from recent history. One is the Terra-Luna crash, which spelled financial disaster for many users of the stablecoin. The crash eliminated about $60billion of total value[2].

Another example is the FTX scandal, which wiped out a $30billion empire[3]. A post-mortem indicated that there were many things many things with the primary culprit being that FTX had created a complicated structure, which allowed it to essentially enter overleveraged positions, by priting its own token and using it as collateral.

Therefore, we need to add one more point to the ones outlined above. Tokenomics should test the robustness of a network and inspire consumer and investor confidence. This is what the new field of tokenomics auditing has been designed to do. A tokenomics audit of any of the tokenomics structures above would have prevented these collapses.

Conclusion: So, why do we need tokenomics?

So, why do we need tokenomics in 2023 and beyond?

Here's an updated list:

1. Improved incentivisation mechanisms
2. Automation of real-world financial mechanisms and metrics
3. Unlocking latent demand
4. Interoperability incentives
5. Interconnectdeness with the physical world
6. Ensuring robustness and inspiring investor confidence.

It's clear that this list might be incomplete, since other experts in the area of tokenomics might add more items. However, I can only imagine this list growing over the next few years. The Web3.0 narrative has now been widely adopted with a new wave of entrepreneurs innovating in this area.

This makes tokenomics more important than ever. However, the whole area still has a long way to go until it matures.

On one hand there is progress, with tokenomics becoming more popular as a field. At the time of writing, a google scholar search for the term "tokenomics" returns about 1200 results.

On the other hand, there is a lack of formalisation in the field. A recent development which is assisting with this direction is the development of tokenomics auditing, which has also been discussed in this journal . Also, tools like agent-based modelling can assist in this direction.

One thing that is evident is that this decade will witness a virtuous loop of more Web3.0 projects, more complicated tokenomics designs, more data from past projects to guide the design of new projects, as well as new and more robust tokenomics frameworks.

Therefore, the question "why do we need tokenomics" is at the same time relevant, and contrived, given that tokenomics, as a field, has proven its importance beyond any doubt. In the next few years, asking "why do we need tokenomics" will be like asking "why do we need physics?", or "why do we need the internet?". No-one would take such a question of this type as meaningful, for the fact that both physics and the internet have parts of the fabric of science and society.

So, in a few years, when this question is revisited, the right thing to ask might not be "why do we need tokenomics", but rather "how can we make the most out of tokenomics to build better systems for the economy and society?". And this is a question that will be answered in more clarity over the next few years as the Web3.0 community collectively experiments with new ways of creating and transferring value.

THE JBBA

COMMENTARY

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-1-(4)2023

'Block-Change': Exploring Change Management Principles to Overcome Challenges in Blockchain Adoption

[1]Gintare Geleziunaite, [2]Sean Manion
[1]*Department for International Trade, UK*
[2]*Equideum Health, USA*

Correspondence: stmanion@gmail.com
Received: 21 December 2022 Accepted: 2 January 2023 Published: 1 April 2023

Abstract

Blockchain technology has attracted significant interest and investment over the past decade across multiple industries. While the research and development has been robust and there has been no shortage of attempts at implementation, successful implementations at scale have been somewhat limited. Evaluations of this limited success have often focused solely on the technology or isolated economic assessment of the business use cases. Individual users and the networks they create are another critical component of a successful blockchain implementation at scale. Change management is the approach of preparing, supporting, and guiding a group of people towards an organisational or network goal. This paper looks at change management as a critical component of successfully building a network for scaled adoption and implementation of blockchain use across industries. We explore what makes individuals resistant to change, offer solutions from the established fields of change strategy and change management, and consider how these can be applied to increase success in blockchain adoption and implementation. Crucial elements include identifying principal stakeholder groups and users, asking key questions and gathering input and feedback from these stakeholders, incorporating this information into the governance structure and consensus mechanisms of the blockchain use, demonstrating and describing value of use to the stakeholders, and aligning these components for successful adoption. We end with impactful recommendations for developers, business leaders, administrators, subject matter experts, advisors, and end users to consider to better incorporate successful change management principles into their blockchain projects.

Keywords: *blockchain, distributed ledger, change management, technology, human centered design, adoption, implementation*

JEL Classifications: *G40, G41*

1. Introduction

It is estimated that projects utilising blockchain technology have a failure rate 'as high as 92%' [1] whilst the technology industry average is at 56%. In a nutshell, more than half of technology-powered transformational initiatives will fail to deliver anticipated value. We can't help but pose a question – where do we go wrong and what can we do differently to deliver technology-powered value?

Research suggests that even technology that is effectively closing a market or functionality gap often fails the adoption challenge. Not because people don't need it, but because they choose to resist it anyway. Humans choose to resist change.

There is a wealth of valuable lessons to be learned from previous technological transformations to inform blockchain's adoption journey and how we manage people through this change. People's readiness for the 'block-change' will be a crucial determinant of whether we get to enjoy at least some of the promises of decentralisation, security, and transparency delivered to us by the 'machine for building trust' [2].

This article is aimed at a non-technical audience – the senior leaders, project directors and managers, and product owners who are considering or implementing blockchain technology to transform their organisations and environments. Therefore, we will begin with the definitions:

1. '**Blockchain** is a distributed ledger, or database, shared across a public or private computing network. Each computer node in the network holds a copy of a shared ledger of data events (e.g., financial transactions), so there is no single point of failure. Every piece of information is mathematically encrypted and added as a new "block" to the chain of historical records. Various consensus protocols are used to validate a new block in tandem with other participants before it can be added to the chain. This prevents fraud or double spending without requiring a central authority. The ledger can also be programmed with "smart contracts," a set of conditions recorded on the blockchain, so that transactions automatically trigger when the conditions are met. For example, smart contracts could be used to automate insurance-claim pay-outs.
Blockchain's core advantages are decentralisation, cryptographic security, transparency, and immutability. It allows information to be verified and value to be exchanged without having to rely on a third-party authority, in effect becoming a computationally validated trust layer. Rather than there being a singular form of blockchain, the technology can be configured in multiple ways to meet the objectives and commercial requirements of a particular use case' [3].

2. **Change management** is the process of ensuring that people that are affected by proposed changes are ready, willing, and able to adopt them. Change management plays a crucial role in enabling adoption of the products and outcomes of projects, resulting in the realisation of anticipated benefits. Change

> management deals with the 'people side' of projects, by identifying and removing emotional and capability barriers and resistance to change at both an individual and organisational level.

Every change initiative – technological or not – presents adoption challenges, a key one being 'resistance'. Neuroscience explains that resistance to change isn't a conscious act. Instead, we resist change because of our evolutionary survival instinct and, as humans, we are inherently cautious about change. As soon as we encounter anything new or unexpected, the brain automatically assesses whether it presents a threat to our survival or a potential reward. This deeply rooted process happens at a subconscious level, and in less than a split second — we have no conscious idea that it is happening [4]. Whilst we cannot remove this natural reaction to change, we can certainly manage it by employing change management techniques and processes.

The purpose of this article is to consider common reasons for resistance to change, how those obstacles manifest in blockchain projects (i.e., initiatives to incorporate blockchain solutions into enterprises), and the impact that an effective change management approach could have on the likelihood of successful adoption of blockchain technology.

2. Why do people resist change and more specifically – 'block-change'?

We have already established that blockchain projects' failure rates are high. This, no doubt, can be partially attributed to the fact that the technology is still in its early stages, is subject to the whims of a speculative market in the eyes of the public, and the fact that no digital transformation goes without technical challenges. However, the human side of the transformation – awareness, willingness, capability, and attitudes – presents, arguably, the greatest challenge to both individual projects and the likelihood of the mass adoption of blockchain-powered change.

In the following section, we will undertake a root cause analysis of why people resist change and how these common reasons might manifest specifically in blockchain projects. This analysis is essential in understanding the reasons for resistance and enables the mitigation research outlined in the next section of this article.

Reasons for resistance to change	Implications for the 'block-change'
Lack of vision and excess uncertainty 'If change feels like walking off a cliff blindfolded, then people will reject it. People will often prefer to remain mired in misery than to head toward an unknown. To overcome inertia requires a sense of safety as well as an inspiring vision. Leaders should create certainty of process, with clear, simple steps and timetables' [5]. If there is no clear and compelling vision that is communicated frequently and with authenticity, then the decisions may feel like they are imposed on people suddenly, with no time to prepare for the future. Change will be heavily resisted or even sabotaged from within.	To date, far too many blockchain projects (some of which could be truly disruptive and game changing) are seen to be 'leading with the "how and what" of their initiatives … and every other technology buzz word imaginable, rather than … with "why" and the outcomes' [1]. In short, little thought goes into crafting a compelling vision and story, as well as clearly articulating why everyone involved should care. People are unlikely to embrace change if it is not immediately clear what's in it for them. Blockchain technology truly offers appealing opportunities and benefits to a wide variety of audiences; however, lack of investment in relevant resources and effort to communicate those results in lack of buy-in and interest. For example, Capgemini, a French consultancy, estimates that consumers could save up to $16 billion in banking and insurance fees each year through blockchain-based applications in the US and EU alone [6]. Powerful statements like this, arguing that blockchain could make $16 billion per annum available for more equitable distribution amongst participants, create excellent awareness and a buy-in opportunity, but are underutilised. Another underutilised message is that blockchain stands to make business and government operations more accurate, efficient, secure, and cheap with fewer middlemen. Projects must become better at utilising positive messaging and the benefits of technology to build their visions that people can rally behind.
Reputation and past experiences By definition, 'change is a departure from the past. Those people associated with the last version — the one that didn't work, or the one that's being superseded — are likely to be defensive about it' [5]. And then there is also the we-have-tried-this-before argument. 'The ghosts of the past are always lying-in wait to haunt us. As long as everything is in a steady state, they remain out of sight. But the minute	Blockchain technology represents a major change, via disintermediation, a threat even, to many people and organisations that have created the modern state of things. For the last century, academics and business leaders have been shaping the practice of modern management. 'The main theories, tenets, and behaviours have enabled managers to build corporations, which have largely been hierarchical, insular, and vertically integrated. Blockchain technology could have profound effects on the nature of companies: how they are funded and managed, how they create value, and how they perform basic functions such as marketing, accounting, and incentivizing people. In some cases, software will eliminate the need for many management functions' [7]. Without surprise, the blockchain potential to disrupt organisations in this way is particularly threatening to the management cohort. Especially if it is unclear where they might fit in the new structure and what this means for their power and influence in the organisation. Care must be taken when communicating this message to prevent resistance and even the attempts to sabotage change.

you need cooperation for something new or different, the ghosts spring into action. Old wounds reopen, historic resentments are remembered — sometimes going back many generations' [5].	As for the ghost of the past, blockchain technology is not an exception as it has already made its first appearance in the form of cryptocurrencies and the speculative market that is attached to it. You only get to make a first impression once they say – and the crypto market has not done the technology many favours with stories on fraudulent tactics, plagiarised documents, and fake executive teams appearing across the media outlets on a regular basis. We, of course, know that blockchain is not a synonym for speculation, but efforts are needed to spread this message far and wide. Within this maelstrom of speculative digital assets that explode and implode in value sit several innovative protocols with battle-tested code and proven efficacy.
Accessibility and competence challenges Change that makes people feel inadequate or incompetent will be resisted. People might express scepticism about whether the new solution will work, whether the outcomes of the project will deliver real benefits and improvements, but in reality, they are worried that their skills will no longer be relevant. The result of this is often the unfounded rumours and statements about the change that emerge to discredit it. Project teams are guilty of inflaming this fear through using inaccessible language to not only describe the future state but the technology itself. This is particularly relevant for the technology-driven change projects which use technical jargon, acronyms, etc. extensively. Additionally, research found that 28–58% of people perceive introduction of workplace technology to be an additional burden to their workload and that 9–20% of people see new technology as a job security concern [8].	Applications that utilise blockchain technology will arguably allow organisations to perform better, faster, and smarter decisions 'with the inclusion of everyone in an organisational context such as employees, partners, customers, and other stakeholders' [9]. Whilst this is altogether a positive message, it is easy to see how it could be worry-inducing for impacted stakeholders and employees leading to the emergence of questions, such as: Will my skills and competence, as an employee, still be relevant to my organisation? Will there be a job for me? Will I be able to keep up with demands? Will I have training opportunities? Unless early communication features proactive answers to all the above questions, projects will fail to even begin to bring their stakeholders on a journey and prevent them from trying to discredit the initiative through rumours and other actions. Loudly voiced environmental concerns around blockchain technology (which are too complex and nuanced to cover here) are a potential example of resistance to change hidden behind the banner of sustainability. Not all blockchains are equal and some are more environmentally friendly than others (and that is without analysing the cost versus benefit of blockchains that utilise a higher energy consumption). For example, the Polkadot network, according to the CCRI rating, 'consumes 6.6 times the annual value of electricity used by an average U.S. family' [10]. This is significantly less than a physical 'brick and mortar' business of a similar size. The second largest public blockchain, Ethereum, has as of September 2022 reduced its energy consumption by 99.98% by changing its validation model [11]. McKinsey's report reinforces the argument more generally. 'The misconception that blockchain is not viable at scale due to its energy consumption and transaction speed is a conflation of Bitcoin with blockchain. In reality, the technical configurations are a series of design choices in which the levers on speed (size of block), security (consensus protocol), and storage (number of notaries) can be selected to make most use cases commercially viable. As an example, health records in Estonia are still in databases "off chain" (meaning not stored on blockchain), but blockchain is used to identify, connect, and monitor these health records as well as who can access and alter them' [3]. We touched on the leadership challenges earlier, but it is worth mentioning that this fundamental lack of awareness, understanding, and capability is also true for many leaders that are expected to lead blockchain-powered transformation in their organisations. Let alone the array of emerging technologies that intersect [1].

Organisational culture and behaviours 'Organization's culture comprises an interlocking set of goals, roles, processes, values, communications practices, attitudes and assumptions' [12]. In short, culture is how we do things around here. Building an effective organisational culture is one of the most difficult challenges that leadership will encounter, let alone changing it. To put the complexity of the task into perspective, in 2017 a study by Deloitte found that 87% of organisations cite culture and engagement as one of their top challenges [13]. Any change being implemented in an organisation will be affected by that organisation's culture and might also require for the culture to change in order to enable the adoption of the outputs. The latter is a significant undertaking and should be (though rarely is) recognised as such and managed carefully.	The promises of blockchain – decentralisation, transparency, accountability, and greater prosperity for all – is more challenging to the status quo of organisational cultures than we may think. It's arguably an anathema to learned human behaviour and norms. And so new behaviours must be introduced and fostered – and that takes desire, effort, and resource. One of the greatest challenges to existing cultures in many organisations is that blockchain represents the emergence of cross-organisational collaboration and 'coopetition'. This requires a total mentality shift because the only way benefits are realised is by working in a consortium setting, often with your fiercest competitors. It is difficult to manage a project in an organisation, let alone one that spans across different organisations. All the usual things a project would do, such as aligning stakeholder interests, onboarding leadership, identifying problem statements and scoping, are more challenging due to multiple agendas and cultures. The likelihood of successful completion relies on making partnerships strong enough to outlive the initiative itself – and that requires a significant shift in the culture and behaviours across those organisations. Including the need to build a common set of values of how we do things around here together. Blockchain presents unprecedented opportunities to affect behavioural change in organisations due to its incentivisation capability. Unfortunately, behavioural change initiatives don't yield instant results, and so are not always perceived as worthy of investment of time and effort. We are yet to see many organisations use blockchain for the purpose of internal organisational development, but this may not be far off.

3. Managing 'block-change'

McKinsey is adamant that '70% of digital transformation initiatives fail to achieve their goals, largely due to resistance to change' [14] and lack of change management efforts. The goal of change management is to ensure that every stakeholder affected by the change is ready, willing, and able to excel in the new ways of working.

In the previous section of this article, we have identified some of the reasons why blockchain-powered change initiatives might be resisted, and in the next section, we will explore what projects need to consider and implement to overcome the resistance to change.

3.1 Vision and leadership

We have established the importance of having a clear vision for the initiative that leadership lives by and that everyone can get behind. A clear vision provides a direction for the business and helps everyone in the organisation make the right decisions. It also acts as a motivator to complete difficult tasks and inspires innovative action to achieve the desired end goal.

It is equally as important to be able to bring that vision to life through a story that is centred around what value the technology will add to the end users and stakeholders' lives.

In the case of blockchain technology, it 'holds the potential to decrease transaction costs, improve privacy and redesign social interactions' [15], amongst other positive outcomes. And whilst there is certainly a positive what's in it for me story to tell, the challenge is having suitably skilled leadership that is able to tell that story in a compelling way. Therefore, it is argued that projects should allocate sufficient time and resources to develop a robust vision and case for change, closely follow change comms best practice principles and invest heavily in preparing the leadership team for the change leadership work.

3.2 Accessibility and competence

To be considered accessible, the technology must be perceived as having a positive risk versus usefulness ratio as well as medium to low ease of use. In fact, ease of understanding and using the technology is quoted as the greatest barrier to adoption [15]. Esoteric terms and jargon used by technical teams, with little importance placed on diversifying these teams to include professionals equipped to decipher the messaging and making it more appealing to wider stakeholder groups, remain an issue. The view that the technology transformation is something that can and should be managed by tech teams alone must be eradicated.

To further remove technology accessibility and competence barriers, projects should consider:

- Including education initiatives as part of every project (for the stakeholders and the end users),
- Incorporating human-centred design involving stakeholder representatives whenever possible, and
- Building and utilising internal networks of innovators and early adopters (or change champions) that would facilitate the onboarding of the critical mass required.

The diffusion theory developed by E.M. Rogers in the 1960s [16] explicitly models the dynamic process of technology adoption every individual will pass through as part of a social system. Diffusion theory distinguishes human stereotypes (Adopter Types) by their innovativeness. The first to adopt are the 'Innovators' and they serve as gatekeepers for a technology's diffusion and inspire the 'Early Adopters', who are often the local opinion

leaders. Then the 'Early Majority' follows. The advantage of building and utilising these internal networks is due to these individuals already having trust across the organisation which is difficult to build at pace for the project team.

Feeling competent and in possession of required knowledge, capability, and skills to perform post-transition is another key enabler of increased adoption and likelihood of the use of the technology. Particular attention must be reserved for the learning needs' analysis and crafting learning material that is suitable for the needs of all segments of the audience. Although we are focusing on technological transformation, the learning needs extend beyond the direct technical capability and will include other skills, attitudes, and behaviours.

3.3 Culture and behaviours

The most desirable change-ready organisational culture traits (which also happen to be the most difficult to achieve for any organisation) are organisational trust, desire for experimentation, and uncertainty tolerance. These traits are crucially important for any organisation that is looking to embark on blockchain-powered transformation. It might feel counterintuitive, but the development of technological transformation should start with the development of relevant values and culture in the organisation. This will enable the users to trust that system aligns with their values and ensure use of the network.

Colonel John Boyd, USAF, noted that organisations should focus on 'People, ideas, and things, in that order', and this holds true with blockchain. The network of users' needs to have buy-in on the shared governance that is built into any particular blockchain configuration [17]. The sweet spot for an effective blockchain use is where the technology and business case overlap with this network of users. Having a 'minimally viable network' of users is critical for the successful implementation of any blockchain use case. Without the network of users, any application of blockchain becomes an academic exercise [18].

4. Conclusion

It is argued that in the short term, blockchain technology will predominantly create value by reducing costs before creating transformative business models [3]. Mass adoption of the internet has set a valid precedent for this thinking; because whilst the potential of the internet was prophesied many decades before, it didn't become mainstream until the 1990s. Web 3.0, powered by blockchain technology, is arguably on a similar path. It can also be argued that in both instances – it is not the technology readiness that is responsible for the prolonged route to mass adoption, but rather the mentality shift that is required to prepare us and our stakeholders for the commercial and organisational disruption that this transformation will entail.

In this article, we have explored the common adoption and people change challenges relevant to blockchain-powered transformation (or 'block-change'), as well as ways for overcoming them. Fundamentally, it all boils down to the fact that there is no such thing as change without emotion. Organisational (even industrial) change happens at an individual level and affects us all differently. To successfully manage the change at hand, we must be able to view it from the angle of each stakeholder group and tailor the change to make it as easy and appealing as possible for all. Finally, we must also remember that we are not starting from a clean slate either – taking into account organisation's history, culture, and norms and how they fit with the proposed transformation is the first step in a change management journey.

There are effective frameworks to help us manage the human response to change, but there is no one-size-fits-all approach. To manage change effectively significant commitment and effort are required. The upside, however, is successful adoption of the technology and the ability to realise the business value and benefits offered by it.

5. Recommendations

- Look to broader industry and cross-industry consortia and partnerships for opportunities for transformational change incorporating business model innovation.
- Begin the development of technological transformation with the development of relevant values and culture in the organisation to ensure that the change is sustained.
- Assess your project's roadmap recognising that the technology readiness is only one of many aspects required for successful adoption.
- Resource the project with non-technical professionals equipped to implement change management frameworks, decipher the technical jargon, and communicate effectively to help you manage the human response to change.
- Clearly articulate the case for and benefits of your project. Successful projects lead with the 'why' and not 'what' and appeal to both logic and emotion.
- Identify people's mentality, capability, and cultural shifts that will be required to prepare your stakeholders for the commercial and organisational disruption that technological transformation will entail.
- Deliver education on technical and non-technical aspects of blockchain to various stakeholders to help them better understand the opportunities and challenges the technology brings and how it compares with existing options.

6. Further research: blockchain and organisational culture development

The scope of this article is limited to managing 'block-change' effectively. However, there is an undeniable link between effective organisational culture and the impact it has on our efforts to land change. In earlier sections, we have explored the most important traits of effective organisational cultures, and the authors strongly believe that further research is required to explore how blockchain technology could facilitate the development of these crucial traits in organisations – in particular, and somewhat paradoxically given a central thrust of the technologies promise – trust.

We have already established that building and maintaining trust within organisations is critical. There is a clear link between trust and corporate performance. 'If people trust each other and their leaders, they'll be able to work through disagreements. They'll take smarter risks. They'll work harder, stay with the company longer, contribute better ideas, and dig deeper than anyone has a right to ask' [19].

Blockchain technology carries the promise of transparency, which is a key enabler of trust, as well as a mechanism to motivate and reward the behaviours to build this crucial trait in organisations. Operant Conditioning theory developed by B. F. Skinner in the 1930s [20] proved that providing a reward for adopting targeted behaviours is the most effective learning approach. And now we have a technology with the promise to implement this at scale. The impact on Organisational Culture is a key outcome of the digital era and Organisational Culture development should be firmly considered as an early non-technical use case of blockchain technology.

References

[1] D. A. Disparte, "Why enterprise blockchain projects fail." Forbes. [online]. *Available at: https://www.forbes.com/sites/dantedisparte/2019/05/20/why-enterprise-blockchain-projects-fail/?sh=681e814a4b96 [Accessed 14 Dec. 2022].*

[2] The Economist, "The trust machine," The Economist, 2015. [online]. Available at: https://www.economist.com/leaders/2015/10/31/the-trust-machine [Accessed 14 Dec. 2022].
[3] McKinsey & Company, "Blockchain beyond the hype: What is the strategic business value?" [online]. Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value. [Accessed 14 Dec. 2022].
[4] G. Freitas, PeopleTalk Online, "Neuroscience behind why employees resist change," 2019 [online]. Available at: https://peopletalkonline.ca/organizational-change-the-neuroscience-behind-why-we-resist-change/ [Accessed 14 Dec. 2022].
[5] R. M. Kanter, "Ten reasons people resist change," Harvard Business Review, 2012. [online]. Available at: https://hbr.org/2012/09/ten-reasons-people-resist-chang. [Accessed 14 Dec. 2022].
[6] Capgemini UK, "Consumers set to save up to sixteen billion dollars on banking and insurance fees thanks to blockchain-based smart contracts," [online]. Available at: https://www.capgemini.com/gb-en/news/press-releases/consumers-set-to-save-up-to-sixteen-billion-dollars-on-banking-and-insurance-fees-thanks-to/ [Accessed 14 Dec. 2022].
[7] Cognitive World, "Digital transformation debts post-Covid-19," n.d. [online]. Available at: https://cognitiveworld.com/articles/blockchain-organizational-culture-part-i [Accessed 14 Dec. 2022].
[8] HR Magazine, "HR Magazine - Technology increasing stress at work," n.d. [online]. Available at: https://www.hrmagazine.co.uk/content/news/technology-increasing-stress-at-work) [Accessed 14 Dec. 2022].
[9] Baslangic Noktasi, "How will blockchain reshape organizational culture on the edge of future of work?" 2019 [online]. Available at: https://baslangicnoktasi.org/en/how-will-blockchain-reshape-organizational-culture-on-the-edge-of-future-of-work/. [Accessed 14 Dec. 2022].
[10] Techtelegraph, "Polkadot electricity consumption is less than solana, bitcoin, and ethereum," 17 Feb. 2022. [online]. Available at: https://techtelegraph.co.uk/polkadot-electricity-consumption-is-less-than-solana-bitcoin-and-ethereum/ [Accessed 14 Dec. 2022].
[11] E. Kapengut and B. Mizrach, "An event study of the ethereum transition to proof-of-stake." arXiv:2210.13655 [q-fin.TR]. [online]. https://doi.org/10.48550/arXiv.2210.13655 [Accessed 20 Dec. 2022].
[12] S. Denning, "How do you change an organizational culture?" Forbes, 12 Nov. 2012. [online]. Available at: https://www.forbes.com/sites/stevedenning/2011/07/23/how-do-you-change-an-organizational-culture/ [Accessed 14 Dec. 2022].
[13] J. Flynn and A. H. Mazor, "The employee experience: Culture, engagement, and beyond," Deloitte Insights, 2017. [online]. Available at: https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2017/improving-the-employee-experience-culture-engagement.html [Accessed 14 Dec. 2022].
[14] B. Ewenstein, W. Smith, and A. Sologar, "Changing change management." McKinsey & Company, 2015. [online]. Available at: https://www.mckinsey.com/featured-insights/leadership/changing-change-management [Accessed 14 Dec. 2022].
[15] F. Knauer and A. Mann, "What is in It for me? Identifying drivers of blockchain acceptance among German consumers," The Journal of the British Blockchain Association, vol. 3, no. 1, pp. 1–16, 2020, doi:10.31585/jbba-3-1-(1)2020.
[16] E. M. Rogers, "Diffusion of preventive innovations," Addictive Behaviors, vol. 27, no. 3 6, pp. 989–993, 2003, doi:10.1016/s0306-4603(02)00300-3.
[17] S. Manion and Y. Bizouati-Kennedy, Blockchain for Medical Research: Accelerating Trust in Healthcare. CRC Press, 2020. ISBN: 0367347466
[18] J. Bass, "The truth about blockchain and its application to health care." Healthcare Financial Management Association, 28 Jan. 2019. [online]. Available at: https://www.hfma.org/topics/hfm/2019/february/63125.html [Accessed 20 Dec. 2022].
[19] R. M. Galford and A. S. Drapeau, "The Enemies of Trust," Harvard Business Review, 2003. [online]. Available at: https://hbr.org/2003/02/the-enemies-of-trust [Accessed 14 Dec. 2022].
[20] J. E. R. Staddon and D. T. Cerutti, "Operant conditioning," Annual Review of Psychology, vol. 54, no. 1, pp. 115–144, 2003. [online], doi:10.1146/annurev.psych.54.101601.145124.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Not applicable.

Funding:
None declared.

Acknowledgements:
The authors would like to acknowledge Dr. Pierre Vigilance, Heather Flannery, Doug Bulleit, Dr. Verena Kallhoff, Dr. Joseph Wood, and Dr. Tiffany Gray for their contributions to the discussion from which this paper developed.

CONFERENCE PROCEEDINGS

5th Blockchain International Scientific Conference 18 March 2023, ISC2023, UK

1. A Design For A Blockchain-Enabled Platform For Carbon Accounting, Reporting And Financing For The Construction Industry

George Blumberg, *Oxford Brookes University, UK*
Category: Oral Presentation

Abstract

This paper presents the outline design for a system based on blockchain technology that has the potential to enable a range of services vital for the trading of carbon emission tokens for the construction sector. The assumption taken in this study is that governments will follow the approach taken for the energy generation industry and impose an emissions trading scheme (ETS), such as a modified Cap & Trade, on construction works. As these are project-based activities with defined stages, ETS payments would be levied at critical points of the building's life cycle, for instance, when applying for planning and building permission, when licensing for habitation and before demolition. If implemented correctly, this electronic marketplace would provide enable funnelling money from those polluting to those who are able to extract and sequester C02 directly from the atmosphere. Such a system would require international collaboration on critical issues, such as a standard measurement protocol, reporting conventions, and tax rates. Although Decentralized Finance (DeFi) protocols are still in the process of development and testing, they could one day help provide useful solutions in distributing the ETS payments throughout the life cycle of the building. On-chain certification of building compliance is also envisioned in this system.

Keywords: *Construction projects, Decentralized Finance, Emissions Trading Scheme, carbon tokens*

2. Designing and Implementing a Blockchain-based Platform for the Exchange of Peer-to-Peer Energy Trading and Modelling Vehicle-to-Grid(V2G) Residential Community

Philip Debrah & M. Saraee, *School of Science, Engineering & Environment, University of Salford, UK*
M Babaie, *University of Leeds, UK*
Category: Oral Presentation

Abstract

The expansion of renewable energy on the national grid has been a struggle throughout the past decade. Rooftop solar photovoltaics (PV) and electric vehicle to Grid (V2G) can function as either load or distributed energy sources. Consequently, presumers can join in a Transactive energy network featuring peer-to-peer (P2P) exchange of excess electricity to enhance the grid load balancing and harmonic filtering performance. The key challenge is keeping track of these transactions and compensating supposing parties. The distributed and unchangeable characteristics of blockchain technology could be utilised to accelerate the ongoing transition to more decentralised and digital energy systems and alleviate some of the challenges the energy sector is now facing.

This report presents an experimental design and implementation of a Peer-to-peer blockchain network to exchange electricity energy among participants based on the Ethereum open-source application called Solar Chain App. This demonstration project simulates the P2P Network of the electricity distribution network. A project consists of a primary network and user nodes (user nodes have homeowners and EVs). Homeowners with solar and electric vehicles Participants, assets, and transactions required to establish the blockchain-based network for tracking Buyer and seller output exchanges are described, and the smart contract, use cases, and implementation. The main purpose is to design a p2p platform that maximize renewable energy Usage and minimize the daily cost of household electricity consumption.

Keywords: *Blockchain, Ethereum, Peer-to-peer trading, Vehicle to Grid, Solar PV, Grid, Smart Contract*

3. Automation in Blockchain-based Dispute Resolution: The Rise of New Standards of Justice

Sara Hourani, *Middlesex University London, UK*

Abstract

Different projects have integrated automation in the blockchain-based dispute resolution procedures and have adopted different designs for automation in the process. To illustrate, the Kleros blockchain-based dispute resolution procedure has adopted automation at every stage of the procedure. Another example is the CodeLegit blockchain-based arbitration procedure that clarifies at what stages of the procedure automation can be used. Automation in the arbitration procedure design has also been adopted by the government-backed UKJT Digital Dispute Resolution Rules. This paper's research question therefore queries the extent to which automation is incorporated in the design of current blockchain-based/smart contract dispute resolution systems, and how automation can be embraced in these procedures to comply with fairness and equity standards that are currently found in traditional private dispute resolution procedures, such as arbitration. The paper tries to explore whether the international business community is moving towards embracing a new conception of procedural fairness. Part one of the paper focuses on a comparative analysis of the use of automation and new procedural characteristics in the blockchain dispute resolution platforms chosen for this study. Part two carries out an analysis of the compatibility of such automation and characteristics with the law on arbitration in different legal systems, and assesses the extent to which such systems are embracing a novel approach towards procedural fairness.

Keywords: *Construction projects, Decentralized Finance, Emissions Trading Scheme, carbon tokens*

4. The Four Types of Stablecoins: An Economic Assessment

M. Hafner, M. Henriques Pereira, J. Beccuti, H. Dietl, *University of Zurich, Center for Cryptoeconomics, and Informal Systems, Switzerland*
Category: Oral Presentation

Abstract

Stablecoins are a class of cryptoassets designed to provide stability in an otherwise highly volatile market. They are designed so that their price is stable with respect to a reference point (e.g., the U.S. dollar). From the hundreds of stablecoins some have succeeded and some have failed. In this paper we categorize the wide variety of stablecoin designs along two dimensions: value source and issuance policy. Value source describes whether the value is backed by an external (e.g., Dai or UDSC) or internal value (e.g., sUSD or UST). Issuance policy describes whether projects pool collateral and issue stablecoins centrally (e.g., USDC and UST) or use collateralized debt positions and issue stablecoins decentralized (e.g., Dai or sUSD). This categorization results in four generic types of stabelcoins. We run agent-based simulations to identify the economic advantages and disadvantages of each type of stablecoin from the perspective of all stakeholders. Finally, we discuss the resulting tradeoffs and explain the main policy implications for managers, investors, traders, issuers and regulators.

Keywords: *cryptoassets, fixed exchange rates, stablecoins, financial technology*
JEL Classification: *F31, G10, G14, G15, G23*

5. Public Sector Audits: Digital Tools to Improve Effectiveness and Efficiency

Carlos Alberto, *The Supreme Audit Institution of Angola*
Category: Oral Presentation

Abstract

Angola is an emerging economy with enormous growth potential. The public sector must be coordinated, efficient and effective. Only then can it meet the challenges facing the country, and in so doing improve the quality of life of citizens. Audits are an essential part of public administration because they help governments to make improvements in their actions, ensure accountability, demonstrate transparency and promote development. The Supreme Audit Institution of Angola (SAI/ Tribunal de Contas) faces complex challenges, both internally and externally. To meet these challenges, the SAI has been implementing new ways of working. For these reasons, various possibilities offered by new technologies such as Blockchain and Artiticial Intellgience are explored in order to improve the SAIs effectiveness and efficiency. Case studies of Courts that have successfully created innovative digital tools are brought to light, namely the Internet Courts in China (Hangzhou, Beijing and Guangzhou) and the Supreme Audit Institution of Brazil. Therefore, a holistic digital transformation strategy is proposed to the Angolan SAI, which involves people, processes and culture. An action research approach is used with a strongfocus on reputable peer-reviewed academic journals and books.

Keywords: *blockchain, artificial intelligence, public sector, audit, digital transformation*

6. An Approach to the Liquidity Risk and Liquidity Bootstrapping Problem of Lending Platforms

Benedetto Biondi, Gidon Katten, Michelangelo Riccobene, Alberto Arrigoni, Matthias Hafner, Romain de Luze, Nicolas Greber, Juan Beccuti
Center for Cryptoeconomics, Switzerland
Folks Finance, Italy
Category: Oral Presentation

Abstract
Previous literature suggests that decentralized finance (DeFi) lending platforms' liquidity risk is closely related to the concentration of liquidity positions. In addition, empirical evidence shows that liquidity concentration is especially high in the early stages of lending platforms. As a result, new lending platforms face a significant liquidity risk that has not been investigated so far. This paper closes this gap by investigating liquidity risk from the perspective of a new lending platform. We do this by describing the use case of Folks Finance in three steps: First, we describe the liquidity risk the lending protocol faces using platform economics. Second, we theoretically assess the efficiency of different liquidity risk measurements. Third, we use simulations to investigate how a reward mechanism can reduce liquidity risk. We show that, due to positive externalities, the liquidity risk is more pronounced for a new lending platform than for an incumbent protocol. In addition, we find that the Herfindahl-Hirschman Index (HHI) outperformed other liquidity risk measurements. Finally, our simulation shows that if rewards are sufficient but not too large, a program that incentivizes borrowers to lock their assets can reduce liquidity risk and increase liquidity bootstrapping. Several conclusions are drawn from the case study: First, new lending platforms should be particularly cautious regarding liquidity risk. Second, lending protocols should use HHI instead other concentration measurements when calibrating their parameters. And lastly, rewards can be used to bootstrap liquidity and incentivize liquidity holdings but should not be overused.
Keywords: *Defi, Lending Platform, Liquidity Pools, Platform Economics, Liquidity Risk*
JEL Classification: *C63, D47, G10, L10*

7. Creating, Analysing and Maintaining Tokenomics Using Algebraic Methods

Dr. Olexandr Letychevskyi, *LitSoft Private Enterprise (Ukrainian Blockchain Association), Ukraine*
Category: Oral Presentation

Abstract
Tokenomics stability and smart contract security are two issues inherent in any cryptocurrency project. Both the investor and the creator of the project are concerned about the problems of equilibrium in the token economy, resistance to external stimuli and the liquidity of the token. Projects often turn into financial pyramids when it is impossible to assess token evolution in dynamics. We present our experience in the creation, maintenance and analysis of tokenomics projects over the past year using algebraic technologies. The presentation discusses projects for the Internet of Things, financial services and education. The practices of token circulation planning and the interaction of tokenomics subjects with the use of modelling are considered. We used our Tokenomics Constructor, which allows a user to create an initial tokenomics project in the generally accepted terms of crypto projects. A project is automatically converted into algebraic specifications that are already used by specialised algebraic programmes. These programmes construct appropriate charts and examine the properties defined by the project author and the classical properties of equilibrium and soundness. When studying the property, appropriate scenarios of desirable or undesirable behaviour of the token are built. Classification models and neural networks based on data from crypto exchanges and statistics on changes in the liquidity of known cryptocurrencies are used to assess changes in token liquidity. As a result of the analysis, we used the methods of tokenomics correction to automatically create a draft of secure smart contract that implements the researched tokenomics.
Keywords: *smart contract, algebraic modelling, token economy, economical equilibrium, formal methods, neuron networks*
JEL Classification: *C680*

8. Work for Decentralised Autonomous Organisation: What Empirical Labour Economics Can Tell Us about the Decentralised Digital Workforce?

Nataliya Ilyushina, *RMIT University, Australia*
Category: Oral Presentation

Abstract
A decentralised autonomous organisation (DAO) is a new type of digitally native organisation with a membership base that has been rapidly growing throughout 2022. A new organisational structure also leads to a new way labour is organised, hired, demanded and supplied. There are also some differences in human capital accumulation and employee decision-making. These issues fall in the domain of labour economics. Existing theories of labour economics are tested on conventional labour market data. However, DAO work is not identical to the traditional post-industrial labour market employer-employee relationship. It can be described as a hybrid of ownership, volunteering, freelancing and conventional employment in different proportions for different people. Whether those differences change how the labour market operates in DAOs needs to be examined. To understand this, we need more information on DAO workers, specifically labour and socio-economic survey data, which currently does not exist. This paper identifies the need for a large-scale survey of DAO workers, discusses the motivation and challenges of data collection

specific to DAOs and some important labour economic policy questions that DAOs might face in the near future that rely on empirical data. Next, the paper critically reviews and summarises the existing small-scale data on work for DAO parameters. Lastly, the article outlines what empirical data needs to be collected and what analysis needs to be done next to inform the emerging research on DAO labour. Overall, the paper aims to set out the way forward for the applied labour economic analysis of DAO labour.

Keywords: *decentralised autonomous organisation, blockchain, labour market, labour economics, data, survey*

JEL Classification: *J21, J22, J23, J24, J46, J49, C83*

9. Value Creation Through Mutualism: Delivering On The Promise Of Enterprise Blockchain

Melissa Appleyard and Kristi Yuthas, *Portland State University, USA*
Category: Oral Presentation

Abstract

Blockchain-based collaboration can be viewed along a continuum that begins with cooperation and moves toward mutualism. In third-party blockchain solutions, participants cooperate by automating and streamlining processes and sharing data. In blockchain consortia, participants become interdependent through joint development and governance of shared networks. In the presence of mutualism, participants deepen these interdependent relationships and develop new ways to create and capture value, possibly leading to new business models. Mutualism in collaborations can take the form of horizontal integration of firms within an industry or vertical integration through customer-supplier relationships, often incorporating industry 4.0 technologies including IoT devices, big data analytics, and artificial intelligence. These collaborations can generate leaps in value not possible with traditional, arm's-length relationships. In this paper, we provide in-depth studies of horizontal and vertical consortia that have used mutualism to capitalize on blockchain technology. We provide specific insights into: 1) how participating organizations have developed new value streams and their source and magnitude; 2) how value is captured within a network of collaborators and across the broader ecosystem; and 3) what new business models have been created, and who has driven and benefitted from their deployment. Through our analysis of existing and potential instances of mutualism, we demonstrate how the strategic integration of blockchain can provide value far beyond what can be achieved by traditional projects that have targeted process frictions and other operational problems.

Keywords: *enterprise blockchain, strategy, interdependence, mutualism, collaboration*

JEL Classification: *O03, M15, L86*

10. The Use of Blockchain Technology in the Scientific Research Workflow

Richard E. Shute, *Curlew Research, Woburn Sands, UK*
Category: Oral Presentation

Abstract

The International Union of Pure and Applied Chemistry (IUPAC) is the world authority on chemical nomenclature, terminology, standardized methods for measurement, atomic weights and many other critically-evaluated data. IUPAC also develops and maintains recommendations that create a common language for the global chemistry community. In 2021, IUPAC identified Blockchain Technology as one of its 10 emerging technologies in chemistry with the greatest capacity to open new opportunities in chemistry and beyond. As part of the generation and development of awareness of Blockchain Technology across the global chemical and scientific communities, IUPAC established a team to research how the technology was being applied along the scientific workflow. Beginning in 2020 the group started interviewing experts around the world with the objective of creating a white paper on the topic; this paper will be published in 2023 in Pure and Applied Chemistry. From the interviews and the team's own experience, they found that Blockchain Technology is indeed being used in almost all the steps in the scientific research workflow - from hypothesis development through to publication - by commercial organizations as well as non-profits, and across all market sectors, even governments. For example, the U.S Department of Health and Human Services (HHS) uses blockchain technology in a pilot program, the Grant-recipient Digital Dossier (GDD), to manage their grant program more efficiently. This presentation will summarize the findings, discuss the pros/cons of the technology, and provide a glimpse of how the technology is impacting the future of scientific research.

11. 'Block-Change': Exploring Change Management Principles to Overcome Challenges in Blockchain Adoption

Gintare Geleziunaite, *Department for International Trade, UK* and Sean Manion, *Equideum Health, USA*
Category: Oral Presentation

Blockchain technology has attracted significant interest and investment over the past decade across multiple industries. While the research & development has been robust and there has been no shortage of attempts at implementation, successful implementations at scale have been somewhat limited. Evaluations of this limited success have often focused solely on the technology or isolated economic assessment of the business use cases. Individual users and the networks they create are another critical component of a successful blockchain implementation at

scale. Change management is the approach of preparing, supporting, and guiding a group of people towards an organisational or network goal. This paper looks at change management as a critical component of successfully building a network for scaled adoption and implementation of blockchain use across industries. We explore what makes individuals resistant to change, offer solutions from the established fields of change strategy and change management, and consider how these can be applied to increase success in blockchain adoption and implementation. Crucial elements include identifying principal stakeholder groups and users, asking key questions and gathering input and feedback from these stakeholders, incorporating this information into the governance structure and consensus mechanisms of the blockchain use, demonstrating and describing value of use to the stakeholders, and aligning these components for successful adoption. We end with impactful recommendations for developers, business leaders, administrators, subject matter experts, advisors, and end users to consider to better incorporate successful change management principles into their blockchain projects.

12. How NFTs can promote the UN Sustainable Development Goals

Kristi Yuthas, *The School of Business, Portland State University, USA*
Category: Oral Presentation

Abstract

NFTs, which in essence are certificates of authenticity that can be programmed to adapt to relevant conditions, have potential that extend far beyond speculative investment and entertainment. Four key capabilities of NFTs include: establishing ownership, proving evidence of identity, regulating access, and tracking the history of transactions. As a result, they are uniquely suited for use in addressing the world's most pressing challenges. For example, they can be useful in demonstrating property ownership, establishing citizenship status, ensuring proper distribution of resources, and establishing financial trustworthiness.

The United Nations' Sustainable Development Goals (SDGs) identify 17 critical goals relating to the most significant global challenges, which include poverty, health, security, and climate. The goals fall into four categories: society, planet, economy and governance. NFTs can be used as tools to promote the goals in each category.

This paper develops a framework that identifies potential and existing use cases in the four SDG categories that employ NFT capabilities to achieve goals. The use cases are identified through typical internet searches of NFT applications and NFT taxonomies that provide nuanced understanding of the potential of these tools. Building upon this knowledge and an understanding of the current approaches used by INGOs to address these issues, we provide examples of ways NFTs could potentially be employed.

The framework can form the foundation for future academic research on the potential of NFTs. And it can be a source of information and innovation for nonprofits, governmental agencies, and companies that seek to contribute to social change.

13. A Review of Upgradable Smart Contract Patterns based on OpenZeppelin Technique

Shaima AL Amri, Dr Aniello Leonardo, Prof Sassone Vladimiro, *University of Southampton, UK*
Category: Oral Presentation

Abstract

The Ethereum blockchain is one of the main public platforms to run smart contracts and enable decentralised applications. Since data stored in a blockchain is considered immutable, smart contracts deployed in Ethereum are regarded as tamper-proof and therefore offer strong protection against attacks aiming at tinkering with the execution flow of an application. Yet, like any other software, a smart contract needs to be maintained over time to fix bugs or add new features. Deploying every updated version as a brand-new smart contract in Ethereum leads to problems such as migrating the contract state from the old version and enabling clients to point to the new version in a timely fashion.

The OpenZeppelin framework addresses this limitation by providing libraries that enable the deployment of upgradeable smart contracts. This is achieved by relying on proxies that act as intermediaries between clients and smart contracts, allowing the latter to be updated transparently.

In this paper, we present the upgradeable smart contract patterns supported by OpenZeppelin and compare them in terms of security, cost, and performance. To show this paradigm's prevalence in Ethereum, we also analyse the usage of OpenZeppelin upgradeable smart contracts over the last four years.

Keywords: *Smart Contract, Immutability, Proxy, Upgradeable, Patterns, OpenZeppelin.*

CEBB Centre for Evidence-Based Blockchain

The British Blockchain Association
Advocating Evidence Based Blockchain

BLOCKCHAIN ASSOCIATIONS FORUM

3RD ANNUAL BAF MEMBER SUMMIT

(VENUE: BBA METAVERSE HEADQUARTERS)

#BAF2023

20 SEPTEMBER 2023

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

THE BBA JOURNAL CLUB

The British Blockchain Association
Advocating Evidence Based Blockchain

BBA FORUM | MARCH 2022

SUNDAY, 27 MARCH 2022 (5 PM BST)

Registration Link: https://bit.ly/375Tsc2

5:00 PM | Welcome
BBA Secretariat

JOURNAL CLUB

5:05 PM | Non Fungible Tokens & Crypto-Punks
Luisa Schaar, University of Law, UK
Author of the 2022 JBBA Paper:
NFT's as an Alternative Investment: Evidence from Crypto Punks

5:20 PM | Blockchain, Contact Tracing and Pandemics
Oritsebawo Paul Ikpobe, The University of Birmingham, UK
Author of the 2022 JBBA paper:
Can Blockchain Take Smartphones Out of Contact Tracing?

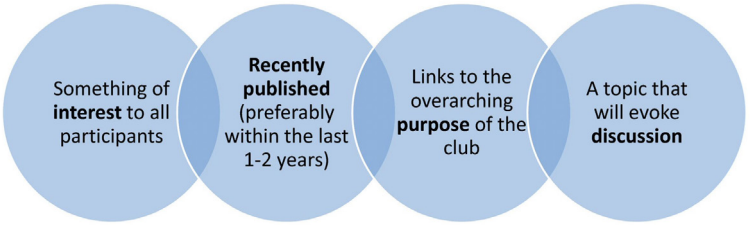
5:35 PM | Crypto Governance and Cryptocurrency Exchanges
Sabino Correa, London Business School, UK
Author of the 2020 JBBA Paper:
Crypto Governance: Analysing Platforms for Crypto Assets Trading

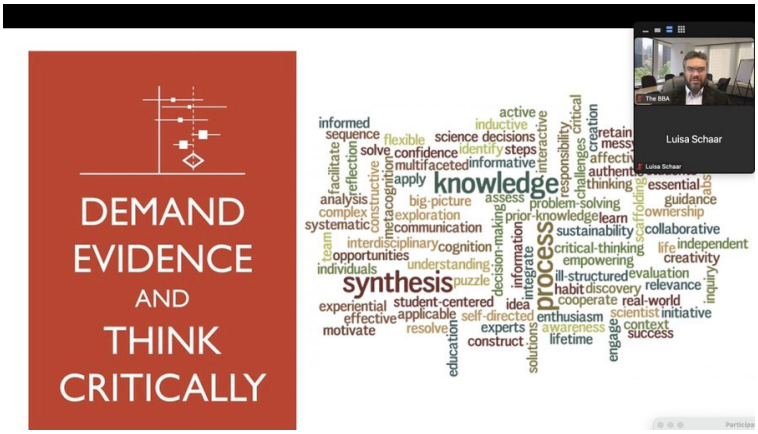
5:50 PM - 6:00 PM: Open Forum AMA & Close

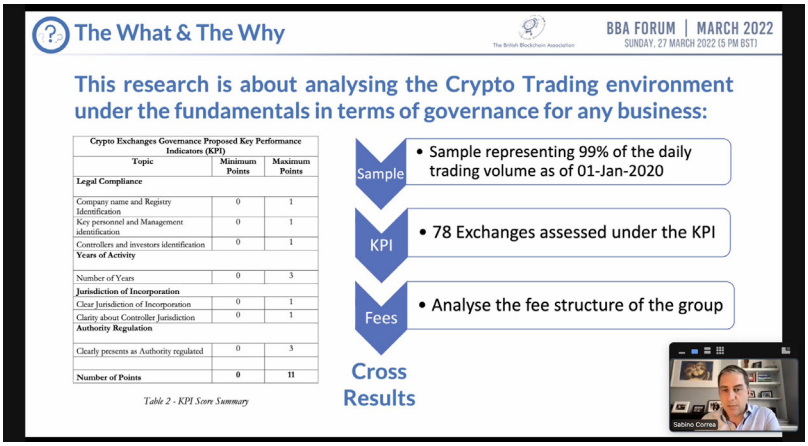
THE JBBA · UNIVERSITY OF BIRMINGHAM · SPEAKERS FROM* CEBB Centre for Evidence-Based Blockchain · The University of Law · London Business School · BLOCKCHAIN ASSOCIATIONS FORUM

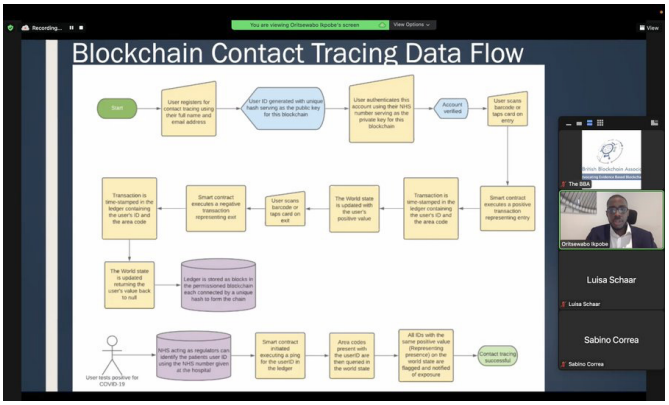
*DISCLAIMER: The views, opinions and factual statements expressed during this webinar are the personal views of the speaker only and do not necessarily represent the official policy, position or views of their organisations.

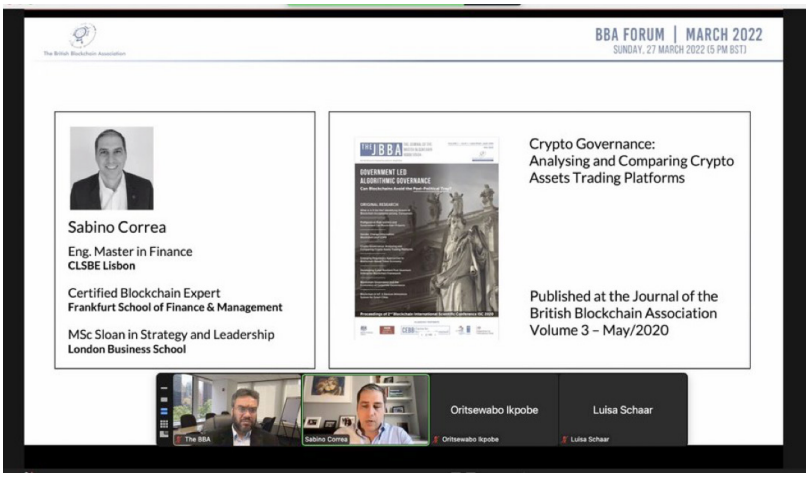
Blockchain and Crypto-assets Journal Club:

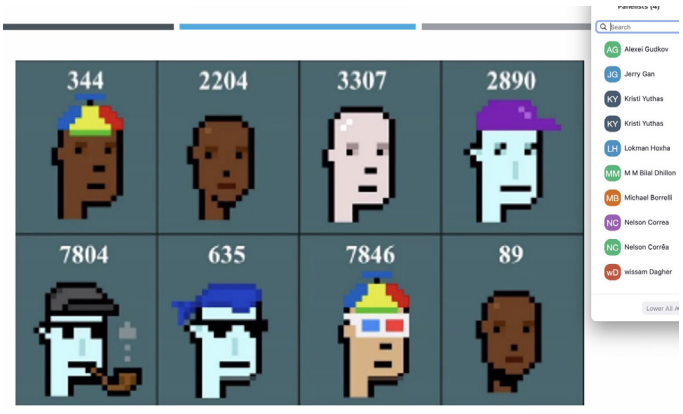












THE BBA STUDENT FORUM

A BBA student chapter helps reinforce classroom and experiential learning. In addition to the learning that occurs during chapter meetings, the submission of research articles to the JBBA journal helps develop industry-specific skills, along with skills in project management, technical writing and interpersonal communications.

Chapter activities culminate at the annual scholars in Blockchain conference, where students interact with students from other chapters, BBA members and advisors and network with industry leaders, scientists, and researchers.

The BBA recognises that students are the future leaders of the industry, and treats them as such. Chapters instil future professionals with an understanding of the role that collaboration, research, development and networking plays in blockchain developments and industry progress.

REASONS TO START THE BBA STUDENT CHAPTER

Encourage student collaboration

Foster dialogue about trends, issues, movements, opportunities impacting the blockchain industry

Connect to industry professionals and career opportunities

Obtain leadership experience driving BBA student chapter activities

Form student and professional relationships across the BBA including those with students from other chapters

Compete in hacking events

Publish papers in the JBBA

For more info, visit https://britishblockchainassociation.org/starting-a-student-chapter

DISCLAIMER

Publication in this journal of scientific, technical and literary material is open to all authors and readers. While every effort has been made to ensure articles published are free from typing, proof reading and formatting errors at the time of going to press, the publisher will be glad to be notified of any errors or omissions brought to our attention after the journal is published in the print format. Articles should not be taken to represent the policy or opinion of the British Blockchain Association, unless this is specifically stated. The publisher, affiliates of the British Blockchain Association, reviewers and editors assume no responsibility for any claims, instructions, methods or recommendations contained in the manuscripts. This publication is not a substitute for professional advice. The contents herein are correct at the time of printing and may be subject to change.

The JBBA is legally deposited at all 6 National Libraries of the UK and has become a part of the "British Heritage":

- British Library
- National Library of Scotland
- National Library of Wales
- Bodleian Libraries,, University of Oxford
- Cambridge University Library
- Library, Trinity College Dublin

The JBBA is indexed in: **Directory of Open Access Journals (DOAJ), Google Scholar and Web of Science**

Articles are indexed in **Semantic Scholar, Microsoft Academic** and available at online repositories at some of the most prestigious universities, worldwide.

The British Blockchain Association is a Publisher Member of:

The JBBA employs a plagiarism detection system. The JBBA is a peer reviewed journal. All manuscripts are reviewed by leaders in the appropriate field.

ISSN: 2516-3949
E-ISSN: 2516-3957

Online publication:
The articles published in this issue can be viewed Open Access on the JBBA website: jbba.scholasticahq.com

Advertising

All advertisements and sponsorships are expected to conform to ethical and business standards. The appearance of an advertisement or sponsorship material does not constitute an endorsement by the British Blockchain Association or by the Editor of this Journal.

Distribution

Print copies of the journal are sent worldwide to selected university libraries, policymakers, government officials, fin-tech organisations, eminent scholars, and major conferences. To request a print copy, please visit the journal website for more details.

Article Submission

To submit your manuscript to The JBBA, please visit:
https://jbba.scholasticahq.com/for-authors

FELLOWSHIP

of

The British Blockchain Association of The United Kingdom (FBBA)

An award of the Fellowship is recognition of exceptional achievement and contribution to Blockchain and allied disciplines. The Fellowship demonstrates a commitment to excellence, leadership, advancing standards and best practice, evidenced by a track record of outstanding contribution to the discipline of Blockchain or other Distributed Ledger Technologies.

FELLOWSHIP PRIVILEGES

- The use of 'FBBA' post-nominal
- Exclusive opportunity to officially represent the BBA by playing an active role in the direction and governance of the Association
- Privilege to take on a leadership role within the BBA and the profession as a whole
- Opportunity to represent the BBA at International Blockchain Conferences
- Significant discounts on BBA conferences and events
- Opportunity to join the Editorial Board of the JBBA
- Complimentary copy of the JBBA posted to your mailing address

The new Fellow appointments will be made twice a year (September and March).

Next Round of Fellowship Applications has been commenced (Applications submission Deadline: 15 July 2023)

For more information visit: **britishblockchainassociation.org/fellowship** or contact: **admin@britishblockchainassociation.org**

ENGAGE WITH
THE BRITISH BLOCKCHAIN ASSOCIATION
AND THE JBBA

'Like' and Share the latest JBBA and BBA updates on Facebook

Follow @Brit_blockchain to stay up-to-date on the latest news and announcements

Subscribe to our channel and view latest updates, research & education webinars, and cutting-edge scholarly content

Subscribe to JBBA RSS feed to keep track of new content and receive Alert notifications each time something new is published in the JBBA.

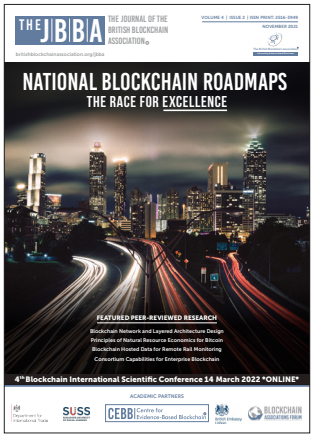
Follow us on Medium to receive exclusive content and stories from the JBBA

Connect with the BBA's Linkedin organisation profile and Follow us to receive real-time official updates

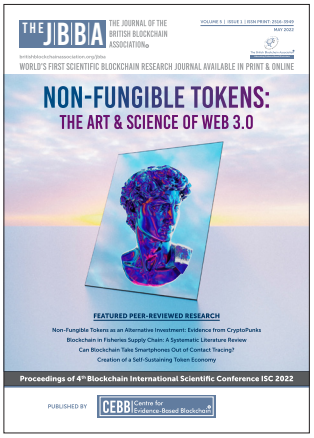
Volume 5 - Issue 2
November 2022

Volume 6 - Issue 1
May 2023

Volume 4 - Issue 1
May 2021

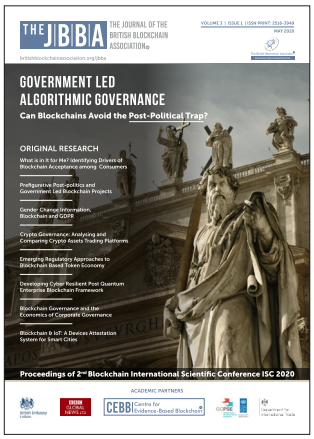


Volume 4 - Issue 2
November 2021

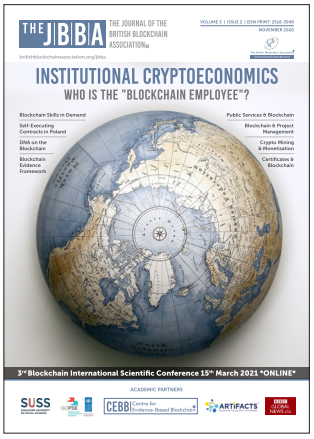


Volume 5 - Issue 1
May 2022

Volume 2 - Issue 2
October 2019



Volume 3 - Issue 1
May 2020



Volume 3 - Issue 2
November 2020

Volume 1 - Issue 1
July 2018

Volume 1 - Issue 2
December 2018

Volume 2 - Issue 1
May 2019

THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION (THE JBBA)

The British Blockchain Association®

Advocating Evidence Based Blockchain

www.britishblockchainassociation.org

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®