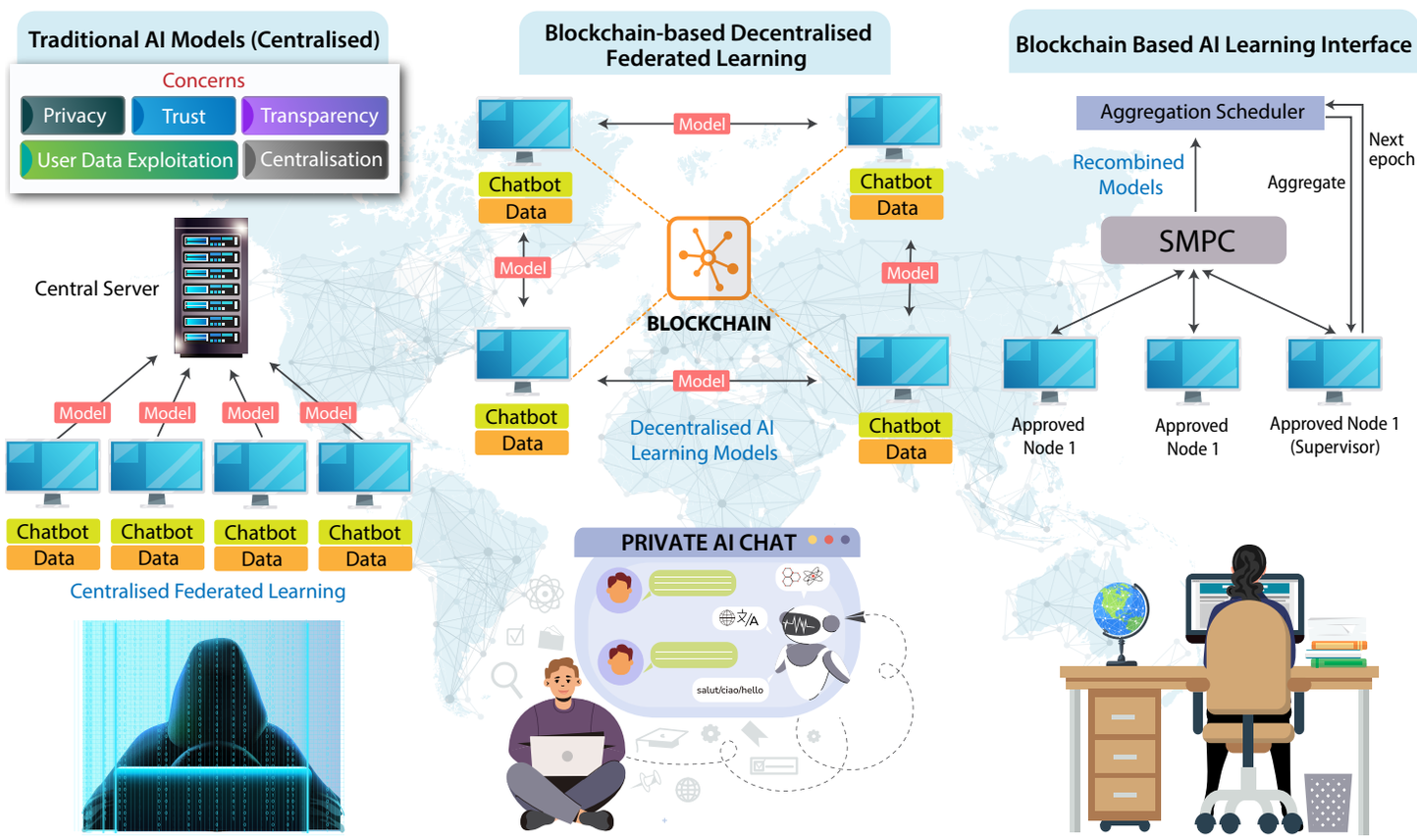
THE JBBA
THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®
britishblockchainassociation.org/jbba
VOLUME 7 | ISSUE 1 | ISSN PRINT: 2516-3949
MAY 2024
The British Blockchain Association
Advocating Evidence Based Blockchain
WORLD'S FIRST PEER-REVIEWED BLOCKCHAIN JOURNAL AVAILABLE IN PRINT & ONLINE

BLOCKCHAIN-BASED AI GOVERNANCE:

Building Trust in Intelligent Systems



FEATURED ARTICLES

Blockchain for AI: Confidential ChatGPTs and Decentralised Federated Frameworks
Blockchain & Trust Model for Traceability Data in Supply Chains
Building Blockchain-Based, Smart Contract Enabled Recycling Systems
Transparent Procurement Processes between Government and SMEs using Blockchain
Designing Blockchain-Based Customer Loyalty Programmes

4TH BLOCKCHAIN ASSOCIATIONS FORUM (BAF) ANNUAL MEMBER SUMMIT | 18 SEPTEMBER 2024

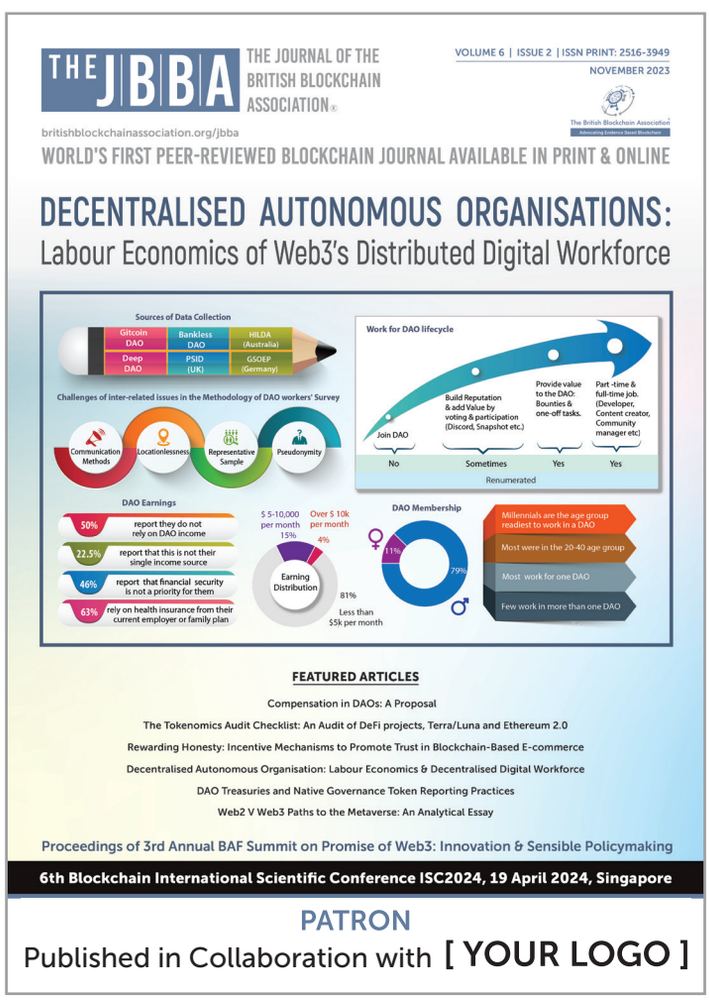
Proceedings of 6th Blockchain International Scientific Conference #ISC2024

PUBLISHED BY
CEBB Centre for Evidence-Based Blockchain®

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

BECOME A PATRON OF THE JBBA?

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



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

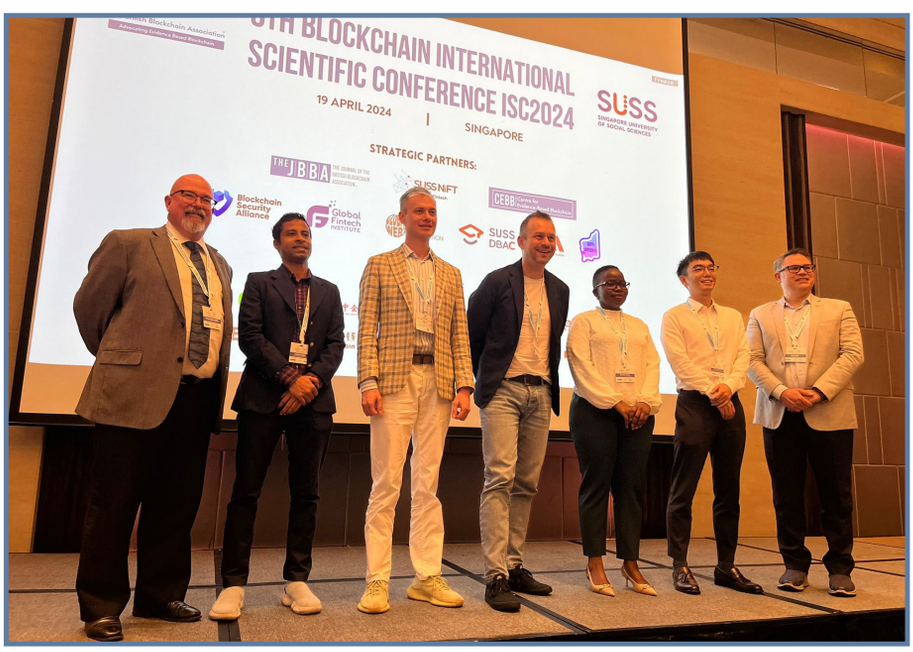
To become an Academic Partner or to Advertise in the Journal, contact us at:

www.britishblockchainassociation.org | info@britishblockchainassociation.org

Follow us on:

TABLE OF CONTENTS

BBA'S 6TH BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE #ISC2024




Dr Lo Swee Won
Deputy Director
SUSS Node for Inclusive Fintech
Alvin Chia
Senior Vice President
Head of Digital Assets Innovation (APAC)
Northern Trust
Arthit Sriumporn
CEO
Rakkar Digital
Jag Foo
Head of Business Development
Safeheron
Shawn Lim
Head of APAC
Avela Network
CEBB Centre for Evidence-Based
THE JBBA


Towards Confidential Chatbots: A Scalable
Decentralized Federated Learning Framework
Bharath Ramesh, PhD
Lecturer in Neuromorphic AI Systems
ternational Center for Neuromorphic Systems @ MARCS
ril 2024
CARLTON


EXIT
CARLTON


6TH BLOCKCHAIN INTERNATIONAL
SCIENTIFIC CONFERENCE ISC2024
19 APRIL 2024 | SINGAPORE
Opening Speech
Prof David Lee Kuo Chuen FBBA
Conference Co-Chair
Associate Editor in Chief, The JBBA
BBA's Regional Advisor for Singapore
Professor of Finance, SUSS
Advisor, SUSS NiFT
CEBB Centre for Evidence-Based Blockchain
SUSS NiFT
THE JBBA
CARLTON


CARLTON

MEMBERS & PARTNERS OF THE BBA ECOSYSTEM

EPOKA UNIVERSITY

HM Government of Gibraltar

Filecoin Foundation

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

GANT

HELLENIC BLOCKCHAIN ASSOCIATION

CANADIAN BLOCKCHAIN CONSORTIUM

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

BLOCKCHAIN ALLIANCE MEXICO

SANBA
South African National Blockchain Alliance

Pakistan Blockchain Institute

ASOSIASI BLOCKCHAIN INDONESIA

ALASTRIA

RMIT UNIVERSITY

GRESHAM INTERNATIONAL

WORKING IN COLLABORATION WITH:

Department for International Trade

BBC NEWS GLOBAL

British Embassy Lisbon

GCPSE Global Centre for Public Service Excellence

UNDP

appg BLOCKCHAIN TECHNOLOGIES
All-Party Parliamentary Group

ARTiFACTS
Researcher Recognition, Accelerated

Join Now at britishblockchainassociation.org/membership

SUBSCRIBE TO OUR YOUTUBE CHANNEL

YouTube

The BBA

@TheJBBA · 360 subscribers · 208 videos

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

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

Subscribe

BBA FORUM APRIL 2024: CBDC and Privacy: BBA's Response to Bank of England's RFI...

13 views • 3 days ago

BBA FORUM APRIL 2024: Blockchain in Fisheries Supply Chain by Dr Trevor...

13 views • 6 days ago

BBA FORUM APRIL 2024: Lord Goddard of Stockport Insights on Blockchain, Digital...

12 views • 7 days ago

BBA FORUM MARCH 2024 | Part 2: BBA Ecosystem Updates - Professor Dr Naseem...

19 views • 1 month ago

BBA FORUM MARCH 2024 | Part 1 - Topic: What are Flat-Coins? Insights from Dr...

24 views • 1 month ago

Industry Reception: APPG on Blockchain Technologies, December 2023

82 views • 3 months ago

BBA President Receiving UK National Honour (MBE) from The King

116 views • 3 months ago

Digital Borders and Blockchain: Insights from Natalie Elphicke MP, APPG Chair

49 views • 4 months ago

The Latest Issue Of The JBBA Has Been Showcased In The Metaverse! #bba...

20 views • 5 months ago

BAF 3rd Annual Summit: Mr Simon Callaghan, CEO of Blockchain Australia on...

26 views • 6 months ago

Danielle Padula, Head of Marketing at Scholastica, speaking at Global Peer Revie...

4 views • 6 months ago

BAF 3rd Annual Summit: Keynote: Prof. Dr. Naseem Naqvi MBE of The British...

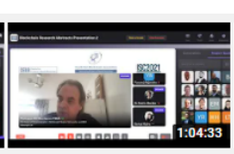
21 views • 6 months ago

ISC2021: Blockchain Research Abstract...

44 views • 1 year ago

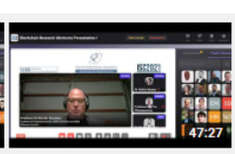
ISC2021: Blockchain Use cases

16 views • 1 year ago



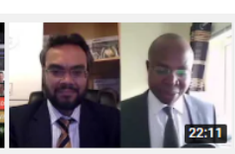
ISC2021: Blockchain Research Abstract Session 2

21 views • 1 year ago



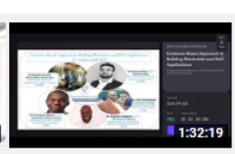
ISC2021: Blockchain Research Abstracts Session...

35 views • 1 year ago



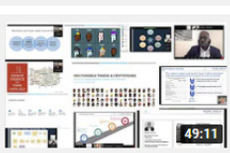
ISC2021 Opening Keynote Dr Naseem Naqvi, President...

52 views • 1 year ago



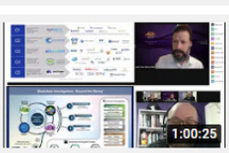
Centre for Evidence Based Blockchain (CEBB) Africa...

29 views • 1 year ago



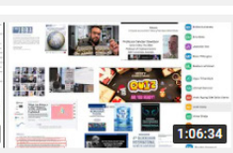
BBA Forum (JOURNAL CLUB) March 2022

1 view • 20 hours ago



BBA Forum, January 2022

38 views • 2 months ago

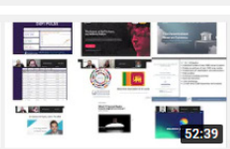


BBA Forum December 2021

15 views • 3 months ago

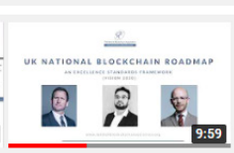
BBA Forum November 2021

17 views • 3 months ago



BBA Forum October 2021

31 views • 5 months ago



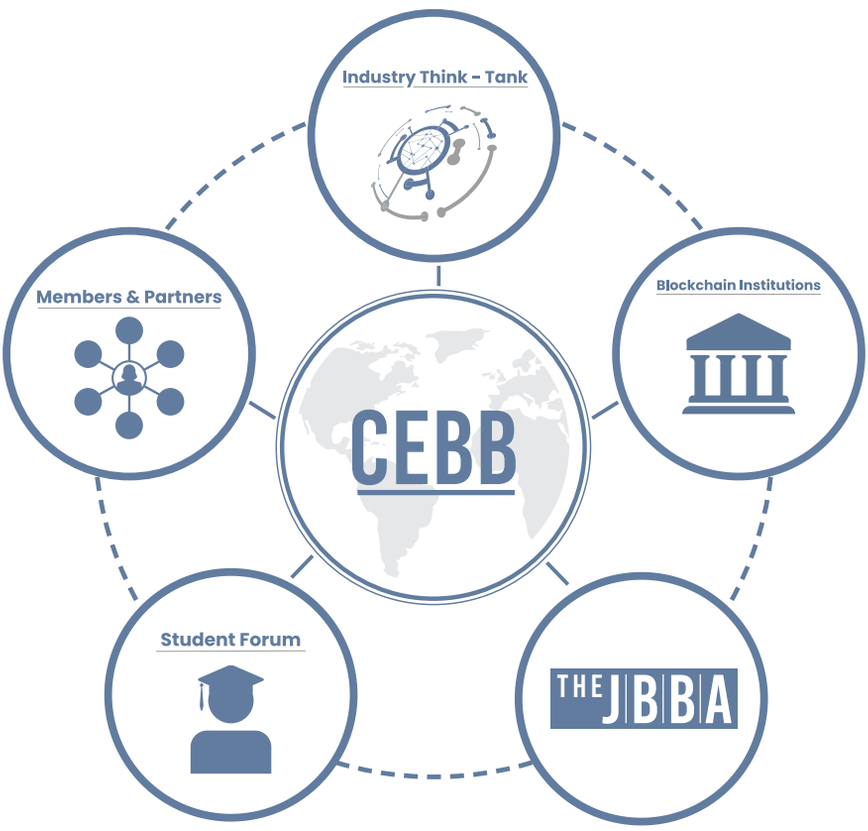
UK National Blockchain Roadmap (UK NBR)

6.7K views • 5 months ago

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

CEBB | Centre for Evidence-Based Blockchain®

Bridging the Blockchain Research and Practice Gap

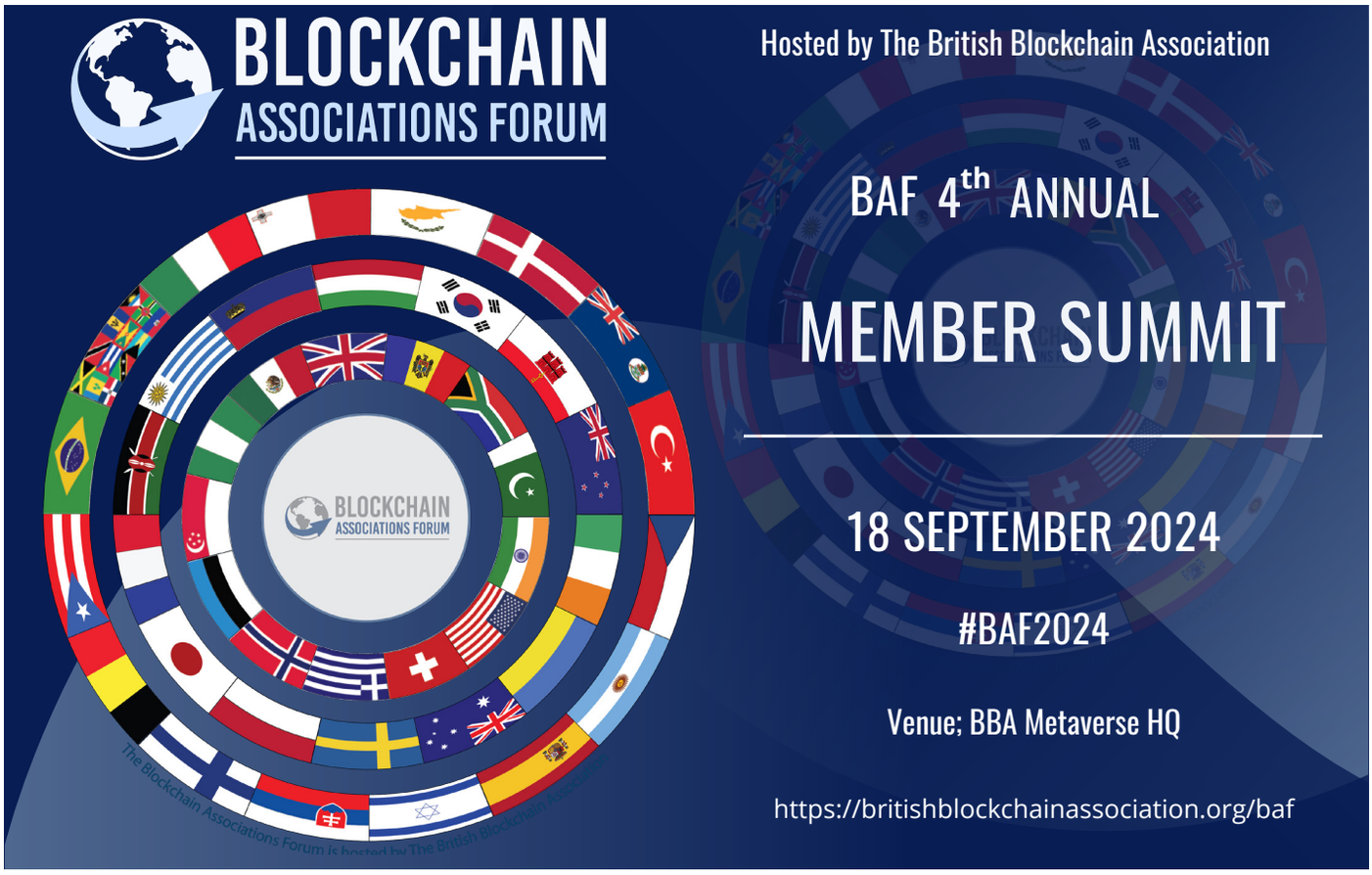


MEMBERS

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
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



CEBB Centre for Evidence-Based Blockchain

The British Blockchain Association
Advocating Evidence Based Blockchain

BLOCKCHAIN ASSOCIATIONS FORUM

4TH ANNUAL BAF MEMBER SUMMIT

(VENUE: BBA METAVERSE HEADQUARTERS)

#BAF2024

18 SEPTEMBER 2024

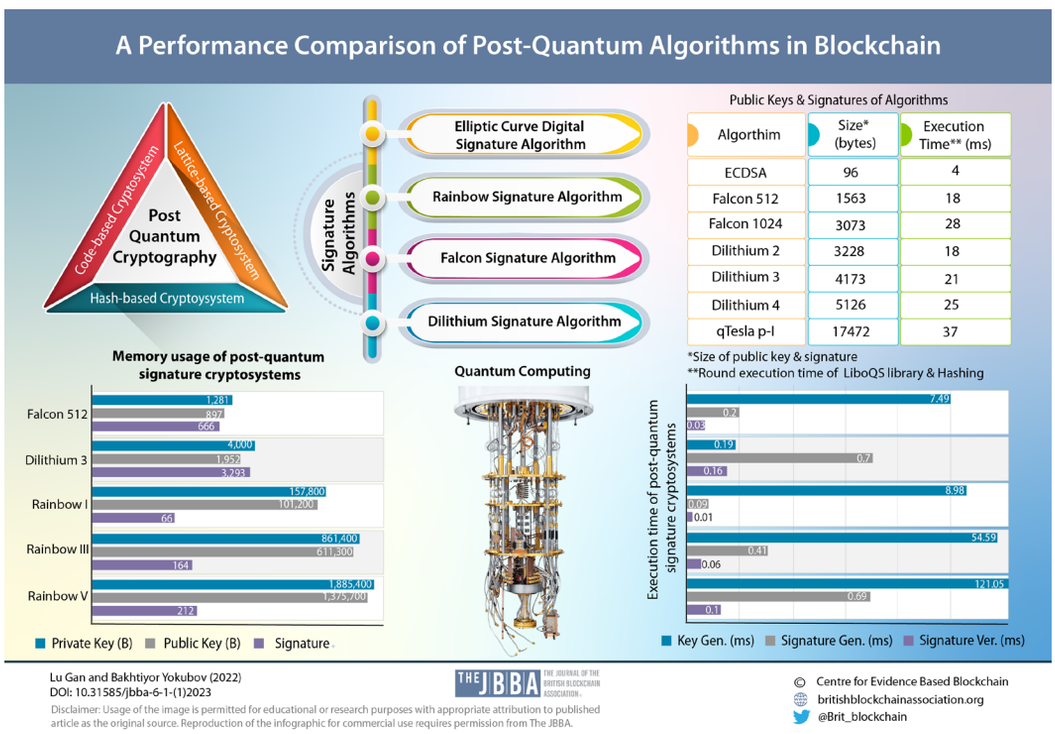
For more info, visit https://britishblockchainassociation.org/baf/

BBA METAVERSE HEADQUARTERS

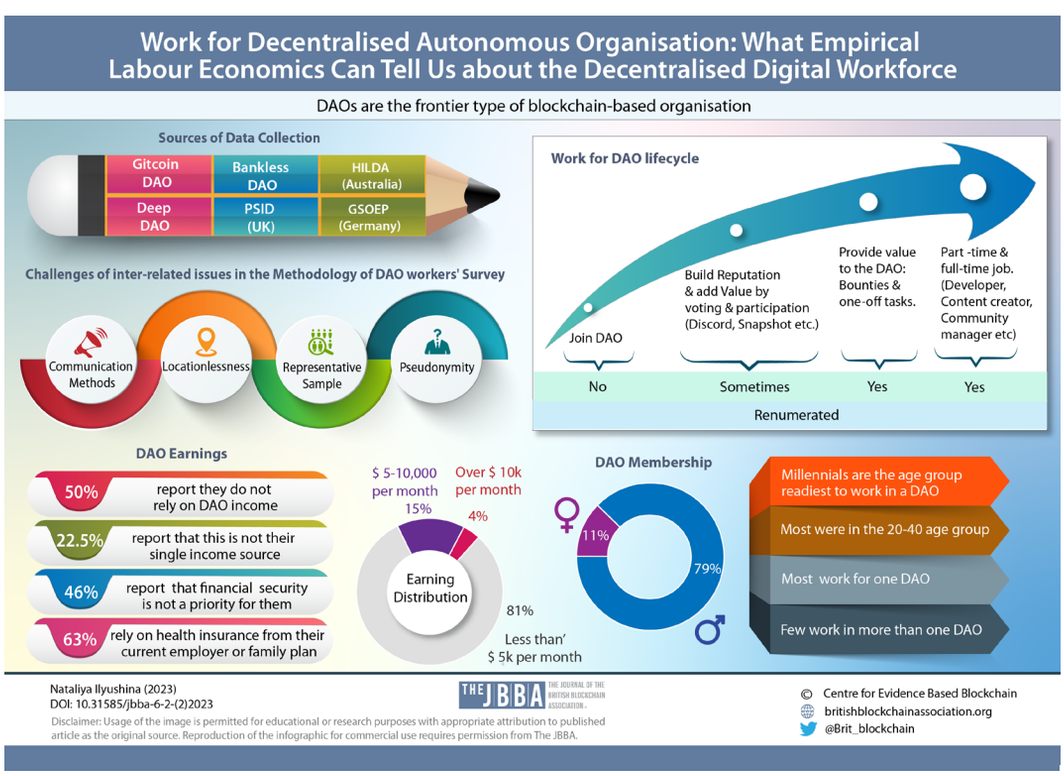
For more info, visit https://britishblockchainassociation.org

JBBA INFOGRAPHICS

PRODUCED BY
CENTRE FOR EVIDENCE BASED BLOCKCHAIN (CEBB)



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



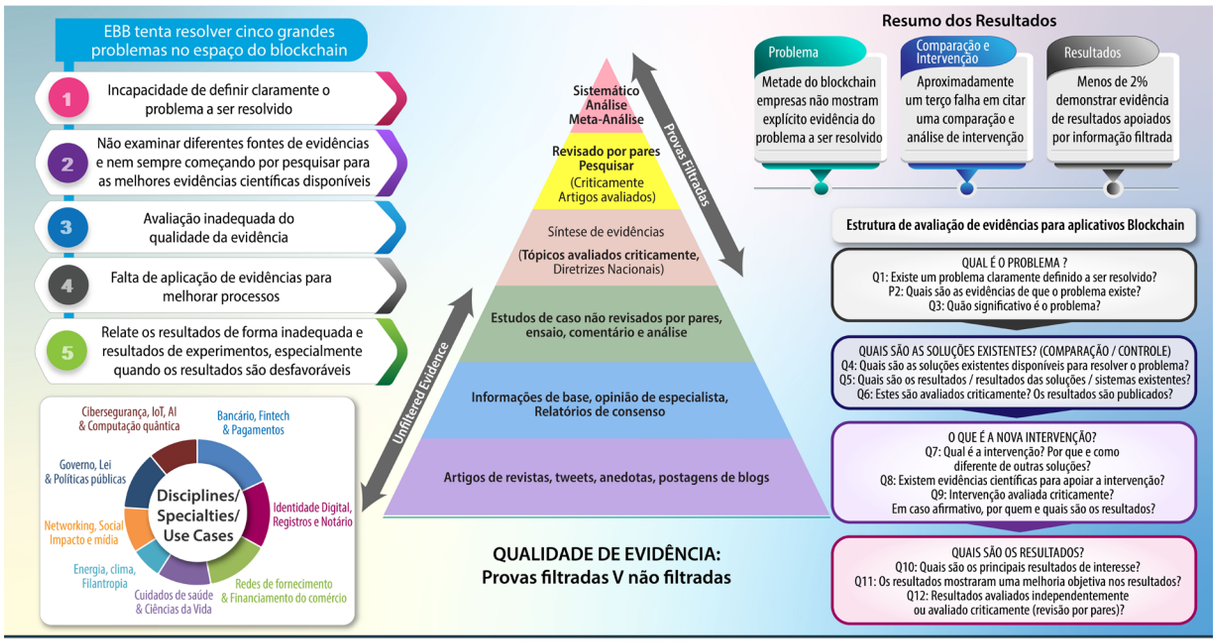
Nataliya Ilyushina (2023)
DOI: 10.31585/jbba-6-2-(2)2023

JBBA RESEARCH INFOGRAPHICS AVAILABLE IN MULTIPLE LANGUAGES

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

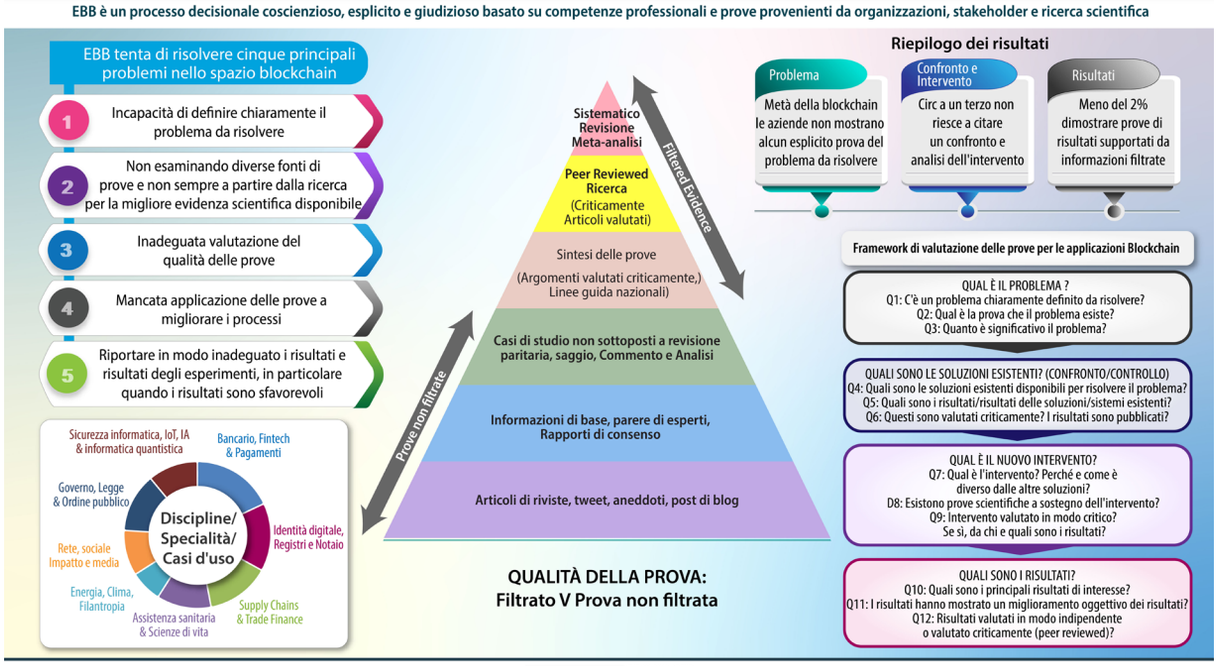


Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020

ITALIAN

Blockchain basata sull'evidenza (EBB): risultati di uno studio globale di Progetti Blockchain e Start-up

EBB è un processo decisionale coscienzioso, esplicito e giudizioso basato su competenze professionali e prove provenienti da organizzazioni, stakeholder e ricerca scientifica

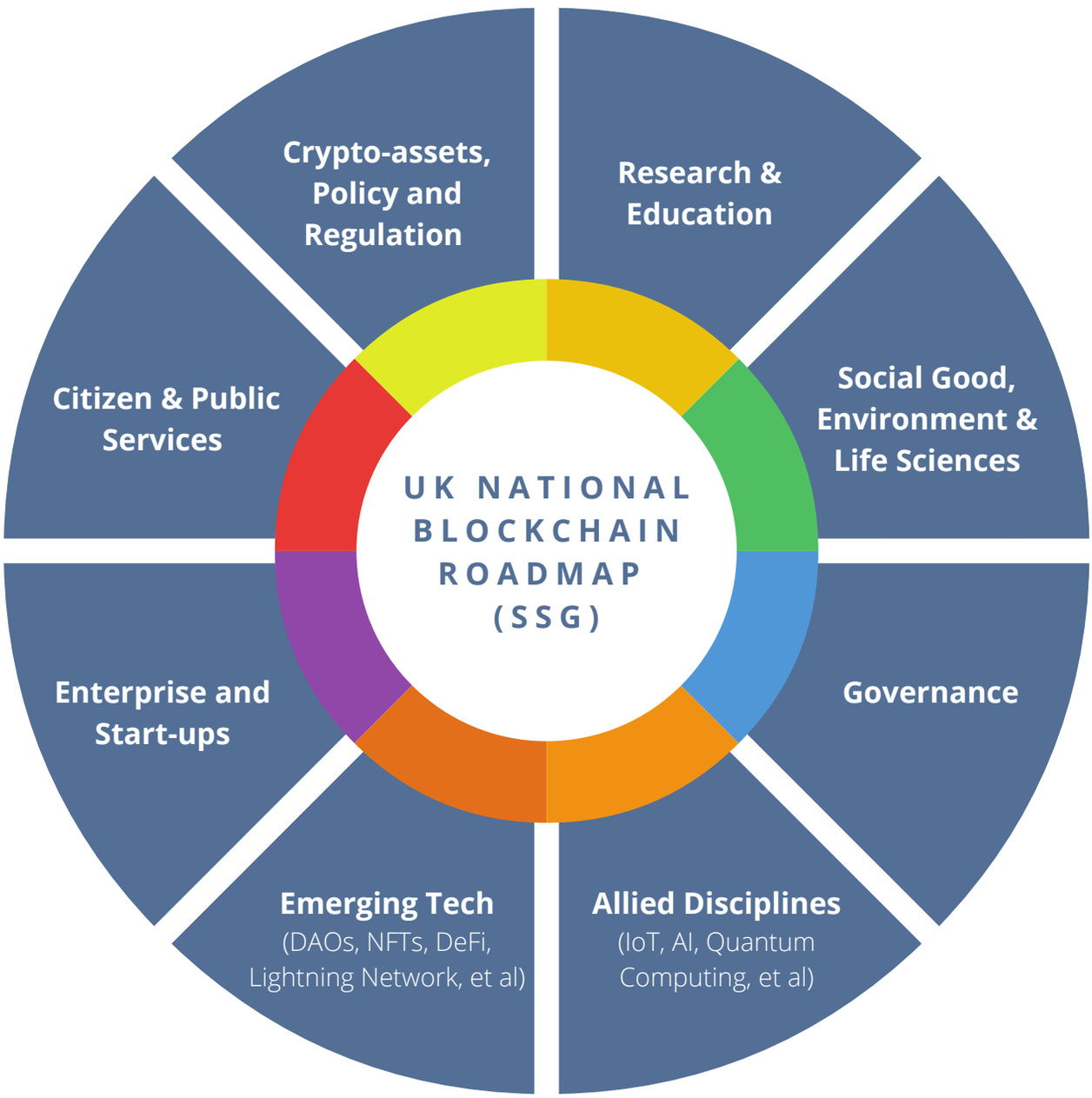


Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020

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

UK NATIONAL BLOCKCHAIN ROADMAP (NBR)

(VISION 2030)



SUB-SPECIALITY STEERING GROUPS (SSG)

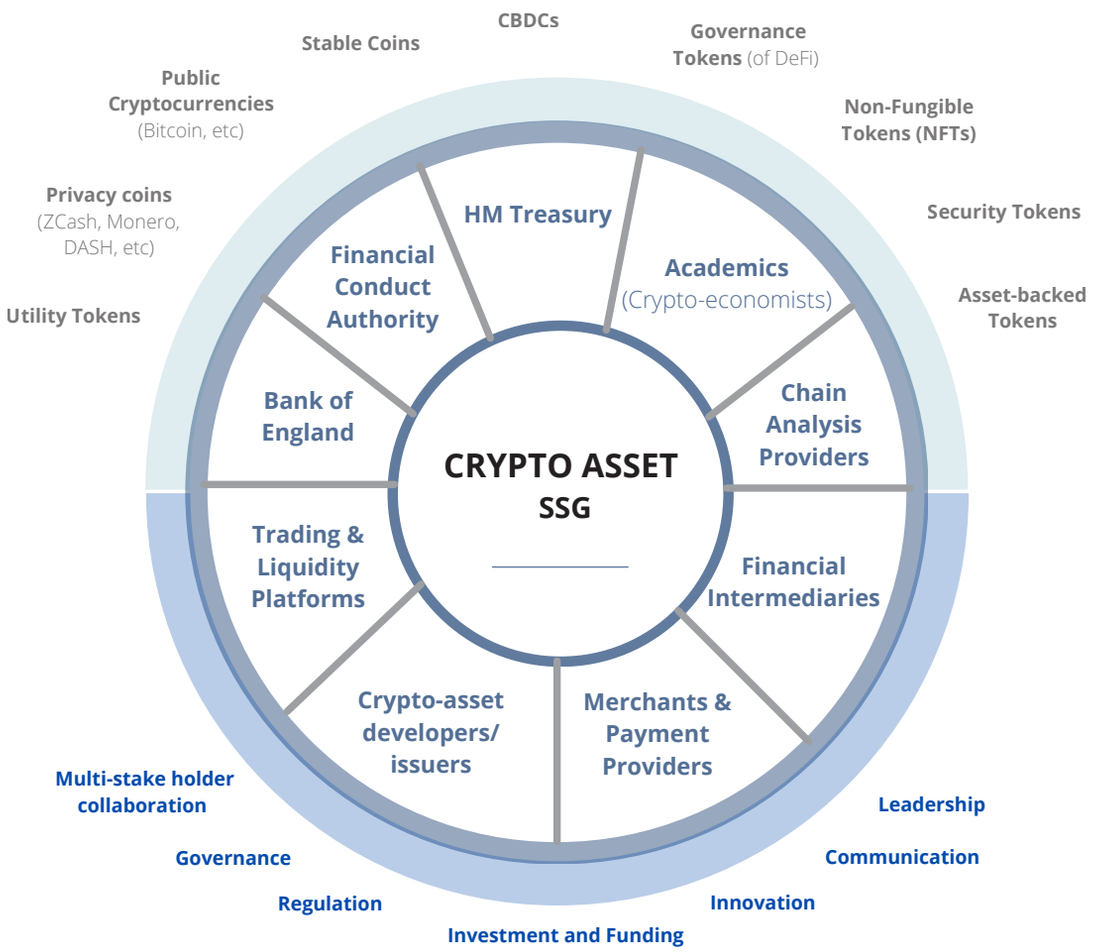
Contribute to the UK National Blockchain Roadmap and join a Sub-Speciality Steering Group (SSG)

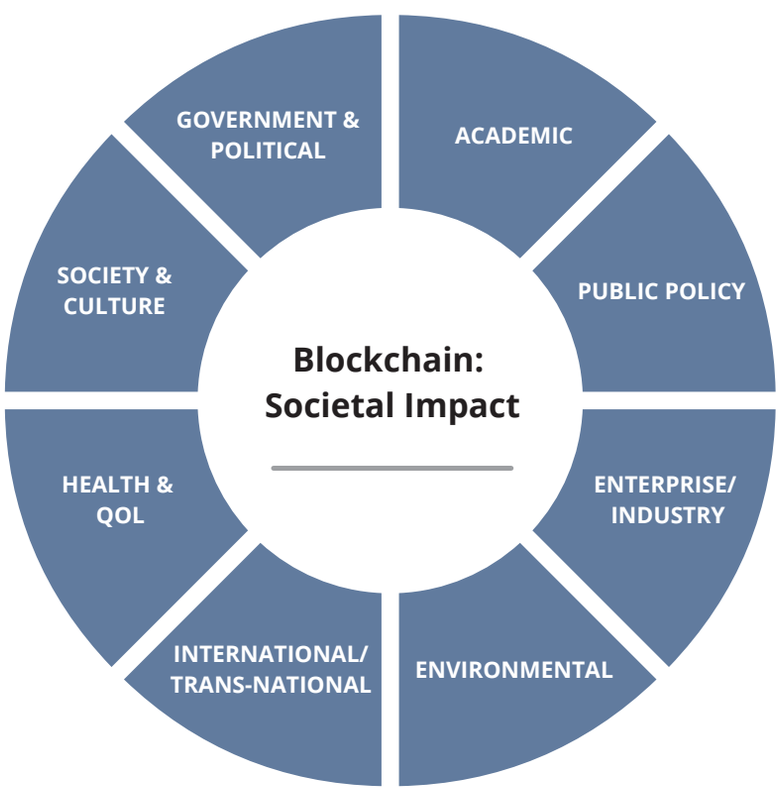
Contact us at cebb@britishblockchainassociation.org

Or visit:

https://britishblockchainassociation.org/national-blockchain-roadmap-vision-2030/

CRYPTO ASSET
SUB-SPECIALITY STEERING GROUP (SSG)
(PROPOSED ARCHITECTURE)





UK NATIONAL BLOCKCHAIN ROADMAP (NBR)

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:

Prof Naseem Naqvi MBE FBBA	UK
Dr Mureed Hussain FBBA	UK
Dr Duane Wilson	USA
Dr Swathi Kaluvakuri	India
Prof Benjamin Cole FBBA	USA
Prof Marc Pilkington FBBA	France
Prof Apostolos Kourtis	UK
Prof Mark Lennon	USA
Prof Ping Wang	USA
Prof Sinclair Davidson FBBA	Australia
Prof Mary Lacity FBBA	USA
Prof Riem Abdelazim	USA
Prof Mark Fenwick	Japan

EDITORIAL

It gives me great honour and delight to present to you the 13th Issue of The Journal of The British Blockchain Association (JBBA).

We stand at an important historical juncture in Web3. By leveraging the power of blockchain technology, we can foster financial inclusion and economic growth. It is expected that in 2024, Web3 will make advancements at a pace that exceeds most people's expectations, providing users in the post-internet era with unprecedented "asset and data ownership." Data security and privacy protection will be the focus, and an uncompromisable mission of the Web3 industry over the coming years. To this end, the Singapore government has already used Ethereum to build digital infrastructure such as TradeTrust for international trade and OpenCert to verify the authenticity of certificates issued by educational institutions. Singapore regulators have also granted DigiFT a license to tokenize real-world assets.

In an era where digital transformation is reshaping the contours of our societies and economies, blockchain technology emerges as a cornerstone for innovation, trust, and security. It is against this backdrop that this special conference edition of The Journal of The British Blockchain Association (JBBA) takes a significant stride in capturing the pioneering research and discussions presented at the 6th Blockchain International Scientific Conference (ISC2024) held in Singapore. For the first time, the ISC chose a venue outside the United Kingdom, reflecting the global nature of blockchain technology and its community. As co-hosts of this landmark event, the Singapore University of Social Sciences, together with The British Blockchain Association, endeavoured to create a platform for international scholars, industry experts, and enthusiasts to share their insights, research findings, and visions for the future of blockchain technology.

The papers selected for publication in this issue represent the cutting edge of blockchain research. They address critical challenges and propose innovative solutions that span across various sectors, including confidential communications, supply chain management, recycling systems, procurement processes, and customer loyalty programs:

Towards Confidential Chatbot Conversations: A Decentralized Federated Learning Framework delves into enhancing privacy in AI-driven communications using Blockchain, a topic of significant relevance as digital interactions become ubiquitous in our personal and professional lives.

Improving the Trustworthiness of Traceability Data in Food Supply Chain Using Blockchain and Trust Model offers a novel approach to securing and verifying the provenance of food products. This paper highlights the role of blockchain in fostering transparency and trust in global food supply chains.

A Blockchain-Based, Smart Contract and IoT-Enabled Recycling System proposes an integrated system that leverages blockchain and IoT to incentivize and streamline recycling efforts. This research exemplifies the potential of blockchain in promoting sustainable environmental practices.

Using Blockchain Technology to Improve the Integrity and Transparency of Procurement Processes between SMMEs and Government: A Systematic Literature Review critically examines how blockchain can address the perennial challenges of transparency and efficiency in public procurement, particularly benefiting Small, Medium, and Micro Enterprises (SMMEs).

Designing a Blockchain-Based Customer Loyalty Program using Design Science Research Method explores the application of blockchain in enhancing customer loyalty programs. This paper suggests a framework that could revolutionize how businesses engage and retain customers through trust and transparency.

As we present these contributions to our readers, it is our hope that they not only advance the discourse in the blockchain community but also inspire further research and innovation. The ISC2024 has been a testament to the collaborative spirit and forward-thinking ethos of the global blockchain community. The proceedings at the conference will reflect our commitment to excellence and the advancement of blockchain technology. The emergence of Web3 aims to solve the problems in Web2, including the loss of privacy, the vulnerability of creators, and the abuse of power by centralised platforms.

The Web3 has seen two major developments in the last year: Bitcoin Inscriptions and the Decentralized Physical Infrastructure Network (DePIN). DePIN will have a strong positive flywheel effect during bull markets. Research predicts that DePIN could reach a scale of $3.5 trillion by 2028. In January this year, the US Securities and Exchange Commission approved the first spot bitcoin exchange-traded funds (ETFs), allowing investors to invest in bitcoin through their brokerage accounts. It is an understatement to say that Bitcoin and Ethereum and other open blockchains have changed the landscape of payment systems, asset classes, and international financial geopolitics.

In closing, I would like to express my heartfelt gratitude to all contributors, reviewers, and the editorial team. Together, we are shaping the future of blockchain technology and its application across diverse sectors. Let us continue on this path of innovation, collaboration, and discovery.

Professor Dr. David Lee Kuo Chuen FBBA
Associate Editor in Chief, The JBBA
Professor of Finance,
Singapore University of Social Sciences

JBBA IN THE METAVERSE

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

WHY PUBLISH IN THE JBBA?

- We publish in real-time, online, as well as in **PRINT - THE HARD COPIES ARE DISTRIBUTED WORLDWIDE**
- Print copies are available at some of the largest libraries in the world including **BRITISH LIBRARY** and over **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-7-1-(3)2024

Towards Confidential Chatbot Conversations: A Decentralised Federated Learning Framework

Hongxu Su[1], Cheng Xiang[1], Bharath Ramesh[2]
[1] *Department of Electrical and Computer Engineering, National University of Singapore, Singapore*
[2] *International Center for Neuromorphic Systems, Western Sydney University, Sydney, Australia*

Correspondence: bharath.ramesh03@u.nus.edu
Received: 13 December 2023 **Accepted:** 14 January 2024 **Published:** 28 February 2024

Abstract

The development of cutting-edge large language models such as ChatGPT has sparked global interest in the transformative potential of chatbots to automate language tasks. However, alongside the remarkable advancements in natural language processing, concerns about user privacy and data security have become prominent challenges that need immediate attention. In response to these critical concerns, this article presents a novel approach that addresses the privacy and security issues in chatbot applications. We propose a secure and privacy-preserving framework for chatbot systems by leveraging the power of decentralised federated learning (DFL) and secure multi-party computation (SMPC). Our DFL framework leverages blockchain smart contracts for participant selection, orchestrating the training process on user data while keeping the data local, and model distribution. After each round of local training by the participants, the blockchain network securely aggregates the model updates using SMPC, ensuring that participants' raw model parameters are not exposed to others. The global model is encrypted and stored in hypermedia protocols such as the InterPlanetary File System. Participants decrypt the global model updates using their private keys to further fine-tune their models. Iterative training rounds are executed through the blockchain network, with participants updating the model collaboratively using SMPC. Experiments show that our approach achieves comparable performance to centralised models while offering significant improvements in privacy and security. This article presents a ground-breaking solution to privacy and security challenges in chatbots, and we hope our approach will foster trust and encourage broader adoption of chatbot technology with privacy at the forefront.

Keywords: *Large language models, Privacy-centric machine learning, Decentralized federated learning, Multi-part computation, Knowledge distillation, Quantized language models*

JEL Classifications: *Privacy-Preserving Learning, Decentralised Federated Learning, Tiny Language Models (TinyLMs), Secure Multi-party Computation (SMPC), Blockchain Technology*

1. Introduction

Natural language processing (NLP) and Large language models (LLMs) have recently revolutionised human–computer interaction [1]. Advanced LLMs such as ChatGPT by OpenAI have shown their potential to transform various industries and automate language tasks on an unprecedented scale [2]. However, this surge in useful applications has also raised significant concerns about privacy, trust, and user data exploitation [3]. As these LLMs process large amounts of user data for training and fine-tuning, it is essential to address the potential risks associated with unauthorised data access, breaches, and misuse. Striking a delicate balance between leveraging the power of chatbot technology and protecting user privacy is a critical challenge for the widespread adoption and ethical deployment of these revolutionary NLP systems.

Federated learning (FL), originally proposed by McMahan et al. [4], is a promising solution for preserving user privacy, especially in the context of NLP technologies [5]. FL enables model training by distributing the learning process across individual user devices, thereby avoiding the need to centralise sensitive data on a single server. This approach keeps user data localised, encrypted, and under the user's control, ensuring that no raw personal information is exposed during the training process. By aggregating model updates from multiple users without sharing their individual data, FL enhances privacy protection and minimises the risk of data breaches and unauthorised access.

Despite the significant privacy advantages offered by FL, centralised FL implementations still pose certain threats. A centralised FL setup introduces the possibility of a single point of failure, where the central server becomes vulnerable to attacks, potentially compromising the privacy of users. Additionally, model privacy concerns arise as the central server might have access to aggregated model updates from various users, raising the risk of information leakage or even malicious central servers as an extreme example [6]. As such, striking the right balance between leveraging the benefits of FL's privacy-preserving capabilities and mitigating the challenges of centralised deployment remains a crucial area of research for fostering trust and upholding user privacy in the dynamic landscape of NLP.

Blockchain-based learning is a promising alternative to centralised FL for addressing concerns about user privacy [7–9], especially for NLP technologies [10]. This approach mitigates the risks associated with a single point of failure by leveraging the decentralised and distributed nature of blockchain networks. In blockchain-based FL, or decentralised federated learning (DFL), participants (nodes) collaborate directly on the blockchain, contributing their encrypted model updates while maintaining control over their individual data [11]. The tamper-resistant nature of blockchain ensures data integrity and prevents unauthorised access, offering a more secure and privacy-preserving environment. Moreover, the use of blockchain smart contracts for aggregating model updates enables transparent and trustless computations without compromising individual

users' data privacy. Embracing blockchain-based FL has the potential to revolutionise the chatbot landscape by instilling user confidence and reinforcing the protection of sensitive information throughout the FL process. Figure 1 showcases the differences between a centralised and a decentralised process and highlights the key differences in the setup, which is the blockchain infrastructure orchestrating the processing of FL instead of a central server.

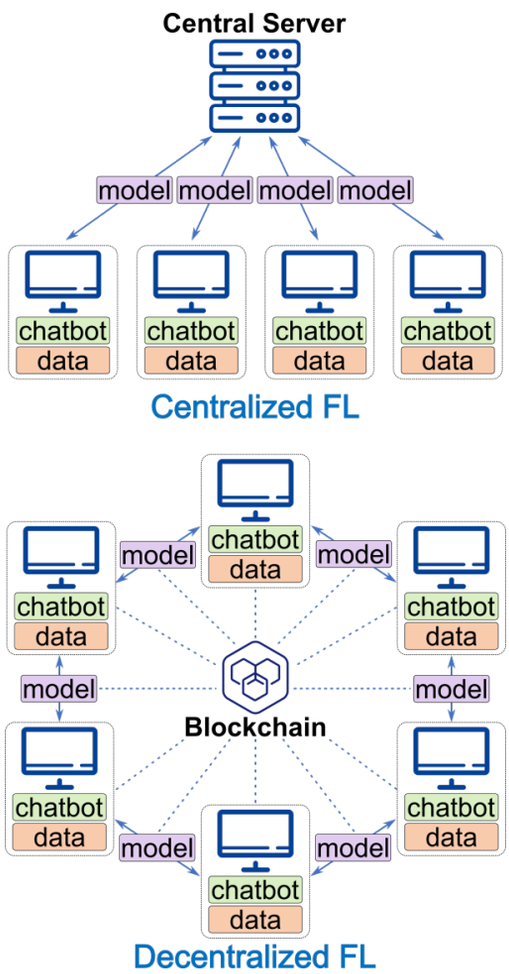


Figure 1. Centralised vs decentralised federated learning.

Firstly, blockchain-based DFL offers promising solutions to user privacy concerns in chatbot applications, but it also introduces specific challenges that need to be carefully considered, as discussed in this latest survey article [11]. One of the main challenges is the scalability and latency of blockchain networks. Because DFL involves multiple participants performing computations and sharing model updates on the blockchain, the sheer volume of data and transactions may result in slower processing times and increased network congestion. InterPlanetary File System (IPFS) [12] can be adopted to address scalability and latency concerns. IPFS allows participants to store models without explicitly relying on the blockchain infrastructure, making it an ideal solution for model communication and storage in DFL. The storage burden is distributed across participants with IPFS, which alleviates the scalability issues faced by a central server or the blockchain network itself.

Secondly, different blockchains use various consensus algorithms, such as Proof-of-Work, Proof-of-Stake, or Practical Byzantine Fault Tolerance [11]. The choice of consensus mechanism affects network performance, energy consumption, and the level of decentralisation. To address this challenge, the DFL process can be adapted to different consensus mechanisms, ensuring compatibility with the selected blockchain. This adaptability allows blockchain-based DFL to optimise its performance while maintaining its privacy-preserving attributes.

Thirdly, blockchain-based DFL faces the challenge of selecting a suitable model evaluation mechanism without compromising on security. We address this by ensuring differential privacy-enabled models [13] are used for peer evaluation and subsequently rewarding users for their participation in the evaluation phase, instead of users allowing access to raw model parameters that may potentially expose the training data via inversion attacks. A related issue is how to perform the model aggregation for the FL process at the end of each epoch without exposing the models of each user. To this end, we implement secure multi-party computation (SMPC) techniques to enable collaborative model aggregation across multiple participants [14]. SMPC can let multiple users combine their private models without knowing each other's inputs. To the best of our knowledge, we are the first to introduce this for blockchain-based FL [11].

Finally, deploying LLMs locally for privacy-preserving DFL chatbot applications is challenging because they require a lot of computational power, especially during inference tasks. LLMs, such as GPT-4, have shown impressive language-generation capabilities, but their large size and complexity require powerful hardware resources for efficient real-time performance [15]. Local deployment on resource-constrained devices can result in slow response times, increased latency, and potential memory constraints, which can hinder the seamless user experience that is critical for chatbot interactions. Similarly, fully homomorphic encryption-enabled LLMs increase the latency while trying to preserve user privacy [16]. Additionally, the continuous evolution of LLMs with ongoing updates and improvements requires consistent access to the latest model versions, which may be impractical to maintain locally. As a result, striking a balance between leveraging the capabilities of LLMs and the computational constraints of local deployment is a critical consideration for achieving optimal performance in chatbot applications.

One way to address the challenges of deploying LLMs locally for DFL applications is to limit the chatbot's functionality and embrace Tiny Language Models (TinyLMs) [17]. TinyLMs are smaller versions of LLMs that have been optimised for specific tasks or domains, reducing the model size and computational requirements without sacrificing much performance. By using TinyLMs that are tailored to the specific needs of the application, one can achieve a more lightweight and responsive deployment, making it feasible to run the chatbot on resource-constrained devices. This strategic use of TinyLMs allows chatbot developers to strike a balance between offering valuable language processing capabilities and ensuring a smooth user experience without the burden of deploying unwieldy LLMs locally.

In summary, by combining the power of blockchain-based DFL with the generation of TinyLMs, we present a novel framework that revolutionises how language models are trained and deployed. Notably, our contribution extends beyond conventional methods by being among the first to implement SMPC in the context of DFL. This innovation ensures that participants' data remains confidential during the collaborative model aggregation process, enhancing the privacy and security of the overall system. In addition, the generation of TinyLMs through fine-tuning, distillation, and quantisation enables the creation of efficient language models suitable for deployment on resource-constrained devices. The next section details our framework, Section 3 demonstrates the effectiveness of our approach, and, finally, the article is concluded in Section 4.

2. Decentralised Federated Learning for TinyLMs

Secure DFL is a type of machine learning that allows multiple devices to collaboratively train a collaborative model without sharing their data and model with each other. This is done by having each device train a local

model on its own data and then periodically exchanging encrypted updates with the other devices. The updates are then used to train a global model that is shared by all of the devices. Our blockchain-based DFL framework uses a smart contract to manage the entire process. The framework also includes a number of features that make it well-suited for NLP applications, including support for different learning algorithms, scalability, and security using SMPC, as shown in Figure 2.

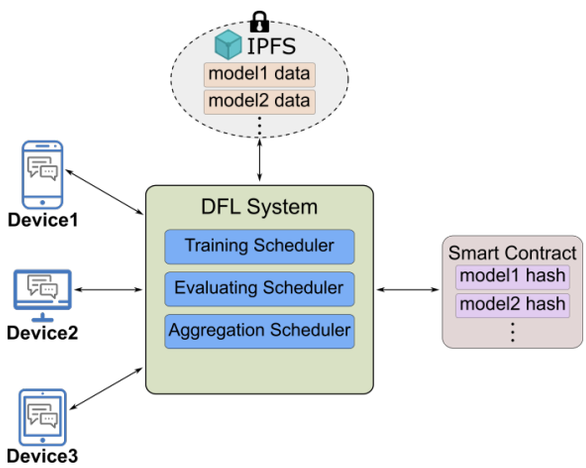


Figure 2. General architecture of our DFL for TinyLMs.

Iterative Federated Learning: Participants are identified as nodes based on predefined criteria such as a registration fee, ensuring their active participation in the DFL process. The baseline dataset is distributed among the selected participants. Each node also possesses its local data and performs individual model training combining it with the distributed dataset, fostering baseline model performance. The training scheduler determines the timing and frequency of training rounds, allowing participants' devices to contribute model updates at specified intervals. Participants contribute to model improvement by providing updated model parameters during each iteration. This iterative process allows the model to learn from various data distributions and adapt to diverse user preferences, which promote continuous model refinement.

Secure Storage: All communication between blockchain nodes and transactions is carefully protected using cryptographic protocols and the blockchain's inherent consensus mechanisms. The global model is encrypted before being stored in the IPFS for added security and privacy. Nodes use their private keys to decrypt the model updates, updating their local models without revealing any sensitive data. This process ensures that the model updates are secure and private, while also allowing for efficient aggregation and distribution.

Privacy-Preserving Learning: Differential privacy measures are incorporated during the evaluation phase. In addition to the normally trained pristine models, we have utilised OPACUS [18] to train models with differential privacy for propagation and evaluation to prevent privacy leakage. The evaluation scheduler coordinates the evaluation of individual model updates contributed by participants during each training round. Participants submit their differential privacy-enabled model updates, and the evaluation scheduler provides an incentive to the nodes who are participating in evaluating pending models. These security features safeguard data and model updates from unauthorised access, ensuring that sensitive information remains confidential throughout the DFL process.

SMPC Collaborative Model Aggregation: To make collaborative model aggregation possible while maintaining individual model privacy, SMPC protocols are integrated into the aggregation scheduler of the smart contract. SMPC enables nodes to jointly compute the aggregated model without revealing their respective model updates. Nodes securely collaborate to combine their encrypted model parameters, ensuring that the raw model parameters remain private throughout the aggregation process. By employing this innovative method, the blockchain-based DFL framework ensures a privacy-centric, secure, and collaborative environment for training language models while preserving user data confidentiality and fostering trust in the decentralised chatbot ecosystem. A detailed implementation of this key feature is explained next.

2.1 SMPC Implementation on the Ethereum Network

Figure 3 illustrates the SMPC implementation for the aggregation process. The aggregation scheduler securely combines these updates using SMPC, which allows individual model updates to be merged without revealing the model parameters, thus protecting the privacy of each participant's contribution. After the secure merging of model updates, the aggregation

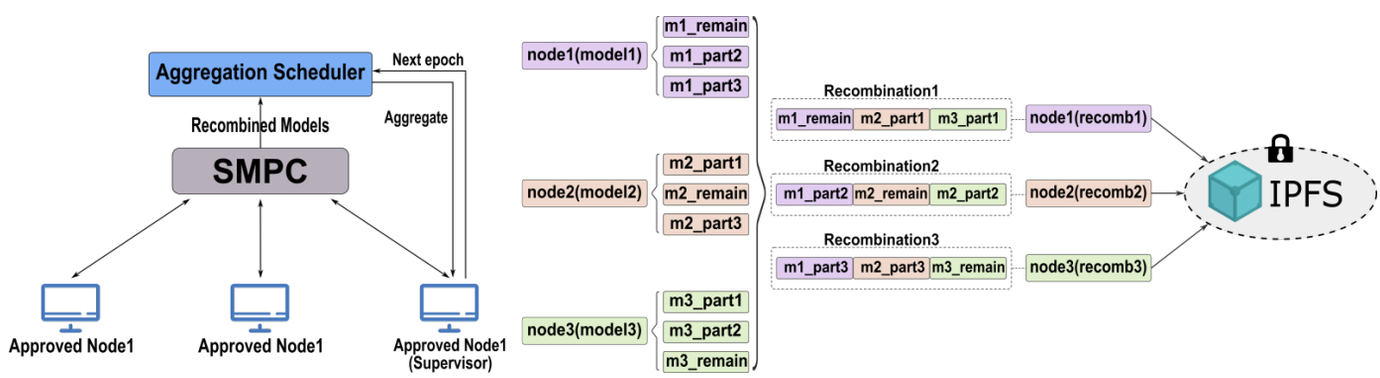


Figure 3. Aggregation scheduler of DFL using SMPC. Each node shares partial models with the other nodes, each of which is encrypted using the recipient node's public key for secure transmission, by uploading them onto the IPFS. Note that the partial model and the remaining model at each node when recombined constitute the original model. Each node now uses the partial models obtained from the other nodes and its own remaining model to recombine them. All these recombined models by the supervisor node, which is randomly chosen at each epoch, can now be securely averaged to get the averaged global model at the end of each aggregation phase. Since the partial models are securely shared with each node, the SMPC process allows averaging by distributing the data without revealing the model of any single node.

scheduler initiates the encryption of the final aggregated model. The aggregated model, which is encrypted for confidentiality, is stored in the IPFS, providing tamper-proof and immutable access for participants.

2.2 TinyLMs

TinyLMs are a viable solution in resource-constrained settings where deploying a large-scale language model (LLM) is impractical due to computational overhead. The process involves transforming an LLM into a more computationally feasible model while retaining its language processing capabilities through fine-tuning, distillation, and quantisation techniques.

Knowledge Distillation: Knowledge distillation is used to refine the TinyLM and compress it without a significant loss in performance. In this step, the fine-tuned LLM acts as a "teacher" model, providing soft target probabilities to guide the training of a smaller "student" model. The student model is trained to mimic the teacher's behaviour, thereby inheriting its language understanding capabilities. Through knowledge distillation, the student model effectively captures the essence of the LLM while reducing its size and complexity, resulting in a more lightweight TinyLM.

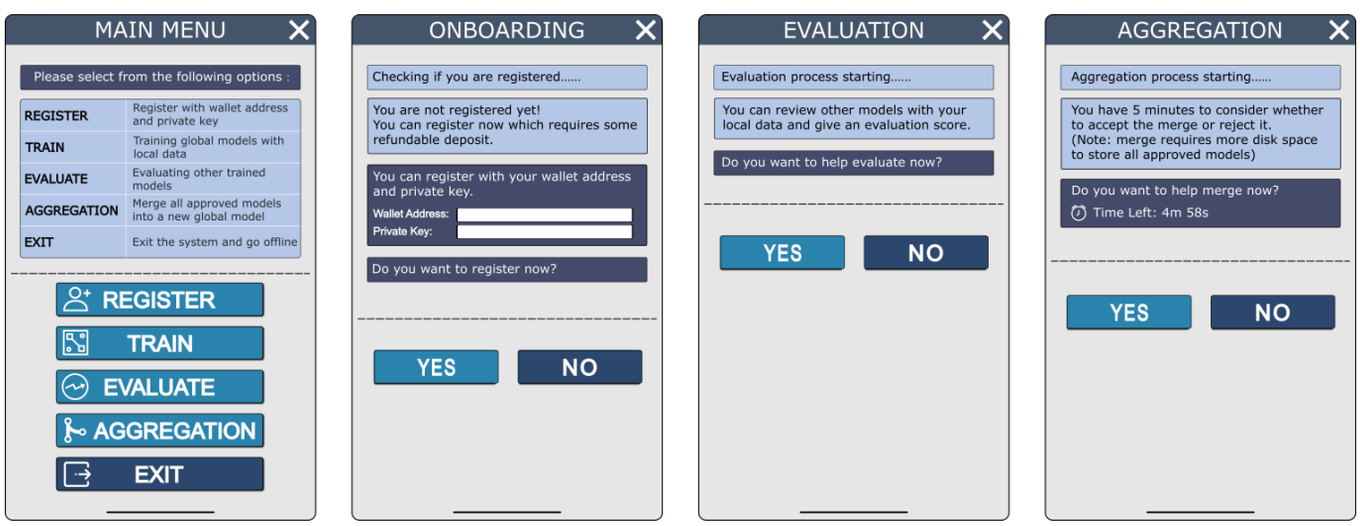


Figure 4. User interface.

Quantisation for Model Pruning: The next step in generating TinyLM is quantisation, which reduces the model's computational requirements even further. Quantisation converts the model's high-precision weights to lower precision, such as 8-bit integers. This significantly reduces the model's memory footprint and computational cost, making it more feasible to deploy on resource-constrained devices. Although quantisation may result in some loss of precision, the impact on performance is often minimal, ensuring that TinyLM can still provide contextually relevant responses for chatbot applications.

Fine-tuning the LLM: The final step in creating a TinyLM is to fine-tune a pre-trained LLM on a domain-specific dataset.

Fine-tuning the LLM allows the model to adapt to the target task by focussing on specific language patterns and contextual understanding relevant to the desired application [19]. This process helps tailor the LLM's vast language knowledge to the specific use case, making it more suitable for the intended application. A TinyLM can be generated from an LLM by fine-tuning, knowledge distillation, and quantisation. The TinyLM is tailored to a specific domain and pruned to a more computationally feasible size while retaining much of the language processing capabilities of its larger counterpart. This makes it well-suited for deployment in resource-constrained settings, enabling efficient and responsive chatbot interactions on a variety of devices with limited computational resources.

2.3 User Interface

To provide a seamless and interactive user experience within the decentralised chatbot ecosystem, we designed a user interface with four distinct modes of operation: Onboarding, Evaluation, Aggregation, and Exiting. These modes facilitate user engagement, incentivise active participation, and ensure timely model aggregation and updates (Figure 4). In the Onboarding stage, new users can join the decentralised chatbot network as participants or nodes. During this phase, users register their devices with a small fee, which contributes to the FL process. As new nodes onboard the network, they receive instructions for training their local models and contributing to collective learning.

The Evaluation stage encourages users to actively participate in evaluating the pending model updates contributed by others. When a node submits its model update, it enters a validation queue for evaluation by other nodes. Nodes evaluate these updates based on performance metrics, model accuracy, and privacy compliance. Evaluators who provide valuable and accurate feedback receive incentives in the form of tokens or rewards. This incentivises nodes to actively contribute to the evaluation process, fostering a collaborative and transparent environment.

The Aggregation stage is responsible for combining the validated model updates from different nodes using SMPC. To ensure timely aggregation, a random node is selected as the designated aggregator. If the chosen aggregator does not respond within a predefined time frame, the system automatically selects another node to perform the aggregation process. This dynamic selection mechanism helps maintain the efficiency and continuity of the model aggregation process.

In the Exiting mode, nodes have the option to leave the decentralised chatbot network while preserving their privacy and data ownership. When a node decides to exit, its local model updates and data are securely deleted from its system. This ensures that participants can retain control over their data and contribute to the FL process as they see fit.

By incorporating these four modes of operation in the user interface, the decentralised chatbot ecosystem encourages active participation, rewards valuable contributions, and ensures seamless model aggregation. The user interface fosters a decentralised and democratic environment, where all participants play a crucial role in the collective improvement of the chatbot's language capabilities while safeguarding their privacy and data

ownership.

3. Experimental Setup and Results

In this section, we present the experimental setup and results conducted to evaluate the performance and effectiveness of the proposed blockchain-based DFL framework, along with the generation of the TinyLM through fine-tuning, distillation, and quantisation processes. We deployed the DFL framework on the Ethereum blockchain using smart contracts to facilitate secure and privacy-preserving FL. Note that the DFL framework is agnostic to the model itself, and the experiments are to only showcase the efficacy of our DFL implementation.

We used the latest Falcon-7B LLM, which outperforms comparable open-source models (e.g., MPT-7B, StableLM, RedPajama, etc.) as witnessed on the OpenLLM leaderboard on the popular HuggingFace platform. It is a raw, pre-trained model, which should be further fine-tuned for most use cases. We chose the Open Orca-K16 dataset for our text summarisation task to fine-tune the LLM and the distilled model. The dataset contains pairs of input text and summary text.

For the generation of the TinyLM, we first employed knowledge distillation techniques [20] using the pre-trained LLM as the teacher model and a smaller but similar architecture as the student model on the Open Orca-K16 dataset. The student model was trained to mimic the teacher's behaviour by learning the value of its output logits, capturing its language understanding capabilities while reducing the model size significantly. Our code loads the test set, converts it into tokens, and then uses the ROUGE metric to evaluate the performance of the distilled model. The ROUGE precision score [21] (average of ROUGE-1, ROUGE-2, and ROUGEL scores) will provide an indication of how well the distilled model performs in comparison to the original teacher model. It is important to note that distilled models are typically expected to have slightly lower performance than their teacher models, but the student model is much faster and more efficient.

Quantisation was then applied to the distilled TinyLM to further compress the model's weights, achieving a more computationally feasible model without sacrificing performance (e.g., 8-bit integers instead of 32-bit floating-point numbers). In this work, we used relevant low-precision optimisers [22] and QLoRA [19] to obtain the fine-tuned quantised student model. Finally, this TinyLM is deployed using the DFL framework to give a further boost to the text summarisation performance on the Open Orca-K16 dataset.

3.1 DFL Evaluation Metrics

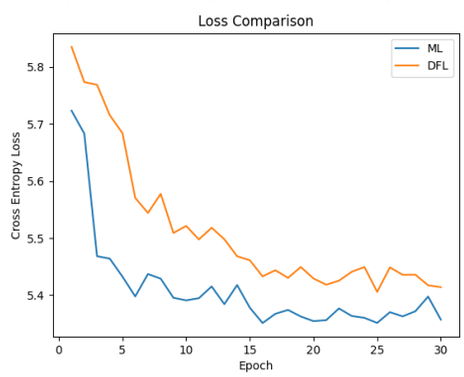
The distilled and quantised student TinyLM fine-tuning happens directly using the DFL framework. The TinyLM currently exhibits baseline proficiency in text summarisation tasks and a compact footprint that permits execution on standard end-user devices, such as a personal PC with a Graphics processing unit (GPU). The initial global model for five separate DFL nodes is established using the deployed TinyLM. These nodes possess private data for training, achieved by dividing the training dataset into five distinct segments, with each segment assigned to a respective node. Subsequently, each of these five nodes proceeds to conduct fine-tuning operations using its private data and subsequently evaluate the model's performance. The resulting fine-tuned private models are subjected to encrypted aggregation, facilitating the preservation of data privacy while also enabling parallel fine-tuning processes. This approach not only facilitates the utilisation of sensitive private data without compromising privacy but also harnesses individual computational resources to do the parallel training to expedite the model training process.

We evaluated the performance of the DFL framework using two metrics, including global model accuracy and training efficiency. The accuracy of the global model was assessed across multiple rounds of DFL using an independent test dataset and ultimately contrasted with the performance of a standalone TinyLM. This standalone TinyLM was trained normally without any FL, denoted as ML in the experiments, on the complete training dataset.

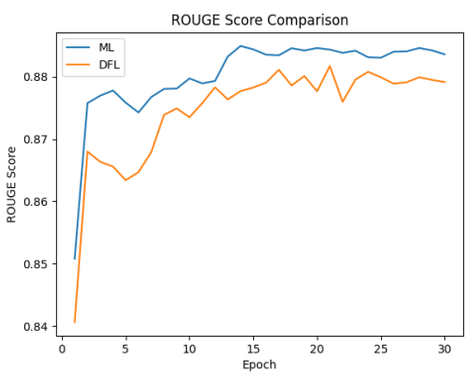
Secondly, as the DFL process splits the training burden across multiple nodes, it can potentially achieve faster convergence compared to a standalone ML model trained on the whole training dataset at a single machine. The DFL training efficiency was assessed by measuring the number of epochs needed to achieve the same performance using the TinyLM, with and without DFL, similar to the way the first metric is designed.

3.2 DFL Results

The size of the original Falcon-7b model was 14.43 GB, and the runtime GPU memory footprint was 26 GB. The size of the student model after knowledge distillation was just 700 MB, and the GPU memory footprint was 3.8 GB. After quantisation, the GPU memory footprint was further reduced to 3.0 GB. The final ROUGE scores of our TinyLM are: ROUGE-1-precision = 88.15%; ROUGE2-precision = 86.56%; ROUGE-L-precision = 88.06% using the first 20,000 samples from the Open Orca-K16 dataset. It is important to mention that we utilise a distinct portion of the dataset for quantisation and distillation. This decision is made to avoid redundancy in subsequent DFL processes. In summary, regarding the generation of the TinyLM, the fine-tuning and knowledge distillation processes yielded a student model that closely resembled the performance of the LLM while significantly reducing model size. The quantisation process further pruned the model, achieving a computationally efficient TinyLM suitable for deployment on resource-constrained devices. As mentioned earlier, the main contribution of the article is the DFL framework itself, and the model used is only for showcasing our successful implementation.



(a) Train/validation loss of the standalone ML model and DFL across the training rounds.



(b) The standalone ML and DFL model ROUGE precision scores on the test dataset across the epochs.

Figure 5. DFL results on the Open Orca-K16 dataset.

In our DFL experiments, we first filtered the dataset for very long input tokens and used part of the filtered dataset for training and the other part for testing with a ratio of 5:1 (this data was not the same one used for generating the TinyLM). We utilised 200,000 samples from the dataset for training and 40,000 samples for testing the standalone ML model and DFL. In our DFL experiments, we took a distribution of five nodes with an equal distribution of the training data. The ML training improved the ROUGE precision score of the TinyLM from 85.08% to 88.36%, while the DFL finally improved to 87.91%. Figure 5 depicts a comparison of the test loss change as well as the ROUGE precision score change, respectively. The results highlight the comparable training impact between DFL and standalone ML, a key outcome of this study. This underscores the successful functionality of our DFL implementation.

In addition to this, we also performed a comparison of the training efficiency of DFL and standalone ML. Under the premise of the same GPU (RTX A6000), each epoch of ML needs to process 200,000 samples, which takes about 55 minutes and 18.4 seconds; while a single node of DFL needs to process only 40,000 samples per epoch, which takes about 11 minutes and 9.3 seconds. Therefore, the time consumption is only 20.17% of that of ML, which is about the ratio of the total amount of data. Relevant to a real-world situation, since the GPUs used for DFL should theoretically have lower computational power than the GPUs used for ML, we arranged the DFL on a V100 GPU with lower computational power for the time computation. In this case, each epoch takes about 24 minutes and 30 seconds, which is only 44.30% of the time consumption of ML. This shows that DLF is more efficient compared to machine learning (ML) while having similar training capabilities.

The experimental results demonstrated the effectiveness of the DFL framework in collaboratively improving the language model. Through DFL, the chatbot's language capabilities were refined iteratively, resulting in enhanced model accuracy and contextually relevant responses. The results of our experiments highlight the potential of the proposed DFL framework in creating privacy-preserving and efficient TinyLMs. By leveraging blockchain technology and decentralised learning, the chatbot ecosystem can ensure user data privacy and foster trust among participants. Additionally, the generation of TinyLMs offers a practical solution for deploying language models on devices with limited computational resources, enabling efficient and responsive chatbot interactions in real-world scenarios.

4. Conclusion

Our article introduces a novel approach to address critical privacy and efficiency concerns in chatbot applications by harnessing the power of blockchain-based DFL and the generation of TinyLMs. Through the incorporation of SMPC within the Ethereum blockchain, we establish a secure and collaborative learning environment that preserves individual data privacy and fosters trust among participants. Additionally, by applying fine-tuning, knowledge distillation, and quantisation techniques, we successfully generated TinyLMs, significantly reducing the model size without compromising language processing capabilities. Our experiments demonstrate the efficacy of the proposed DFL framework and TinyLM generation, exhibiting similar model accuracy with much higher computational efficiency compared to standalone machine learning and real-world practicality.

The combination of decentralised learning and lightweight language models introduces new possibilities for efficient chatbot deployments on resource-constrained devices, offering privacy-preserving and responsive language interactions in diverse domains. By integrating SMPC and encryption methodologies, our research advances the development of secure, efficient, and user-centric language processing applications, promising a future of decentralised chatbot technology that safeguards user privacy and empowers individuals to take control of their data.

References

[1] G. Caldarini, S. Jaf, and K. McGarry, "A literature survey of recent advances in chatbots," Information, vol. 13, no. 1, p. 1: 41, 2022.

[2] A. Bahrini, M. Khamoshifar, H. Abbasimehr, R. J. Riggs, M. Esmaeili, R. M. Majdabadkohne, and M. Pasehvar, "Chatgpt: Applications, opportunities, and threats," in 2023 Systems and Information Engineering Design Symposium (SIEDS), 2023, pp. 274–279.

[3] J. Homolak, "Opportunities and risks of chatgpt in medicine, science, and academic publishing: A modern promethean dilemma," Croatian Medical Journal, vol. 64, no. 1, p. 1, 2023.

[4] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Artificial Intelligence and Statistics. PMLR, 2017, pp. 1273–1282.

[5] M. Liu, S. Ho, M. Wang, L. Gao, Y. Jin, and H. Zhang, "Federated learning meets natural language processing: A survey," arXiv preprint, 2021.

[6] L. Lyu, H. Yu, J. Zhao, and Q. Yang, Threats to Federated Learning. Cham: Springer International Publishing, 2020, pp. 3–16.

[7] H. Wu, B. Fang, C. Xiang, G. Cohen, A. van Schaik, and B. Ramesh, "Evolving neuromorphic systems on the ethereum smart contract platform," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain). IEEE, 2022, pp. 1–6.

[8] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial IoT," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5926–5937, 2020.

[9] C. Li, Q. Shen, C. Xiang, and B. Ramesh, "A trustless federated framework for decentralized and confidential deep learning," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain). IEEE, 2022, pp. 1–6.

[10] S. Aich, N. K. Sinai, S. Kumar, M. Ali, Y. R. Choi, M.-I. Joo, and H.-C. Kim, "Protecting personal healthcare record using blockchain & federated learning technologies," in 2022 24th International Conference on Advanced Communication Technology (ICACT). IEEE, 2022, pp. 109–112.

[11] Y. E. Oktian and S.-G. Lee, "Blockchain-based federated learning system: A survey on design choices," Sensors, vol. 23, no. 12, p. 5658, 2023.

[12] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXiv preprint arXiv:1407.3561, 2014.

[13] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 308–318.

[14] R.-H. Hsu, Y.-C. Wang, C.-I. Fan, B. Sun, T. Ban, T. Takahashi, T.-W. Wu, and S.-W. Kao, "A privacy-preserving federated learning system for android malware detection based on edge computing," in 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), 2020, pp. 128–136.

[15] A. S. Luccioni, S. Viguier, and A.-L. Ligozat, "Estimating the carbon footprint of bloom, a 176b parameter language model," arXiv preprint arXiv:2211.02001, 2022.

[16] X. Liu and Z. Liu, "Llms can understand encrypted prompt: Towards privacy-computing friendly transformers," arXiv preprint, 2023.

[17] P. Kaliamoorthi, A. Siddhant, E. Li, and M. Johnson, "Distilling large language models into tiny and effective students using pqrnn," arXiv preprint, 2021.

[18] A. Yousefpour, I. Shilov, A. Sablayrolles, D. Testuggine, K. Prasad, M. Malek, J. Nguyen, S. Ghosh, A. Bharadwaj, J. Zhao, G. Cormode, and I. Mironov, "Opacus: User-friendly differential privacy library in PyTorch," arXiv preprint arXiv:2109.12298, 2021.

[19] T. Dettmers, A. Pagnoni, A. Holtzman, and L. Zettlemoyer, "Qlora: Efficient finetuning of quantized llms," arXiv preprint arXiv:2305.14314, 2023.

[20] Y. Gu, L. Dong, F. Wei, and M. Huang, "Knowledge distillation of large language models," arXiv preprint arXiv:2306.08543, 2023.

[21] C.-Y. Lin, "Rouge: A package for automatic evaluation of summaries," in Text Summarization Branches Out, 2004, pp. 74–81.

[22] T. Dettmers, M. Lewis, S. Shleifer, and L. Zettlemoyer, "8-bit optimizers via block-wise quantization," 9th International Conference on Learning Representations, ICLR, 2022.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
BR is the main author for writing the manuscript and proofreading. SH collected the data and performed the experiments as supervised. XC co-supervised the project and provided timely feedback on a weekly basis.

Funding:
None declared.

Acknowledgements:
BR would like to acknowledge the efforts of Long Yinyun during the initial stages of the project in brainstorming sessions.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-7-1-(2)2024

Improving the Trustworthiness of Traceability Data in Food Supply Chain Using Blockchain and Trust Model

Oratile Leteane, Yirsaw Ayalew
University of Botswana, Gaborone, Botswana

Correspondence: 200808199@ub.ac.bw
Received: 19 December 2023 **Accepted:** 15 January 2024 **Published:** 16 February 2024

Abstract

The food supply chain is characterised by its complexity and interconnectedness, involving various actors, from farmers to consumers. It emphasises the critical importance of maintaining product integrity, safety, and quality throughout the process to meet stringent regulatory standards and consumer expectations. However, food supply chain is plagued by challenges such as counterfeiting, quality issues, and safety concerns, prompting the adoption of product traceability as a remedy. Current traceability systems (e.g., systems based on centralised and EPCIS architectures) aim to capture traceability data from the initial link to the final link in the supply chain, allowing for tracing a product from the end consumer back to its origin. Nevertheless, trust issues persist in these systems, particularly concerning the integrity and reliability of traceability data. Blockchain has been proposed to address these trust issues by creating an immutable and transparent ledger distributed across all peers. Despite this innovation, different studies underscore the inadequacy of relying solely on blockchain to ensure the trustworthiness of traceability data. This paper addresses this gap by proposing an adaptable and extensible framework that combines blockchain with a multi-trust packages-based trust model. The framework seeks to strengthen trust relationships among supply chain actors by improving the accuracy of identifying specific areas within the supply chain where compromises in quality and safety have occurred.

Keywords: *Traceability, Trust Metrics, Trust Score, Trust Package, Trust Package Smart Contract, Metrics Developer, Trust Model, Blockchain, Data Trust*
JEL Classifications: *D82, D85*

1. Introduction

Several scandals and recalls resulting from quality and safety compromise, as well as product counterfeiting, have been reported from supply chains around the world [1–4]. Many lives have been lost due to quality and safety compromise problems. For example, regarding food supply chains, the World Health Organisation reported that an estimated 600 million people become sick because of consuming food products and 420,000 end up dying [5]. This has resulted in many consumers losing trust in supply chains. To address this issue, several studies have suggested end-to-end traceability [6–8]. End-to-end traceability can provide an audit trail in the movement of a product in the supply chain [9], which helps detect quality and safety issues at the early stages of the supply chain [10]. It also makes product recalls to be managed systematically [11] and shortens the time taken to trace and pinpoint exactly where the product might have been compromised [12]. In food and pharmaceutical supply chains, many governments have taken the initiative to make traceability a legal obligation to protect consumers [13, 14].

To support traceability processes in supply chains, automated traceability systems are being used. These traceability systems can store traceability data in centralised repositories [15] or in repositories using distributed ledger technologies such as blockchain [16–19]. Centralised traceability systems provide non-tamper-proof data repositories. However, repositories whose data can be tampered with have data trust problems, as nothing stops the parties from tampering with the data to favour their interests [10]. Therefore, traceability systems based on a centralised approach fail to protect traceability data from the possibility of tampering [20, 21]. Although blockchain can provide tamper-proof repository, Powell et al. [20] argue that there exists a Garbage in Garbage Out (GIGO) problem with the blockchain approach. This is because blockchain does not have the capability to correct faulty and malicious data from the source to the ledger. To address the GIGO problem, Malik et al. [22], Dedeoglu et al. [21], and Al-Rakhami and Al-Mashari [23] proposed approaches that integrate blockchain and trust model, referred to in this study as blockchain + trust model approach. In this approach, the trust model's role is to establish trust in the ecosystem by computing the degree of trust (trust score) and associating the score with the network participants and data, while the blockchain provides tamper-proof repository. To develop trust models, trust metrics (TMs) are used. TMs are vital in determining whether a trust model accurately computes trust [24, 25].

In blockchain + trust model frameworks, a single set of TMs is used to quantify and compute trust scores. Using trust models that rely on a single TMs set to solve the trust problem is less effective because (1) as traceability data is generated by different data sources in different supply chain links, different sets of trust metrics are required to quantify trust values effectively; (2) whenever there are changes in the supply chain trust needs (e.g., new data produced in the supply chain), the framework's degree of accuracy in estimating trust score becomes low. This is because new trust requirements need different metrics to accurately compute trust. We agree with the views of other researchers that the problem can be solved by addressing the data trust problem [26, 8, 20, 21]. Therefore, our approach is to develop a framework that improves the end-to-end trustworthiness of traceability data by assessing the trustworthiness of traceability data and storing both data and associated trust values in a tamper-proof repository.

The remainder of this article is organised as follows: Section 2 discusses the existing traceability frameworks; Section 3 presents the proposed framework; Section 4 discusses the case study; Section 5 provides a

description of how trust metrics are developed; Section 6 presents the evaluation procedure for the framework; Section 7 discusses the limitations of this research, and Section 8 summarises the main points of the research and future work.

2. Related work

The literature presents several frameworks that attempt to address the problem of data trust. The frameworks can be categorised into three based on their architectural designs [8]. These include centralised [15, 27], blockchain [28], and blockchain + trust model [21].

In a centralised architecture, data from the supply chain is sent to a centralised repository mainly hosted in wide area networks. Some systems use one central repository, while others have distributed repositories. Electronic Product Code Information Service (EPCIS) is an example of a distributed centralised repositories network. EPCIS network has an extra repository called Discovery Service, whose function is to route the data requests from traceability applications to the right EPCIS data servers and re-route the queried data back to the requesting traceability applications. Central repositories are managed by intermediaries in the supply chain [29, 15]. Whenever traceability is needed, the central data repository is queried by traceability systems to acquire the data used for tracing the product. Traceability in this approach is solely dependent on the central data repositories. In all traceability systems based on a centralised architecture, intermediaries can tamper with the data and, hence, do not adequately address data trust issues in the supply chain [21, 22, 26, 48].

In blockchain architecture, traceability data from the supply chain is evaluated for validity by a consensus mechanism and, if valid, then passed into an immutable ledger. However, one of the drawbacks with the current blockchain consensus mechanism is that it cannot verify data veracity [20, 21]. The merits of this approach lie in the following: (1) there is a high level of transparency as nodes can always see data from other peers, which many researchers claim it encourages nodes to be honest. It should be noted that transparency is observed at different levels depending on the type of blockchain. In public blockchains, the same ledger is visible to all members; therefore, transparency is guaranteed to all members of the blockchain, while in consortium and private blockchains, transparency is at the group members level (those with common ledger). For example, in the Hyperledger Fabric consortium blockchain, transparency is limited to those within the same cluster. In this study, transparency is discussed in the context of consortium blockchains featuring a shared ledger among members; (2) immutability of data once in the ledger.

Different researchers have proposed frameworks using this architecture. To control the distribution of counterfeit products in pharmaceutical supply chains, Kumar and Tripathi [31] developed a traceability system that uses blockchain technology and quick response (QR) code. In their traceability system, the encrypted QR code consists of the details of the medicine that a pharmaceutical company manufactures, and the information is stored in the immutable ledger. In agri-food supply chains, Lin et al. [32] integrated blockchain and Long-Range Radio (LoRa) IoT-based architecture and demonstrated that minimising manual data entry by humans improves trust in food supply chains. A similar approach was also proposed by Tan, Gligor, and Ngah [33], who developed a traceability system using blockchain technology for tracing and confirming the authenticity of halal products. Similarly, Walmart piloted a blockchain traceability system on mango and pork supply chains, showing that traceability can be reduced from seven days to 2.2 seconds [19]. The blockchain approach provides the advantages of transparency, immutable ledger, and consensus mechanism that filter invalid data from entering the ledger. Since there is a lack of a mechanism to check the trustworthiness of the data before entering the ledger, the current blockchain is not sufficient to guarantee the trustworthiness of traceability data [8, 21, 22, 49]. This has also been observed by Powell et al. [20], who highlighted the GIGO problem.

To address the drawbacks highlighted in the blockchain-based approaches, blockchain + trust model approach has been proposed. The trust model is introduced to establish trust in the blockchain network so that both network nodes and data flowing into the network can be trusted to a certain degree. Trust and trustworthiness are two concepts used in the development of trust models. Trust is drawn from human life and, as Sagar et al. [24] highlighted, "It is a fundamental aspect of human life for building relationships with each other." Research in trust cuts across various disciplines, such as psychology [34, 35], sociology [36, 37], economics [38, 39], and computer science [40–46]. What is common in all the disciplines is that there is a trustor and trustee. The trustee makes a promise by sharing information, and the trustor accepts to rely on the information that the trustee will fulfil the promise. Computer science has multiple domains where the concept of trust is applied. These include software engineering [40], networking [41], data trust [42, 43], artificial intelligence [44], and web management [45, 46]. In these areas, trust is associated with the trustor and it is the behaviour displayed by the trustor based on the trustworthiness of the trustee. Thus, trustworthiness is a characteristic displayed by the trustee.

Our focus in this research is on addressing trust in traceability data for supply chains. Accordingly, trust models are built to mathematically quantify trustworthiness in a particular domain and context [47]. In the existing trust models, the quantified value is the measure of the trustworthiness of the trustee. It is mostly referred to as the trust score. Trust models typically normalise trust scores to fall between 0 and 1. 0 implies no trust at all, while 1 means full trust. Low trust values are those near 0, and high trust values are those near 1.

Few frameworks have been observed in the literature developed using this approach. These include Malik et al. [22], Al-Rakhami and Al-Mashari [23], Dedeoglu [21], and Rouhani and Deters [48]. Malik et al. [22] suggested trust metrics for generating trust scores that measure the level of quality and safety of the product. This means that a trust score close to 1 implies high quality and safety of the product. However, the framework does not adequately address the trust problem in traceability data. The IoT devices are vulnerable to data security compromise [60]. This is because: (1) the devices are heavily dependent on batteries for power supply, which makes them vulnerable to energy-depletion attacks [61]; (2) the devices have a limited amount of memory and processing power, incapable of running complex cryptographic security algorithms [62]. Since IoT devices are vulnerable to so many security attacks, there is no guarantee that the data from the devices used by the framework to calculate trust scores is not malicious.

Al-Rakhami and Al-Mashari [23] and Rouhani and Deters' [48] frameworks attempt to assess trust in the data using blockchain + trust model approach. The problem with the frameworks is the use of one set of trust metrics. A supply chain comprises a consortium that contributes to and records various traceability data for a product. The consortium uses diverse data sources and using one set of trust metrics by these frameworks is a bottleneck in accurately assessing the trustworthiness of traceability data. For example, if there is a supply chain link that uses GPS devices to send location data about a product and another supply chain link that uses temperature and humidity sensors to capture data about the environmental conditions of the perishable products storage, using a single set of trust metrics cannot accurately assess data from GPS devices and environmental condition sensory data. Thus, using one set of trust metrics is limited in computing accurate trust scores.

3. Adaptive and extensible framework

We propose the development of a framework which improves the trustworthiness of traceability data across all the links of a supply chain. The framework uses different packages of TMs to quantify trust into numerical values. Figure 1 shows the different components of the

framework. These include trust model, ledgers, access management, metrics management module, application management module, supply chain and metrics developers.

The trust model comprises two smart contracts: metrics selection smart contract and trust computation smart contract. Overall, the trust model evaluates the data produced by data sources found in the supply chain links to check its validity in terms of trust. The trust model then computes trust scores and sends data and computed trust scores to the blockchain ledger. The trust model uses the metrics selection smart contract to select an appropriate trust package developed for trust assessment of the generated data. Trust packages refer to a set of TMs and the instructions on how they are used to establish trust. The metrics selection smart contract is triggered when an application sends data from the data generator to the blockchain. Trust computation smart contract uses the trust package to compute trust and send the data and trust score to the ledger. The data repositories consist of two main ledgers: the metrics ledger shaded green and the base ledger shaded grey. The base ledger stores traceability data and trust scores. This protects data and trust scores from tampering. Metrics ledger, on the other hand, stores different trust packages. TMs are protected in the ledger because of their criticality for accurately assessing trust scores. Metrics developers continuously assess the effectiveness of existing trust packages, and if some are seen to be less effective, then they develop new trust packages to replace them. Also, if new data generators generate data that none of the existing packages can assess for trust, then metrics developers develop trust packages to address those trust needs. This makes the framework to be more effective and relevant. The application module provides an interface between the blockchain ledger and end-user applications. Traceability systems used by end users will communicate load traceability data from the ledger by interacting with this module.

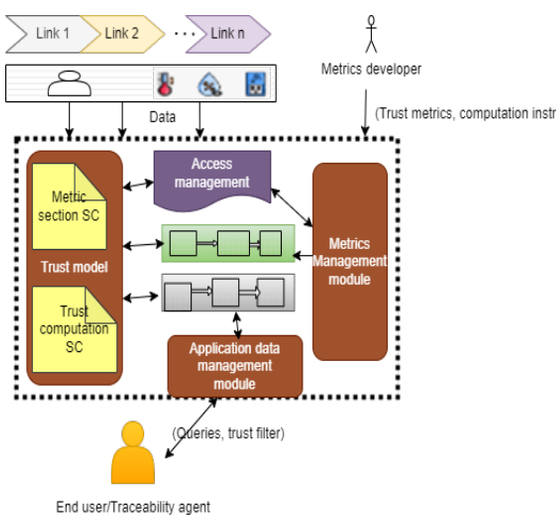


Figure 1. Framework for enhancing trust in supply chain links. Adapted from [25].

The supply chain is plugged into the framework, and data generators are available to generate data from traceability units and send it to the blockchain network. Data generators[1] may involve manual entry by a human being who observes the product, or it can be an autonomous set-up where various sensors transmit data to the network. Metrics developers are members of the consortium whose sole responsibility is to provide the framework with appropriate trust packages for efficient computation of trust scores. This helps the framework to be up to date in accurately computing trust scores.

4. Case study

Botswana beef supply chain is chosen as a case study. The two farming methods practised at the farm link are free range and ranched. About 90% of farmers practise free range [50]. In terms of quantity and quality, Botswana is the biggest supplier of beef to the European Union (EU) from the African region [51]. While the Botswana beef supply chain is one of the top exporters of high-grade cattle meat from the continent [52], an audit by Engelen et al. [50] highlighted issues related to data trust. Due to traceability data trust, the country was temporarily banned from exporting to the EU [50] and, in 2023, lost one of the lucrative markets in Norway [53].

Beef supply chain links have been identified from the Botswana Agri-food Value Chain Project [50] and attached to the framework as an off-chain pluggable component. Figure 2 shows the links extracted from the report. The Botswana beef supply chain currently uses a centralised traceability system called Botswana Animal Identification and Traceability System (BAITS) [54, 55].

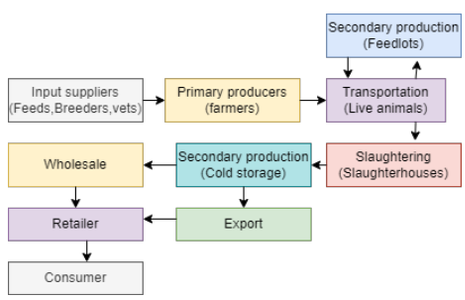


Figure 2. Product transformation links in Botswana beef supply chain.

5. Trust packages development

We used the guidelines provided by Leteane and Ayalew [25] to identify trust metrics and use them to develop trust packages for the Botswana beef supply chain. For demonstration purposes, trust packages for farm and cold room links are developed.

5.1 Trust at the farm link

Trust issues mainly emerge from free-range farming because it is difficult to monitor the location of the cattle. Botswana has different zones to identify areas affected by diseases such as foot and mouth disease (FMD). One of the major requirements of the EU market is that all meat products should be coming from disease-free zones. Assuring the markets that the cattle come from free-range farming has never passed through the FMD zones remains a big challenge. Collecting real-time data of cattle movement using IoT devices in this supply chain would be ideal. Nevertheless, the integrity and truthiness of the data from IoT devices could be compromised, resulting in data trust problems. Therefore, it is important to develop a trust package that the framework can use to enhance trust in the data coming from the cattle using IoT devices.

The location of cattle data is collected from a GPS device. The devices are attached to the cattle and continually send GPS coordinates to the blockchain network through the internet. In the above data source, where IoT devices generate the data, there is a correlation between data quality and trust. Therefore, data trust issues may arise from what Byabazaire, O'Hare and Delaney [56] identify as intrinsic data quality dimensions. The dimensions include problems associated with data quality and integrity, provenance, and abnormality. While we acknowledge that all the dimensions must be addressed for data trust to be enhanced, data trust is broader, and quality does not always mean trust. Since existing approaches can be used to enhance data quality, we focus on the metric that improves trust in the data. The following factors are identified to help extract the

trust metrics: (1) device malfunction (hardware and software) – we argue that a device with valid calibration is likely to generate correct data; (2) data tampering – IoT devices are known to have limited security features and are vulnerable to data attacks. For example, a node in the network can change its behaviour to become an adversary and try to inject malicious data into the ledger. This kind of attack can be addressed by both temporal and spatial sensory data correlation and by evaluating the trust score of the data item. In the free-range farming set-up where cattle can go astray and graze on their own, there are challenges with spatial data as there will be reliance on one sensor. Temporal correlation of time series data is likely to evaluate and provide high accuracy of trust in this scenario; (3) the battery problems (low battery or high power consumption) – devices with low battery are likely to generate faulty data, and devices with high power consumption are likely to be malicious [57]. This can be addressed by monitoring the battery level and usage. Thus, to compute the trust values of data from IoT devices, device calibration, battery level and consumption, and temporal correlation are used as TMs.

Device calibration: To quantify trust for device calibration trust metrics, a value of 1 is assigned if the device is calibrated; otherwise, a value of 0 is assigned, as shown in Equation (1).

$$T_v = \begin{cases} 0, & if\ not\ calibrated\ or\ date\ expired \\ 1, & Calibrated \end{cases} \quad (1)$$

Battery level and consumption: When the battery level goes below some threshold, the likelihood of the device producing correct data becomes low [57]. Also, malicious nodes are known to consume more energy than usual. Therefore, we chose energy level and consumption as one of the trust metrics of the data coming from IoT devices. We use two thresholds as follows: α = maximum energy consumption. Any node consuming energy above this threshold is considered malicious and produce untrustworthy data; ρ = minimum energy level. A device whose energy level is lower than ρ is considered to produce erroneous data that cannot be trusted. Like in [57], 5% is reasonable ρ. However, the appropriate threshold value can be chosen based on the application use case. The rate of consumption ΔE and energy level E_c are computed as:

$$E_c = E_{t+1} \quad (2)$$

$$\Delta E = E_t - E_{t+1} \quad (3)$$

Where $E_c < \rho \Rightarrow$ incorrect data produced and $\Delta E > \alpha \Rightarrow$ energy level trust value $T_e = 0$.

In Equation (4), we quantify the energy trust metrics using both E_c and ΔE to produce trust value as follows:

$$T_e = \begin{cases} 0, & if\ \ E_c < \rho\ or\ \Delta E > \alpha \\ 1, & Otherwise \end{cases}$$

Temporal correlation: Due to the movement of cattle, there is a gradual change in location data. As in [58], temporal features of the location data over time are used in changing the TMs to numerical values. The GPS sensor provides data as latitudes and longitudes. To use these latitudes and longitudes for estimating distance, we use Haversine's formula as in Equation (5). Let's denote the distance between two points (previous and current position) to be Ry. We use average deviation to compute distance deviation tolerance.

$$R_y = 2 \times R \times sin^{-1}\left(\sqrt{sin^2(\emptyset_2 - \emptyset_1) + cos(\emptyset_1) \times cos(\emptyset_2) \times sin^2(\Psi_2 - \Psi_1)}\right) \quad (5)$$

where R represents the earth's radius, $\emptyset_1$ and $\emptyset_2$ represent latitudes, $\Psi 1$ and $\Psi 2$ represent the longitudes.

To determine whether the data is trusted or not, we use the average deviation, like Zhang [59]. After calculating the distance covered, we determine the tolerance value range. The tolerance value range is used to determine the trust value. To determine the tolerance value, we look at the latest normal behaviour of the cattle movement. We consider five days of normal behaviour data and use it to define the tolerance value range. Five days is chosen to use just enough data to observe general distance coverage daily. We limit history data to five days since using large data covering more than five days can affect the efficiency of the framework by taking a long time to process data. On the other hand, using less data covering less than five days may not give the accurate behaviour of cattle movement. Let D represent the normal behaviour data for five consecutive days. The average of distances covered within a fixed defined time duration in D is R_0, and the degree of deviation of each distance is δ. If the degree of deviation $\delta_i > 0$, then an outlier exists that can be used to estimate the degree of trust in the incoming data.

$$R_0 = (R_1 + R_2 + R_3 + \ldots + R_n)/n \quad (6)$$

In Equation (6), there are *n* positions, and the *n*th position is represented by R*n*. The deviation in the movement of cattle is calculated as follows:

$$\lambda_i = |R_y - R_0|\ i = 1,2,\ldots,n \quad (7)$$

In this formula, sample data is represented as Ry. The deviation in the expected distance of coverage is:

$$\delta_i = \lambda_i / R_0 \quad (8)$$

Next, we calculate the average sum of deviations from the previous samples. This gives us the approximate deviation of every sample. Thus, every deviation is expected to be close to the average degree of deviation. The average deviation and average coverage distance are used to set the tolerance threshold. The tolerance value is calculated using Equations (9) and (10):

$$\Delta = \sum \frac{\delta_i}{n} \quad (9)$$

$$\eta = \Delta \times R_0 \quad (10)$$

We then check whether the incoming radius of coverage falls within the range of ($R_{0-\eta}$, $R_0 + \eta$). If the radius falls within the range, then the trust score Tc for the metrics is considered high and falls within the range $50 < Ts < 100$. Otherwise, the trust score is low and falls in the $0 < Tc < 50$ range. Hence, we qualify the data set as trusted if the trust score is 0.5 or higher and not trusted if it is below 0.5. Tc is calculated as:

$$T_c = \begin{cases} 1 & if\ \lambda = 0 \\ 1 - \delta\ if\ \lambda > 0\ and\ R_0 - \eta \le \lambda \le R_0 + \eta \\ 0.5 \times \delta & Otherwise \end{cases} \quad (11)$$

The total trust score (Ts) represents the total trust score aggregated from all three TMs of the location. The choice of aggregation technique is determined by metrics developers based on the technique that gives better accuracy.

A weighted sum is chosen in this case for demonstration, as shown in Equation (12). Equation (5) gives the actual distance of coverage between two positions over a time window. The time window is defined at the time of sensor configuration.

$$T_s = w_1 T_v + w_2 T_e + w_3 T_c, w_1 + w_2 + w_3 = 1 \quad (12)$$

where w_1, w_2, and w_3 are weights of each TM. The weights are assigned based on the importance of the TM to the overall trust score.

5.2 Trust at the cold room links

IoT temperature and humidity sensors are used to collect and forward the data to the framework. Here, we are interested in ensuring that the data represents the actual condition of the environment where the product is stored. Unlike in location data, sensors are not mobile. However, the first two trust metrics from the previous section remain important as sensors depend on battery and correct calibration to provide trusted data. Thus, we use the battery management and calibration metrics again. According to Karthik and Ananthanarayana [57], a correlation exists between data from a sensor and data from neighbouring sensors. We consider the spatial correlation of the sensory data from all the sensors in the same room. It is suggested that multiple similar sensors be used in the same room to collect the same environmental condition data [43]. The expectation is that the data generated by the sensors must be almost the same. A correlation coefficient of data from all the sensors in the cluster observing the same phenomena is calculated and used to represent the trust score. Equation (15) is used to compute the trust score for spatial correlation of data. Let $\boldsymbol{Sen_i}$ be a sensor in a room with a set of $\boldsymbol{S}$ sensors measuring the same phenomena, in this case, temperature. Then, we calculate the mean as:

$$\mu = \frac{\sum_{i=1}^{n} sen_i}{n}, \forall sen_i \in \boldsymbol{s} \quad (13)$$

and the deviation of the sensory data as:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(sen_i - \mu)^2} \quad (14)$$

The trust score is given by subtracting the correlation coefficient from the possible highest trust score:

$$T_{sp} = 1 - \left(\frac{\sigma}{\mu}\right) \quad (15)$$

Like in the previous package, a weighted sum is used to aggregate all trust scores from the metrics to compute the total trust score. Thus,

$$Total\_trust_{cold} = \alpha T_{corr} + \beta T_{sp} + \gamma T_{Batt}, \alpha + \beta + \gamma = 1 \quad (16)$$

ALGORITHM 1 BATTERY LEVEL

Input: *Battery*$_{level}$
Output: *Battery*$_{trustscore}$
Battery$_{thrsd} \leftarrow 0.05$
if *(Battery*$_{level} \leq$ *Battery*$_{thrsd}$*)* ***&*** *(consumption* $\leq \theta$*)* ***then***
  TS$_{bat} \leftarrow 1$
else
  if *(Battery*$_{level} \geq$ *Battery*$_{thrsd}$*)* ***&*** *(consumption*$_{rate} \leq \theta$*)* ***||*** *(Battery*$_{level} \leq$ *Battery*$_{thrsd}$*)* ***&*** *(consumption*$_{rate} \leq \theta$*)* ***then***
    TS$_{bat} \leftarrow 0$
  else
    TS$_{bat} \leftarrow 1 -$ *Battery*$_{level}$
  end if
end if
return *TS*$_{bat}$

5.3 Developing trust packages smart contracts

Each trust package is added to the framework as a special smart contract called trust package smart contract (TPSC). Four algorithms are provided below and used by the TPSC to quantify and compute trust from data coming from supply chain links. The sensor collects environment data and proposes the transaction to the blockchain. Algorithm 1 is used by TPSC when data is sent from the supply chain to the framework. TPSC uses algorithm 1 to compute the trust score for battery-level trust metrics. The computation is based on Equations (2)–(4). Algorithm 2 computes trust score for the calibration trust metrics. TPSC uses the algorithm to get the trust score for the metrics and is used in computing the total trust score for the data. TPSC also uses algorithm 3 to compute trust score for temporal correlation metrics. The algorithm uses Equations (5)–(11) to compute the trust score. Then, TPSC uses Equation (12) to compute the trustworthiness of the location data. The sensor triggers the appropriate TPSC for computing the trust score for the data and passes the data together with the trust score to the ledger. Algorithms 1–3 use Equations (1)–(12) to compute the trust score.

ALGORITHM 2 CALIBRATION_DATA

Input: *Validation expiry date*
Output: *Total trust score for calibration (TS_cal)*
if *validation expiry date* $\leq$ ***today then***
  calibration$_{valid} \leftarrow$ ***TRUE***
else
  calibration$_{valid} \leftarrow$ ***FALSE***
End if
If *calibration*$_{valid} =$ ***TRUE then***
  TS_cal $\leftarrow 1$
else
  TS_cal $\leftarrow 0$
End if
Return *TS_cal*

The trust package that computes the trust score of the data from the GPS data source in the farm link uses algorithms 1–3. The TPSC takes the quantified trust metrics values and uses weighted sum aggregation to compute the final trust score for the data. The trust score is then passed to the smart contract that writes the data and trust score to the blockchain ledger. Algorithm 4, on the other hand, is used by the TPSC to compute the trust score for the data coming from cold storage links. When the sensors send environmental condition data, it triggers the appropriate TPSC smart contract to execute. The TPSC then uses algorithm 4 and returns the trust score written with data to the blockchain ledger.

ALGORITHM 3 TEMPORAL CORRELATION TRUST SCORE

Input: *PosLat, PrevLat, PosLong, PrevLong, PrePos (latitudes and longitudes of previous and current positions)*
Output: *Total trust score based on data temporal correlation*
R $\leftarrow$ *6371 // Radius of the earth as a constant*
Sleepdur $\leftarrow$ *720 (maximum time in minutes of no movement)*
if *(PosLat = PrevLat) &* *(PosLong = PrevLong)* ***then***
  Total trust score $\leftarrow 0$
else
  dlat $\leftarrow$ *|PosLat − PrevLat|*
  dlon $\leftarrow$ *|PosLong − PrevLong|*
  coverage$_{Radius} \leftarrow$ *sine(dlat/2)*^{2} + *cosine(PrevLat)* $\times$ *cosine(PosLat)* $\times$ *sine(dlon/2)*^{2}
  Actual$_{distance} \leftarrow$ *(2R* $\times$ *sine*$^{-1}\left(\sqrt{coverage_{Radius}}\right)$
  Prev$_{Averages} \leftarrow \frac{\sum_{i=1}^{5} ave\_d_i}{5}$
  Deviation $\leftarrow$ *|Actualdistance – PrevAverages|*
  if *Deviation = 0* ***then***
    trust score $\leftarrow 1$
  else
    deviation$_{degree} \leftarrow \frac{Deviation}{Prev_{Averages}}$

16 $Average_{deviations} \leftarrow \frac{\sum_{j=1}^{5} dailyDeviation_j}{5}$
17 $tolC \leftarrow Average_{deviation} + Prev_{Averages}$ //(maximum tolerance)
18 $tolF \leftarrow |Average_{deviation} - Prev_{Averages}|$ //(minimum tolerance)
19 **if** $(deviation_{degree} \geq TolC)$ **&** $(deviation_{degree} \leq tolF)$ **then**
20 $Trust\_score = 1 - deviation_{degree}$
21 **else**
22 $trust\ score = 0.5 - deviation_{degree}$
23 **End if**
24 **End if**
25 **End if**
26 **Return** *trust_score*

5.4 Adding trust packages to the framework

After a trust package is developed, it must be accepted in the network by all affected supply chain actors for it to be used in the framework. The acceptance process is initiated by the metrics developer who wants the developed trust package to be used. If the package is accepted, then the metrics developer packages the accepted trust package as TPSC and adds it to the blockchain network.

ALGORITHM 4 TEMPERATURE DATA TRUST PACKAGE

Input: *Temperature and battery level data*
Output: *Total trust score for the cold room data*

1 $\mu \leftarrow \frac{\sum_{i=1}^{n} \boldsymbol{temp\_dataset_i}}{\boldsymbol{tem\_dataset.size}}$
2 $div \leftarrow \sqrt{\frac{1}{n}\sum_{i=1}^{n}(sen_i - \mu)^2}$
3 $corr_{coef} \leftarrow \frac{div}{\mu}$
4 $Trust_{spatial} \leftarrow 1 - corr_{coef}$
5 **if** $(Battery_{level} \geq Battery_{thrsd})$ & $(consumption\_rate \geq \theta)$ **then**
6 $TS_{bat} \leftarrow 1$
7 **else**
8 **if** $(Battery_{level} \geq Battery_{thrsd})$ **&** $(consumption\_rate \leq \theta)$ // $(Battery_{level} \leq Battery_{thrsd})$ **&** $(consumption\_rate \leq \theta)$ **then**
9 $TSbat \leftarrow 0$
10 **else**
11 $TS_{bat} \leftarrow 1 - Battery_{level}$
12 **End if**
13 **End if**
14 **if** $calibration_{valid} =$ ***TRUE then***
15 $TS\_cal \leftarrow 1$
16 **else**
17 $TS\_cal \leftarrow 0$
18 **End if**
19 $Trust_{cold} \leftarrow \frac{Trust_{spatial} + TS_{bat} + TS\_cal}{3}$
20 **Return** $Trust_{cold}$

The cluster members accept the smart contract into the network. All the data from the supply chain is then proposed through the organisation's peer. The peer then selects and triggers the appropriate TPSC to compute the trust score. The metrics developers may now be given some incentives for successfully providing a useful trust package. However, the mechanism of providing incentives is outside the scope of this paper.

6. The development of the framework

We chose the Hyperledger Fabric blockchain platform. One key advantage is its modular architecture, allowing flexibility and customisation to meet diverse business requirements. Additionally, Hyperledger Fabric ensures enhanced privacy and permissioned access, making it well-suited for enterprise use, especially in industries where data confidentiality and fine-grained control over permissions are crucial. Its support for smart contracts and a pluggable consensus mechanism further contributes to its appeal for building the framework. As shown in Figure 3, data flows from the supply chain through the internet into the framework. Since the cattle being monitored are mobile, we recommend building a LoRaWAN network and attaching the LoRa end devices that sense and communicate

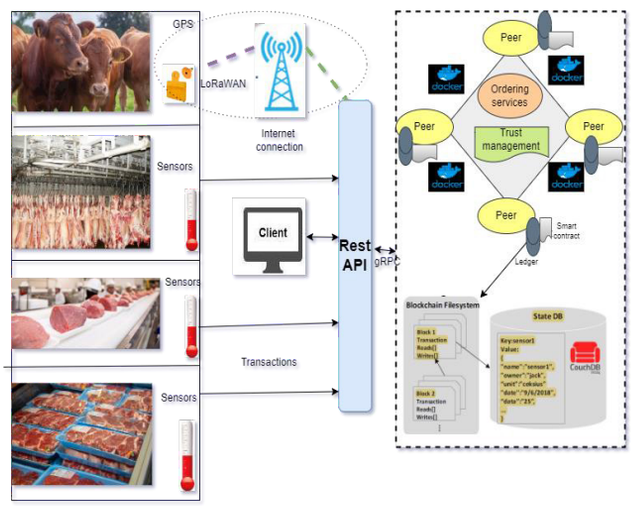


Figure 3. Implementation procedure.

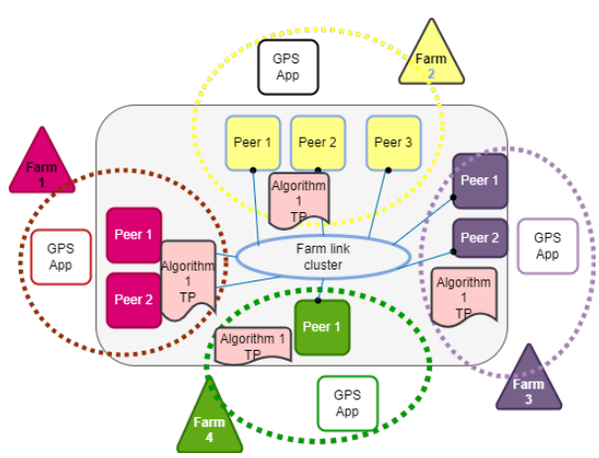


Figure 4. The farm link cluster.

GPS coordinates. In areas where there is no internet coverage, the gateway can communicate with the blockchain network through a GSM network. The LoRaWAN gateway will then redirect the data to the blockchain network, where the endorsement process will start. The fabric gateway will propose a transaction by sending the proposal to appropriate peers for endorsement signatures. The network set-up for the farm link cluster is shown in Figure 4. The procedure for adding location data to the ledger is as follows: the GPS data application proposes the transaction once the data is collected from the environment by connecting to the appropriate peers. The phases starting with the endorsement to the commitment of the block to the ledger are followed. In this case, when data is proposed to be added to the ledger, the triggered trust package smart contract is the one that uses algorithms 1–3. All data from a GPS sensor in the farm link will trigger this smart contract. Organisations in the cold room link also form a cluster in the blockchain network. Similarly, applications from

temperature and humidity sensors propose transactions by sharing the proposal with appropriate peers for endorsement, ordering service, and then committing peers. In this cluster, endorsing and committing peers compute trust score by engaging trust package smart contract that uses algorithm 4. It is important to note that trust package smart contracts used in this cluster are different from those used in the farm link cluster, hence our idea of the use of multi-trust package to improve trust in traceability data in the supply chain.

7. Limitations of the study

Most farmers rear their cattle in rural areas where there is no internet coverage, limited network infrastructures, and no power supply grid. This poses a challenge in collecting real-time data on the correct movement and positions of the animals using network devices. An option to address this challenge is to build the infrastructure from scratch. Developing economies still face financial constraints to develop such infrastructure, hence low-power wireless area networks (LPWAN) are considered to be the most appropriate options. To address the challenge in our case study, we considered building LoRaWAN network with just a single gateway and 14 end devices to collect real-time data from the farm link. To tackle the power issue, solar panels will be utilised to supply power to the gateway.

To collect the data, LoRa end devices are attached to the cattle's neck. An adversary can potentially penalise the farmer by disconnecting the devices from the cattle and allowing them to enter the FMD zone. In this case, the data in our framework, which may be rated highly trusted, may not be true about the cattle. However, an approach proposed in [63] can be used to prevent the detaching of the LoRa end devices from live animal's neck. It can also be argued that an untrusted farmer may not attach the devices to the cattle but rather give them to herd boys or moving objects and still allow the cattle to graze in the FMD zones while our framework receives false data on the animal's location. The farmer can then attach the devices when it is time to take the cattle to the abattoir, where the data in our framework will perhaps suggest with a high degree of trust that the cattle has never grazed in the FMD zones. While this is a limitation in our case study, alternative devices such as rumen boluses with embedded RFID microchips can be used as end devices. The device is planted in the stomach of a cattle and starts sending signals to the gateway from the stomach [64]. The device is only removed when the cattle are slaughtered at the abattoir.

Another challenge in our framework is developing trust metrics to detect false data entered by a human being. A way around this is to limit human data entry using IoT devices. Thus, in the current implementation, our framework can evaluate trustworthiness of the data only from IoT devices. However, it should be noted that our framework has metrics developers whose sole responsibility in the network is to develop and provide trust packages. While trust packages that can detect the trustworthiness of data from manual entry seem to be far-fetched at the moment, we believe that with time, metrics developers may come up with such trust packages.

8. Conclusion

Current traceability frameworks do not adequately address issues of trustworthiness of the data. This makes it difficult to convince consumers that the traceability data represents the truth about the condition of the product they purchase for consumption. As a result, consumers lose trust in the quality and safety of products from supply chains. Our approach presented a framework that improves trust in traceability data by integrating blockchain with a trust model. We demonstrated how blockchain and trust model can be integrated in developing an adaptive and extensible framework. The use of blockchain ledger as a repository guarantees that no actor can tamper with the data to their favour at any time.

Our future work will focus on the evaluation of the framework and develop an incentive mechanism that can be used to reward metrics developers.

References

[1] S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, and D. Masouras, "A review and classification framework of traceability approaches for identifying product supply chain counterfeiting," Sustainability, vol. 14, no. 11, 6666, 2022.

[2] P. Danese, R. Mocellin, and P. Romano, "Designing blockchain systems to prevent counterfeiting in wine supply chains: A multiple-case study," International Journal of Operations & Production Management, vol. 41, no. 13, pp. 1–33, 2021.

[3] E. R. Blickem, J. W. Bell, D. M. Baumgartel, and J. Debeer, "Review and analysis of tuna recalls in the United States, 2002 through 2020," Journal of Food Protection, vol. 85, no. 1, pp. 60–72, 2022.

[4] W. Wu, A. Zhang, R. D. van Klinken, P. Schrobback, and J. M. Muller, "Consumer trust in food and the food system: A critical review," Foods, vol. 10, no. 10, 2021.

[5] The World Health Organisation, "Food safety," 2020. Available at https://www.who.int/news-room/fact-sheets/detail/food-safety.

[6] P. Jahanbin, The investigation of blockchain and IoT integration for designing trust-driver information systems in agricultural food supply chain. PhD thesis, The University of Canterbury, Christchurch, New Zealand, June 2022. Available at https://ir.canterbury.ac.nz/server/api/core/bitstreams/f4fa19ea-a083-4807-af9a-3bcf8123810c content.

[7] R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: Implications for operations and supply chain management," Supply Chain Management: An International Journal, vol. 24, no. 4, pp. 469–483, 2019.

[8] O. Leteane, Y. Ayalew, and T. Motshegwa, "A systematic review of traceability issues in beef supply chain management," in 2021 IEEE International Conference on Big Data (Big Data), pp. 3426–3435, IEEE, 2021.

[9] G. Alfian, M. Syafrudin, N. L. Fitriyani, J. Rhee, M. R. Ma'arif, and I. Riadi, "Traceability system using IoT and forecasting model for food supply chain," in 2020 International Conference on Decision Aid Sciences and Application (DASA), pp. 903–907, IEEE, 2020.

[10] F. Tian, "An agri-food supply chain traceability system for China based on RFID blockchain technology," in 2016 13th international conference on service systems and service management (ICSSSM), pp. 1–6, IEEE, 2016.

[11] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," Computers Industrial Engineering, vol. 154, p. 107130, 2021.

[12] L. C. H. Ghadafi, M. Razak, and M. Stevenson, "Supply chain traceability: A review of the benefits and its relationship with supply chain resilience," Production Planning & Control, vol. 34, no. 11, pp. 1114–1134, 2023.

[13] F. Fung, H.-S. Wang, and S. Menon, "Food safety in the 21st century," Biomedical Journal, vol. 41, no. 2, pp. 88–95, 2018.

[14] European Commission, "Regulation EC No 178/2002." https://eurlex.europa.eu/eli/reg/2002/178/oj, 2004.

[15] J. Feng, Z. Fu, Z. Wang, M. Xu, and X. Zhang, "Development and evaluation on a RFID-based traceability system for cattle/beef quality safety in China," Food Control, vol. 31, no. 2, pp. 314–325, 2013.

[16] R. Garrard and S. Fielke, "Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry," Technology in Society, vol. 62, p. 101298, 2020.

[17] S. Cao, W. Powell, M. Foth, V. Natanelov, T. Miller, and U. Dulleck, "Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism," Computers and Electronics in Agriculture, vol. 180, p. 105886, 2021.

[18] K. M. Botcha, V. V. Chakravarthy, and Anurag, "Enhancing traceability in pharmaceutical supply chain using internet of things (IoT) and blockchain," in 2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT), pp. 45–453, 2019.

[19] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," The Journal of the British Blockchain Association, vol. 1, no. 1, p. 3712, 2018.

[20] W. Powell, M. Foth, S. Cao, and V. Natanelov, "Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains," Journal of Industrial Information Integration, p. 100261, 2021.

[21] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 190–199, 2019.

[22] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and IoT supported supply chains," in 2019 IEEE International Conference on Blockchain (Blockchain), pp. 184–193, IEEE, 2019.

[23] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the internet of things supply chain management," Sensors, vol. 21, no. 5, p. 1759, 2021.
[24] S. Sagar, A. Mahmood, Q. Z. Sheng, J. K. Pabani, and W. E. Zhang, "Understanding the trustworthiness management in the social internet of things: A survey," arXiv preprint arXiv:2202.03624, 2022.
[25] O. Leteane and Y. Ayalew, "An adaptive and extensible framework to enhance end to end trustworthiness of traceability data," in 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA), pp. 1–8, IEEE, 2022.
[26] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain internet of things," in 2017 International Conference on Service Systems and Service Management, pp. 1–6, IEEE, 2017.
[27] M. Thakur and E. Foras, "EPCIS based online temperature monitoring and traceability in a cold meat chain," Computers and Electronics in Agriculture, vol. 117, pp. 22–30, 2015.
[28] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A trusted blockchain-based traceability system for fruit and vegetable agricultural products," IEEE Access, vol. 9, pp. 36282–36293, 2021.
[29] A. Kassahun, R. J. M. Hartog, and B. Tekin-erdogan, "Realizing chain-wide transparency in meat supply chains based on global standards and a reference architecture," Computers and Electronics in Agriculture, vol. 123, pp. 275–291, 2016.
[30] G. Hartley, "The use of EPC RFID standards for livestock and meat traceability," New Zealand RFID Pathfinder Group, 2013.
[31] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in 2019 11th International Conference on Communication Systems Networks (COMSNETS), pp. 568–570, COMSNETS, 7–11 Jan. 2019.
[32] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT-based food traceability for smart agriculture," in Proceedings of the 3rd International Conference on Crowd Science and Engineering, pp. 1–6, 2018.
[33] A. Tan, D. Gligor, and A. Ngah, "Applying blockchain for halal food traceability," International Journal of Logistics Research and Applications, vol. 25, pp. 1–18, 2020.
[34] B. R. Schlenker, B. Helm, and J. T. Tedeschi, "The effects of personality and situational variables on behavioral trust," Journal of Personality and Social Psychology, vol. 25, no. 3, p. 419, 1973.
[35] S. M. Ghafari, "Towards time-aware context-aware deep trust prediction in online social networks," arXiv preprint arXiv:2003.09543, 2020.
[36] X. Zheng, Trust prediction in online social networks. PhD thesis, Macquarie University, Faculty of Science and Engineering, Department of, 2015.
[37] M. R. Welch, R. E. Rivera, B. P. Conway, J. Yonkoski, P. M. Lupton, and R. Giancola, "Determinants and consequences of social trust," Sociological Inquiry, vol. 75, no. 4, pp. 453–473, 2005.
[38] K. Jones and L. N. Leonard, "Trust in consumer- to-consumer electronic commerce," Information & Management, vol. 45, no. 2, pp. 88–95, 2008.
[39] R. E. Backhouse and S. G. Medema, "Retrospectives: On the definition of economics," Journal of Economic Perspectives, vol. 23, no. 1, pp. 221–233, 2009.
[40] M. T. Thielsch, S. M. Meeßen, and G. Hertel, "Trust and distrust in information systems at the workplace," PeerJ, vol. 6, p. e5483, 2018.
[41] K. N. Qureshi, G. Jeon, et al., "A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities," Journal of Ambient Intelligence and Smart Environments, vol. 13, no. 3, pp. 235–252, 2021.
[42] C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance," in Secure Data Management: 5th VLDB Workshop, SDM 2008, Auckland, New Zealand, August 24, 2008. Proceedings 5, pp. 82–98, Springer, 2008.
[43] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, pp. 2–7.
[44] K. Siau and W. Wang, "Building trust in artificial intelligence, machine learning, and robotics," Cutter Business Technology Journal, vol. 31, no. 2, pp. 47–53, 2018.
[45] X. Yin, J. Han, and S. Y. Philip, "Truth discovery with multiple conflicting information providers on the web," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 6, pp. 796–808, 2008.
[46] D. Gefen, I. Benbasat, and P. Pavlou, "A research agenda for trust in online environments," Journal of Management Information Systems, vol. 24, no. 4, pp. 275–286, 2008.
[47] S. P. Marsh, Formalizing trust as a computational concept. Thesis, 1994.
[48] S. Rouhani and R. Deters, "Data trust frame- work using blockchain technology and adaptive transaction validation," IEEE Access, vol. 9, pp. 90379–90391, 2021.
[49] W. Powell, M. Foth, S. Cao, and V. Natanelov, "Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains," Journal of Industrial Information Integration, vol. 25, p. 100261, 2022.
[50] A. V. Engelen, P. Malope, J. Keyser, and D. Neven, "Botswana agrifood value chain project: Beef value chain study," Report, Food and Agriculture Organization of the United Nations and Ministry of Agriculture, Botswana, 2012.
[51] T. Prinsloo, Livestock traceability systems in Swaziland and Namibia: Towards an impact-for-sustainable-agriculture framework. Thesis, 2017.
[52] T. Seleka and P. Kebakile, "Export competitiveness of Botswana's beef industry," The International Trade Journal, vol. 31, pp. 76–101, 2017.
[53] K. Ontebetse, "Norway dumps BMC beef," Sunday Standard, 03 April 2023. Available at: https://www.sundaystandard.info/norway-dumps-bmc-beef/ (Accessed: June 24th, 2023).
[54] Botswana Government, "User application for Botswana animal identification and traceability system (BAITS)," https://www.gov.bw/animal-husbandry/user-application-botswana-animal-identification-and-traceability-system-baits, 2022.
[55] L. Modisa, "Botswana animal identification traceability system," 14 September 2022, 2013.
[56] J. Byabazaire, G. O'Hare, and D. Delaney, "Data quality and trust: Review of challenges and opportunities for data sharing in IoT," Electronics, vol. 9, no. 12, p. 2083, 2020.
[57] N. Karthik and V. Ananthanarayana, "Sensor data modeling for data trustworthiness," in 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 909–916, IEEE, 2017.
[58] G. C. Karmakar, R. Das, and J. Kamruzzaman, "IoT sensor numerical data trust model using temporal correlation," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2573–2581, 2020.
[59] Z. Zhang, "Computer simulation method for data trust analysis based on average deviation algorithm," IEEE Access, vol. 11, pp. 19602–19612, 2023.
[60] K. K. S. Gautam, R. Kumar, and D. N. Gupta, "Challenges, attacks, QoS, and other security issues for an IoT environment," in AIP Conference Proceedings, vol. 2555, AIP Publishing, 2022.
[61] A. Alsirhani, M. A. Khan, A. Alomari, S. Maryam, A. Younas, M. Iqbal, M. H. Siqqidi, and A. Ali, "Securing low-power blockchain-enabled IoT devices against energy depletion attack," ACM Transactions on Internet Technology, vol. 23, no. 3, pp. 1–17, 2023.
[62] S. K. Sharma and X. Wang, "Live data analytics with collaborative edge and cloud processing in wireless IoT networks," IEEE Access, vol. 5, pp. 4621–4635, 2017.
[63] P. K. Wamuyu, "A conceptual framework for implementing a WSN based cattle recovery system in case of cattle rustling in Kenya," Technologies, vol. 5, no. 3, p. 54, 2017.
[64] E. Hajnal, L. Kov 'acs, and G. Vakulya, "Dairy cattle rumen bolus developments with special regard to the applicable artificial intelligence (AI) methods," Sensors, vol. 22, no. 18, p. 6812, 2022.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
The two authors contributed equally to the manuscript.

Funding:
None declared.

Acknowledgements:
Not applicable.

[1] In our case study, data generators are restricted to IoT sensory devices.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-7-1-(2)2024

A Blockchain-Based, Smart Contract and IoT-Enabled Recycling System

Manaf Zghaibeh
Department of Electrical and Computer Engineering, Dhofar University, Salalah, Oman

Correspondence: mzghaibeh@du.edu.om
Received: 12 July 2023 **Accepted:** 15 September 2023 **Published:** 21 October 2023

Abstract

The current state of recycling systems is marked by significant impediments to their efficacy. A lack of transparency often pervades these systems, which may result in an increased likelihood of fraudulent and corrupt activity. Additionally, traceability pertaining to recycled materials frequently proves inadequate. Together, these inefficiencies in the collection and processing of recyclables can lead to higher costs and environmental impact. Furthermore, low incentives may deter individuals and businesses from participating in recycling initiatives. Certain recycling systems may also suffer from limited compatibility with specific materials, further reducing their effectiveness. To address these challenges, we propose a permissioned Ethereum blockchain-based system that aims to incentivise and encourage recycling practices in a transparent and secure manner. The platform's modular and multi-layered design makes it adaptable to various recycling scenarios, allowing it to handle diverse types of recyclable materials. Automated and streamlined recycling processes are achieved through the use of smart contracts. The proposed system offers a secure, transparent, and efficient platform for the management of recycling processes, promoting environmentally responsible behaviour towards a circular economy. Potential applications for the system include waste disposal and recycling management for smart cities, waste management for organisations, and tracking and management of operations for recycling companies. The platform is highly versatile and can accommodate various use cases in the recycling industry, including those involving traceable and untraceable materials, as well as individual and corporate use cases.

Keywords: *Blockchain, Sustainability, IoT, Recycling, Smart Contracts, DPoS*

JEL Classifications: *D82*

1. Introduction

Recycling plays a pivotal role in mitigating the carbon footprint and combating the environmental repercussions associated with single-use waste, contributing significantly to the principles of the circular economy [1]. However, the efficacy of voluntary recycling programmes at a large scale is often questioned when compared to mandatory initiatives [2]. The reliance on individual adherence to consistent and proper recycling practices in voluntary programmes has proven challenging, resulting in contamination and compromised quality of recycled materials [3]. To address these concerns, the enforcement of recycling policies and regulations becomes imperative. Mandatory recycling programmes, bolstered by effective enforcement mechanisms, establish individual responsibility for appropriate waste recycling [4, 5]. This approach holds the potential to elevate recycling rates and foster the production of superior-quality recycled materials, thereby diminishing the demand for virgin resources and promoting sustainable production practices [6, 7, 8].

Numerous studies have explored the integration of technologies to optimise waste collection, sorting, and recycling processes. For instance, IoT sensors have been used to collect data on waste generation, predict waste amounts, and optimise waste bin collection processes, as demonstrated in [9, 10]. In [9], the authors designed a system that uses IoT sensors to collect data on waste generation and designed an algorithm to predict the amount of waste generated. The system also provided information on the location and capacity of waste bins to optimise the collection process. The authors concluded that their system could reduce the time and cost of waste collection while also promoting recycling by providing insights into waste composition. Similar to [9], [10] evaluated the performance of a smart waste management system in a university campus in Taiwan. The system used RFID technology to track the movement of waste bins and sensors to determine the fill level of each bin. The study found that the smart waste management system improved waste collection efficiency and reduced the overall collection frequency. In the realm of blockchain, several studies discussed the implementation of blockchain to recycle e-waste in particular [11, 12, 13, 14]. [11] specifically emphasised the effectiveness of deploying blockchain technology effectively in order to improve the recycling rate of waste electronics and building trust in consumers. [12] explored the capabilities of a blockchain system to track products and analysed different aspects of costs associated with implementing blockchains for solid waste management and costs spent by existing waste management companies to adapt to the blockchain platform. The systems in [13, 14, 15] suggest blockchain-based e-waste tracking systems for smart cities. The main goal of these systems is to address the issues associated with e-waste management specifically. To achieve this, the proposed solutions combine the use of RFID tags and blockchain technology to monitor and track e-waste throughout its lifecycle, from generation to disposal or recycling. However, these systems only track e-waste that are originally equipped with RFIDs and do not provide incentive and penalising mechanisms to promote recycling and penalising. Furthermore, they require a significant investment in infrastructure for such specific purpose, and their scope and scale are limited with predefined functionalities.

In this paper, we introduce a permissioned Ethereum blockchain-based platform that aims to encourage and incentivise recycling through a transparent and secure system. It provides a digital platform where clients can track their purchase and recycle activities to realise their impact on the environment. This ensures that all parties involved have access to accurate

and verified data. The system's main goal is to establish a sustainable ecosystem that incentivises and fosters responsible behaviour towards the environment. The platform achieves this by employing a tracking system for the acquisition of disposable items. By assigning unique identifiers to recyclable items and utilising scanning technology, it tracks the entire lifecycle of these items, starting from their production to their eventual disposal. This valuable information enables authorities to identify products that are not being recycled and determine their final destination. Such insights can inform targeted interventions and policies to improve recycling rates and minimise the negative impacts of improper waste disposal [16]. This method would also help to increase accountability among manufacturers, distributors, and consumers. By having an accurate record of the products that are not being recycled, authorities could penalise or fine organisations or individuals who are not properly disposing of their waste [17]. In contrast to previous work on blockchain, our system offers a comprehensive waste management solution that can handle all types of waste, including both recyclable and organic materials. Through its smart contracts capabilities, the platform ensures the secure and efficient tracking of waste from the point of purchase to its disposal or recycling. Unlike other blockchain-based waste management systems, such as those discussed in [14, 18], the proposed system has the flexibility to adapt to different types of waste and use cases, making it a highly versatile and scalable solution for promoting responsible waste management practices. Furthermore, the potential uses of the system can be expanded to accommodate a wide range of waste management scenarios beyond its initial scope, enhancing its utility and value to users. The main contributions of this work can be summarised as follows:

- Incentivising recycling system: Unlike other blockchain systems that only track the recycling of specific material, our proposed system is the only one that functions as an all-encompassing circular ecosystem which employs blockchain technology to incentivise and promote proper recycling practices [1]. Through the utilisation of blockchain, users' purchasing and recycling activities are meticulously recorded and tracked.
- Modularity: The system's modular design enables it to be adaptable and flexible to different recycling scenarios, thanks to its multi-layered and multi-tiered structure. This modularity allows for easy integration with existing recycling infrastructures and can be customised to suit the specific needs of individuals or businesses. Additionally, the system's modular approach enables the platform to evolve and expand over time to include new features and functionalities as required, making it a sustainable solution for waste management.
- Ethereum-based: The Ethereum network is a popular blockchain platform that supports smart contracts and decentralised applications DApps. It is known for its security features and its ability to handle large amounts of data and transactions. Our system leverages the Ethereum network to ensure the security and transparency of its waste management platform, enabling users to track and manage their recycling activities efficiently.
- Applicability: Unlike other blockchain waste management systems, the applicability of this proposed system is not limited to a specific type of recyclable items, and it is designed to accommodate both traceable and untraceable items. This feature enhances the system's versatility and enables its integration into different recycling scenarios, thereby offering a highly adaptable and scalable solution.
- Use cases: The modular design of the system allows for the implementation of different use cases targeting various recycling scenarios. For example, it can track recyclable materials in households, businesses, and public places, as well as incentivise users through rewards for responsible recycling behaviour. Additionally, it can also be used to track the recycling of hazardous materials such as batteries and electronic waste. This versatility in application makes the system a valuable tool in promoting responsible behaviour towards the environment and reducing the negative impact of waste on our planet.

2. The System

The system is structured into distinct layers, each housing elements that possess unique roles and responsibilities. These elements are identified and categorised by the system based on their designated addresses (Figure 1):

2.1 Layers

The initial layer in the system is designated as the **Control Layer**, serving as the foremost authoritative entity within the system. The primary function of this layer is to regulate access to the blockchain through the process of sanctioning new nodes and admitting new clients based on their national identification. The term "node" refers to a point of sale, encompassing facilities such as hypermarkets, supermarkets, grocery stores, and vending machines that provide recyclable products for sale. Within our system, the assignment of responsibilities is formed into three distinct levels, each categorised based on the capabilities and resources possessed by the nodes. Nodes with greater capabilities, including hypermarkets and supermarkets, occupy level 1 and maintain a comprehensive copy of the ledger. The sanctioning process for level 1 nodes entails an on-site, off-chain, bureaucratic procedure, wherein the node is formally recognised as a licensed participant in the system and assigned a unique address within the blockchain. Additionally, nodes at this level possess the authority to authorise nodes in the subsequent level, in addition to clients and IoT terminals like vending machines, recycling depots, and bins.

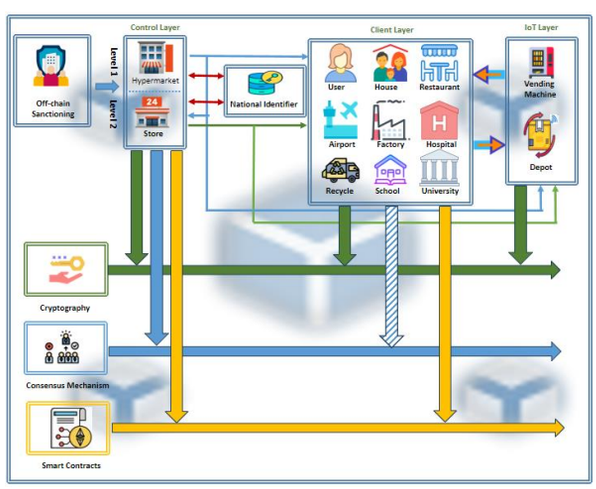


Figure 1. Abstraction of the proposed system.

Level 2, situated within the control layer, comprises nodes with relatively fewer resources, such as small markets and retail shops. Similar to level 1 nodes, those in level 2 retain the entire ledger; however, their sanctioning privileges are limited to clients and IoT terminals at the subsequent level. Nodes in this level do not have the authority to sanction other nodes. This arrangement of distributed functionality among the nodes allows for a more efficient and practical use of resources within the retail blockchain system. Furthermore, each node has a unique private cryptographic key that acts as its identification in the system, used to generate its public cryptographic keys that are shared with the system in a secure manner.

To enable automated and precise monitoring, the system utilises IoT devices to capture real-time data on product acquisition and disposal. This data is securely stored on the blockchain, ensuring transparency and accountability throughout the purchasing and recycling process. Accordingly, the IoT Terminals Layer of the system hosts authorised IoT-

enabled devices, such as vending machines and recycling depots, which play a crucial role in scanning and documenting the purchase and disposal of products. They possess no sanctioning capabilities and do not hold the entire ledger; rather, such terminals only require access in writing mode to add entries to the client's records in the ledger. To ensure the authenticity and integrity of the IoT devices within the network, a registration process is implemented in the control layer: Before an IoT device can be recognised as a sanctioned apparatus, it must undergo registration at the control layer and receive a unique system identity. This registration process establishes a trusted relationship between the IoT device and the platform, ensuring that only authorised devices contribute to the purchasing and recycling process.

The third layer in our system is the Client Layer. A client refers to an individual or organisation that interacts with the platform to participate in purchasing and recycling activities such as individuals, households, restaurants, airports, factories, hospitals, schools, universities, and government and private offices. The admission of new clients to the system is facilitated by the generations of addresses, which are based on government-issued national or tax identifications. Levels 1 and 2 nodes of the control layer in the system are responsible for coordinating with other non-system agencies that maintain the tax or the national identifier database. During the registration process, an individual submits an application with their unique national identifier, which must then be validated by the relevant government agency.

Clients within the system are identified by their unique addresses in the blockchain. Each client is assigned a 2-of-2 multisignature address, which ensures the secure storage of their transactions. Clients do not have exclusive control over their records in the blockchain. Instead, they can collaboratively add new transactions to their records through their associated node or terminal, which is responsible for providing the product or handling the recycling process.

After creating their addresses, clients can access information about recycling locations and events, record and track their purchasing and recycling activities, and earn credits for their contributions to environmental sustainability. They access the system through their wallets.

The wallet, available at trusted locations such as nodes or affiliated websites, provides several functionalities, including key storage, request initiation, and record viewing. It is conceptualised as a software application that is installed on the client's mobile device or terminal. This application holds the private cryptographic key that serves as the client's identification within the blockchain network. To maintain security, the private key must be kept confidential and not shared with unauthorised individuals. In order to provide access to the client's records within the blockchain, the wallet generates a public cryptographic key, derived from the private key. This public key is then transmitted to the node, granting it permission to access the client's records. The lifespan of the public key is determined by a time limit set within the wallet system, which can be altered based on the client's specifications and expires after a predetermined interval.

Recycling companies are also located in the client layer. Those are clients that collect, process, and sell recyclable materials, such as paper, plastic, glass, and metal, to manufacturers that use these materials to make new products. They are sanctioned into the system similar to regular clients by nodes in levels 1 and 2. Upon joining the system, a recycling company will be assigned a "Credit" ledger based on its recycling capacity and collection effort. The credits, or tokens, in this ledger are used to pay other entities for the amount of untraceable recyclables they generate and require special collection and treatment. The credit ledger for each company in the system is reviewed regularly and increased or decreased based on the company's recycling performance. Ultimately, a blockchain constitutes the inclusive layers aforementioned, excluding the off-chain components, and serves as the repository for clients' factual records and transactions. Specifically, this private blockchain serves as the pivotal depository for all client records within the system. Access to this decentralised ledger is conferred upon all authorised nodes ensuring its widespread accessibility. The blockchain operates on the premise of replication, thereby safeguarding previous records against tampering while permitting read-and-write operations with the client's explicit consent. These records are organised into two distinct stacks: one for confirmed purchased items and another for confirmed disposed items.

2.2 Addresses

Entities within the system possess distinct privileges and responsibilities based on their designated address class. Level 1 nodes in the control layer are assigned *Class 1* addresses, granting them the authority to approve new nodes and clients, as well as maintain the global blockchain. Level 2 nodes are assigned *Class 2* addresses, enabling them to admit clients, participate in transaction verification and approval, and maintain a complete copy of the blockchain. However, they lack the authorisation to sanction new nodes. On the other hand, IoT terminals such as vending machines and recycling depots are assigned *Class 3* addresses, allowing them to engage in transaction verification and approval only. Furthermore, clients, designated with *Class 4* addresses, do not possess sanctioning privileges or participate in the consensus mechanism. However, they can initiate and execute smart contracts and access their own records. Lastly, *Class 5* addresses represent n-of-m multisignature addresses exclusively reserved for smart contracts. These addresses are initiated by clients and triggered by nodes within the system.

The process of generating cryptographic addresses, also known as private-public key generation or asymmetric cryptography, involves generating a private key that must be stored in secrecy to ensure data security. Asymmetric cryptography is widely used in blockchain technology to ensure the authenticity and confidentiality of transactions [19, 20]. In the process of private-public key generation or asymmetric cryptography, a private key is randomly generated and should be kept secret by its owner. This key is used to create digital signatures, which are required for proving ownership of records. Applying the private key to a transaction generates a numerical signature, and it is also used to decrypt messages that were encrypted with its public key. The public key is derived from the private key and is used by other entities to encrypt messages addressed to the key's owner. Transactions in the network can be directed to the client's public key, yet for added security, it is recommended to generate addresses from the public key using a hashing algorithm instead of using the public key itself as an address [21, 22].

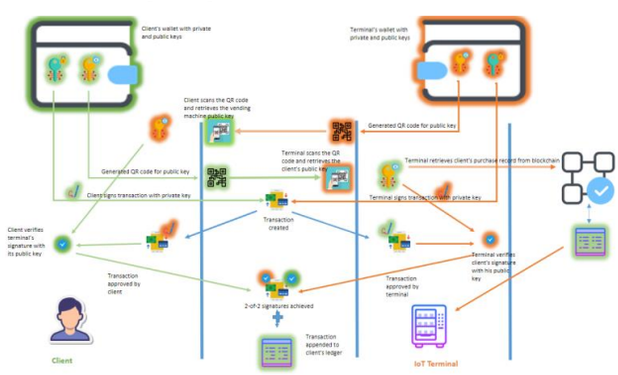


Figure 2. Sequence diagram illustrating the 2-of-2 multisignature scheme as a record is being appended to the client's ledger.

2.3 Multisignature

The use of multisignature schemes in blockchain technology provides an additional layer of security and accountability to transactions. A multisignature scheme is a security mechanism used in blockchain

technology that requires the approval of multiple parties before a transaction can be validated [23]. In a traditional transaction, a singular party initiates the transaction, affixes their digital signature using the corresponding private key, and subsequently broadcasts the transaction into the blockchain. However, in a multisignature scheme, multiple parties are required to sign the transaction before it can be verified and added to the blockchain. The most common multisignature scheme used in blockchain is the *n-of-m* scheme, where *n* represents the number of signatures required to validate a transaction, and *m* represents the total number of parties involved.

All transactions within our system, including the addition of purchase or recycle records, are completed through the utilisation of *n-m* multisignatures. The implementation of multisignature ensures that every transaction necessitates approval from a minimum of two parties, thereby augmenting the system's security and transparency – for instance, when a client is purchasing a bottle of water from a vending machine, which serves as an IoT terminal in our system (Figure 2). The transaction process begins with both the client and the machine exchanging their public keys which are facilitated as scannable QR codes. Subsequently, using the client's public key, the machine retrieves their records from the blockchain and verifies his eligibility to complete the purchase process. If the client's purchase record is full demonstrating negligent recycling behaviour, the transaction will be reverted (Figure 3). Conversely, after verifying the records, both the client and the vending machine employ their private keys to sign the transaction that appends the identifier of the bottle to the client's purchase record in the blockchain. The signatures of both parties are verified by testing them against the public keys they retrieved from each other in the first stage. Finally, the transaction is emitted into the network for approval as detailed in Algorithm 1. Figure 4 illustrates the successful execution of the VendingMachine smart contract.

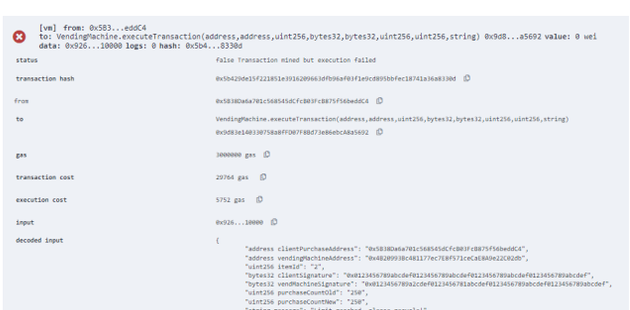


Figure 3. Remix IDE output for VendingMachine contract in Algorithm 1: The transaction has been reverted due to reaching a maximum level of purchased items.

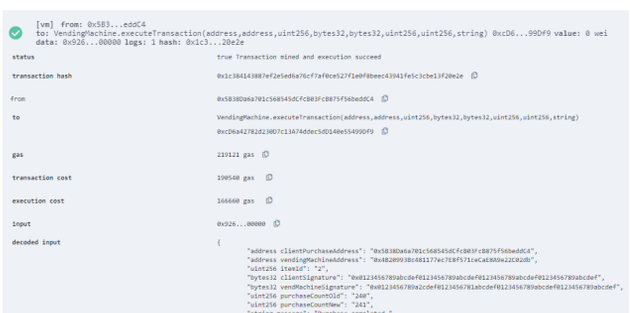


Figure 4. Remix IDE output for VendingMachine contract in Algorithm 1: The transaction mined and executed successfully.

2.4 Blocks

The system's blockchain consists of blocks, wherein each block contains a verified list of transactions executed within the network. These transactions are denoted by 2-of-m multisignature records assigned to individual clients for recyclable items. The blockchain promotes accountability and sustainability by tracking both purchased and recycled items. Hence, as mentioned earlier, in our system every client has two distinct records: one for purchased items and the other for recycled items. To illustrate, consider the scenario where a client wishes to recycle a previously purchased item. He disposes the item at the recycling depot, where it is scanned for its unique identifier and signed (Algorithm 2). The depot then searches the client's purchase record to check if he had previously purchased the item. If a match is found, the recycling depot initiates a transaction to remove the entry from the client's purchase record. Otherwise, the depot initiates a transaction to add the item to the client's recycled items. Either of the signed transactions is then broadcasted to the network for verification and eventual inclusion in the client's record in the blockchain (Figure 5).

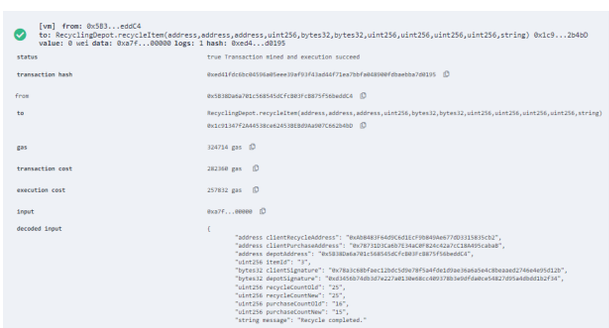


Figure 5. Remix IDE output for RecyclingDepot smart contract in Algorithm 2: The transaction mined and executed successfully with updated recycling and purchasing records.

2.5 Consensus mechanism

Given the nature of our system as an ecosystem that tracks individual transactions related to recycling, a consensus mechanism that prioritises speed and scalability over security is more suitable. This is because the proposed system is likely to have a large number of transactions that need to be processed quickly and efficiently. Hence, a consensus mechanism like Delegated Proof of Stake (DPoS) elevates as a good fit for this system. DPoS is faster and more scalable than both Proof of Work (PoW) and Proof of Stake (PoS) and is more suitable for ecosystems that require high transaction throughput. Additionally, DPoS is more energy-efficient than PoW, which is a significant consideration in a system that tracks individuals' carbon footprint.

The consensus algorithm is utilised to validate all n-of-m transactions carried out within the system by clients, nodes, and terminals. In our system, nodes at levels 1 and 2, along with clients of substantial capacity, super-clients, such as schools, hospitals, and universities, actively participate in the consensus mechanism. Conversely, smaller entities within the system, such as regular users and households, do not engage in the consensus mechanism. The exclusion of smaller entities, such as regular users and households, from the consensus mechanism is a deliberate design choice to ensure scalability and efficiency. By limiting the participation to nodes and clients with substantial capacity, the system can maintain a manageable number of delegates while still benefiting from their expertise and resources.

In our system, the delegate node selection process is automated and endeavours to elect nodes with transparency and efficiency as its primary objectives. By incorporating specific criteria and constraints, the underlying algorithm systematically identifies a subset of delegate nodes that assume pivotal roles within the blockchain consensus mechanism. The selection process entails a comprehensive evaluation of multiple criteria, encompassing factors such as node's uptime, accumulated tokens from

previous processing, node's level, processing capacity, and the location of the node in the area. Each node's performance in these areas is meticulously assessed, and a reward function is employed to quantitatively gauge their overall suitability as delegates. For a system of N nodes participating in the consensus mechanism, we set the following:

$U(n)$: Uptime of node n for $n \in N$.

$T(n)$: Tokens collected from previous processing for $n \in N$.

$L(n)$: Node level (1 or 2) or super-client for $n \in N$.

$C(n)$: Processing capacity of node n for $n \in N$.

$S(n)$: Node location (sector) for $n \in N$.

$D(n_1, n_2)$: Euclidean distance between nodes n_1 and n_2 for $n_1, n_2 \in N$

Where the objective function is to maximise combination of factors such as node uptime, tokens collected, node level, processing capacity, and distance between nodes:

$$\sum_{n\in N}\big(U(n).X(n)\big) + \sum_{n\in N}\big(T(n).X(n)\big) +$$

$$\sum_{n\in N}\big(L(n).X(n)\big) + \sum_{n\in N}\big(C(n).X(n)\big) -$$

$$\sum_{n_1,n_2\in N}(D(n_1,n_2).X(n_1).X(n_2))$$

expecting the output of S, the set of selected delegate nodes, where $\boldsymbol{X(n)}$ is the binary decision variable indicating if node $\boldsymbol{n}$ is selected as a delegate for $\boldsymbol{n \in N}$, subject to the constraints that include selecting a desired number of delegates, level restrictions, fair selection from sectors, and prioritising processing capacity: $\sum_{n\in N}\boldsymbol{X(n)=k}$ where $\boldsymbol{k}$ is the desired number of delegates to be selected, $\boldsymbol{X(n) \le L(n)}$ for all n ∈ N, to ensure that level 2 nodes or super-clients are selected only if necessary, $\sum_{n\in N, S(n)=s} X(n) \ge (1-\varepsilon)(\frac{k}{s})$ for all s, where s is the number of sectors in the geographic area where the nodes are located, and ε is a small tolerance value, to ensure fair selection from sectors, $\sum_{n\in N}(C(n).X(n)) \ge \theta . \sum_{n\in N}\big(T(n).X(n)\big)$ where θ is a trade-off parameter, to prioritise processing capacity over tokens collected, and $X(n) \in \{0,1\}$ for all $n \in N$

3. Use cases

3.1 The case of businesses

A proprietor of a downtown restaurant that generates a significant amount of recyclable items creates a smart contract to facilitate the collection of these recyclables in exchange for a fee[1]. The smart contract encompasses the terms of the agreement between the restaurant and recycling companies, specifying the types and amount of recyclables to be collected and the corresponding service fee. Upon creation, the smart contract is disseminated across the network, allowing interested parties to participate (Algorithm 3). The execution of the smart contract occurs when at least one recycling company acknowledges and accepts the contractual terms and conditions. The involved parties then proceed to endorse the transaction by signing the associated 2-of-m multisignature address. During the collection process, the recycling company scans the deposited recyclables and ascertains their quantities and values. Upon completion of the recycling process and the mutual agreement on the value of the collected recyclables, the parties affix their signatures to the transaction, which is subsequently submitted for approval on the blockchain. Consequently, the restaurant's "purchase record" is adjusted and reduced to account for the items that have been acquired through recycling, and the company's "recycling record" is updated to indicate the items they have received from the restaurant. Figure 6 shows an excerpt of RecyclingContract smart contract output. It shows the success of executing the function executeTransaction presented in Algorithm 3. The function executes after the recycling company agrees to collect 200 items from the client for a fee of 100 according to the function acceptAgreement. In conclusion, the result of recycling the 200 items is reflected in both the client's purchase record and the company's recycle record.

Figure 6. Remix IDE output for the executeTransaction function in the RecyclingContract contract in Algorithm 3.

3.2 The case of untraceable recyclables

Untraceable recyclables are those types of waste that are difficult to track and monitor throughout the recycling process due to a variety of reasons such as having a longer lifespan and multiple uses beyond their initial purchase. Some common examples of untraceable recyclables include paper, bulk plastic, bulk metal, and construction and demolition waste [24]. These types of untraceable waste present significant challenges for recycling programmes and require innovative solutions to incentivise their disposal and recycling. For example, tracking the recycling of paper items poses a significant challenge compared to other recyclable products. The primary reason is that paper has a longer lifespan and multiple uses beyond its initial purchase, making it difficult to track its disposal and recycling. Some of the paper purchased may be archived or stored for long periods, rendering it impossible to trace its recycling journey. For instance, while plastic bottles have unique identifiers that make tracking their purchase and recycling records relatively easy, items such as A4 paper blocks lack this feature. To overcome this challenge, incentives should be created to encourage the recycling of paper products. One such incentive is rewarding individuals and entities based on the volume or weightage of waste they recycle by crediting their "recycling records." As an illustration, a company that wishes to recycle considerable amount of paper waste generates a 2-of-m smart contract in the network requesting recycling companies to submit their bids for collecting the paper waste based on its volume or weightage (Algorithm 4). The contract triggers once at least one company satisfies the conditions set in the smart contract such as weightage or volume, time of collection, and credits rewarded. Figure 7 presents an excerpt of the output of the function submitBid in the smart contract PaperWasteCollection. In this function, two companies submit their bids to collect recyclables offered by a client. The first company bids with 300 to collect 2 tons whereas the second company bids with 250 to recycle 1 ton. As the output of the smart contract shows, the first company's bid is only accepted. Next, upon the collection of the waste, a 2-of-2 transaction is initiated that shifts the credits from the recycling company ledger to the client's "Recycling Record" in the system. Specifically, the transferCredit function in the smart contract PaperWasteCollection is invoked, which transfers 300 credits from the recycling company to the client's recycling record (Figure 8).

3.3 The case of unmatched recyclables

Addressing the challenge of unmatched recyclables is a fundamental

aspect of the system's operational framework. Instances may arise where items are procured and logged in the system but remain unrecycled by the purchasers. This issue can be attributed to a range of factors or circumstances impeding the successful recycling of those specific items. To address this issue, clients are afforded the opportunity to mitigate the impact of unmatched recyclables by reducing their purchase record. This can be accomplished through the process of recycling alternative items that qualify for redemption. By engaging in this practice, clients can reconcile the discrepancy between the purchased items and the actual recycling activities, ensuring the accuracy and integrity of the system's records.

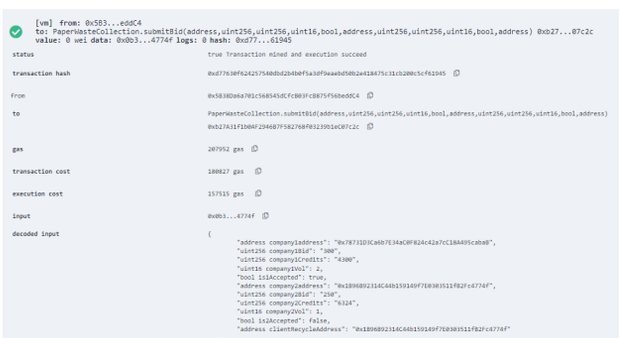


Figure 7. Remix IDE output for the submitBid function in the PaperWasteCollection smart contract in Algorithm 4.

Figure 8. Remix IDE output for the transferCredit function in the PaperWasteCollection smart contract in Algorithm 4.

This approach allows for the effective management of unmatched recyclables, promoting transparency, accountability, and operational efficiency within the system. By providing clients with the means to rectify the situation through the recycling of suitable alternatives, the system fosters a streamlined and reliable recycling process while maintaining a comprehensive and accurate purchase record.

The system employs a value differentiation mechanism to account for the inherent variations among different items, considering their distinct characteristics, such as size and weight. This approach enables the system to establish equivalencies between items, exemplifying the ability to equate items of different quantities based on their defined value ratios. For instance, a one litre bottle is deemed equivalent to four 250 ml bottles, thus establishing a quantitative relationship that facilitates streamlined record-keeping and transactional operations within the system. This not only reduces the size of the ledger but also ensures that the system remains efficient in keeping track of the records.

Algorithm 5 illustrates the AdjustRecords smart contract that enables clients to reduce their purchasing records by recycling unmatched items. In the scenario where a client intends to enhance their recycling record by recycling a quantity of bottles that were not originally theirs, they can accomplish this by depositing the bottles at a designated recycling depot. Subsequently, the recycling depot updates the client's recycling record to accurately reflect the newly recycled items. At this point, both the recycling and the purchasing records contain unmatched items. To adjust the ledgers, the deleteItems function will undertake the following actions: (1) if the items in the recycling record are identical to those in the purchase record in terms of values, albeit with different identifiers, the system will delete the corresponding entries from both records (Figure 9); (2) if the items differ in value, the system will refer to the value of each item and equate them based on that, that is, one litre bottle versus a 250 ml bottle, the system may equate four items of the 250 ml size with one item of the one litre size and subsequently delete them from both records (Figure 10).

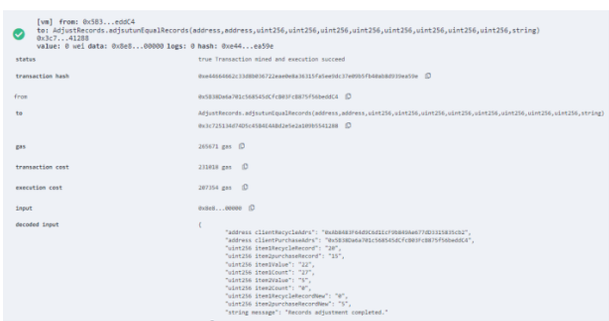


Figure 9. Remix IDE output for the transferCredit function in the AdjustRecords smart contract in Algorithm 5.

Figure 10. Remix IDE output for the transferCredit function in the AdjustRecords smart contract in Algorithm 5.

4. Conclusion

The utilisation of blockchain technology in recycling management has immense potential, and this proposed recycling system is a notable example of how this technology can be harnessed to address critical issues faced by the recycling industry. Our system ensures transparency and accountability in the recycling process. It is a multi-layered and multi-tiered modular blockchain-based recycling management system. The three distinctive layers of control, client, and IoT devices ensure that each stakeholder has a unique role and responsibility in the system. The use of smart contracts equipped with fully automated and secured management capabilities further enhances the efficiency of the system. Additionally, the implementation of the automated DPoS consensus mechanism ensures low overhead and less resource utilisation. The proposed system has the potential to revolutionise the recycling industry by providing a secure, transparent, and efficient platform for managing the recycling process. The proposed system exhibits diverse potential applications within the recycling industry. It can be effectively utilised by governments as an integral component of smart cities for waste disposal and recycling management. Furthermore, organisations can employ the system to monitor and enhance their waste management processes. Individuals can leverage its capabilities to facilitate efficient and environmentally conscious waste disposal practices. Additionally, recycling companies can utilise the system to streamline their operations and ensure effective tracking and management of recyclable materials.

References

[1] S. Ponis, "Industrial symbiosis networks in Greece: Utilising the power of blockchain-based B2B marketplaces," JBBA, 2020. https://doi.org/10.31585/jbba-4-1-(4)2021.

[2] J. C. Borck and C. Coglianese, "Voluntary environmental programs: Assessing their effectiveness," Annu. Rev. Environ. Resour., vol. 34, pp. 305–324, 2009.

[3] "Enhancing policy coherence for development: Workshop," Organisation for Economic Cooperation and Development, Tech. Rep., 2016, OECD Publishing.

[4] J. D. Ward and D. W. Gleiber, "Citizen response to mandatory recycling," Public Product. Manag. Rev., vol. 16, no. 3, pp. 241–253, 1993.

[5] J. W. Everett and J. J. Peirce, "Curbside recycling in the U.S.A.: Convenience and mandatory participation," Waste Manag. Res., vol. 11, no. 1, pp. 49–61, 1993.

[6] R. Pantcheva and G. Mengov, "Recycling rate in Europe: econometric modeling and dart clustering analysis," in 2022 Int. Conf. Automatics Inform. (ICAI), 2022, pp. 179–182.

[7] A. Bongers and P. Casas, "The circular economy and the optimal recycling rate: A macroeconomic approach," Ecol. Econ., vol. 199, p. 107504, 2022. [Online].

[8] S. Park, "Factors influencing the recycling rate under the volume-based waste fee system in South Korea," Waste Manag., vol. 74, pp. 43–51, 2018.

[9] M. Paturi, S. Puvvada, B. S. Ponnuru, M. Simhadri, B. S. Egala, and A. K. Pradhan, "Smart solid waste management system using blockchain and IoT for smart cities," in 2021 IEEE Int. Symp. Smart Electron. Syst. (iSES), 2021, pp. 456–459.

[10] E. Shanthini, V. Sangeetha, M. Jagadeeswari, B. Shivani, P. Selvapriya, K. Anindita, D. Divya Shree, and R. Suryanarayanan, "IoT based smart city garbage bin for waste management," in 2022 4th Int. Conf. Smart Syst. Inventive Technol. (ICSSIT), 2022.

[11] X. Wang, D. Ma, and J. Hu, "Recycling model selection for electronic products considering platform power and blockchain empowerment," Sustainability, vol. 14, no. 10, p. 6136, 2022.

[12] P. K. Gopalakrishnan, J. Hall, and S. Behdad, "Cost analysis and optimization of blockchain-based solid waste management traceability system," Waste Manag., vol. 120, pp. 594–607, 2021. [Online].

[13] S. Sahoo, A. Mukherjee, and R. Halder, "A unified blockchain-based platform for global e-waste management," Int. J. Web Inf. Syst., vol. 17, no. 5, pp. 449–479, 2021.

[14] A. U. R. Khan and R. W. Ahmad, "A blockchain-based IoT-enabled e-waste tracking and tracing system for smart cities," IEEE Access, vol. 10, pp. 86256–86269, 2022.

[15] M. K. Nallapaneni and S. S. Chopra, "Blockchain-based online information sharing platform for improving the resilience of industrial symbiosis-based multi energy systems," in Actionable Science for Urban Sustainability 2020 (AScUS-2020): AScUS Unconference, 2020.

[16] T. Ding, G. Yan, Z. Zhou, and Y. Lei, "Research on product life cycle data traceability based on multiblockchain," in 2021 3rd Int. Symp. Robot, Intell. Manuf. Technol. (ISRIMT), 2021.

[17] C. Wankm¨uller, J. Pulsfort, M. Kunovjanek, R. Polt, S. Craß, and G. Reiner, "Blockchain-based tokenization and its impact on plastic bottle supply chains," Int. J. Prod. Econ., vol. 257, p. 108776, 2023.

[18] S. Pandey, V. Chouhan, D. Verma, S. Rajrah, F. Alenezi, R. Saini, and K. Santosh, "Do-it-yourself recommender system: Reusing and recycling with blockchain and deep learning," IEEE Access, vol. 10, pp. 90056–90067, 2022.

[19] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org, 2008.

[20] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc., 2014.

[21] J. Sun, L. Ren, S. Wang, and X. Yao, "A blockchain-based framework for electronic medical records sharing with fine-grained access control," PLOS ONE, vol. 15, no. 10, pp. 1–23, 2020.

[22] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE Int. Congr. Big Data (BigData Congress), 2017, pp. 557–564.

[23] J. Shah and S. Parveen, "Understanding the blockchain technology beyond bitcoin," In Advances in Industrial and Production Engineering: Select Proceedings of FLAME 2020, pp. 499–516, Springer.

[24] V. Ram, K. C. Kishore, and S. N. Kalidindi, "Environmental benefits of construction and demolition debris recycling: Evidence from an Indian case study using life cycle assessment,"J. Clean. Prod., vol. 255, p. 120258, 2020. https://www.sciencedirect.com/science/article/pii/S095965262030305X.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
MZ designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

1 Implementing the generation of smart contracts through a GUI interface within the user's wallet offers a user-friendly approach to creating blockchain-based agreements. This intuitive method streamlines the process by integrating contract creation directly into the wallet interface. Users can interact with the wallet's graphical tools to design, configure, and deploy smart contracts without the need for extensive coding knowledge.

Appendix

Algorithm 1 Adding purchase entry to client's record

```
contract VendingMachine.
Declare:
struct PurchaseTransactions(clientPurchaseAdrs, vendingMachineAdrs, itemId, clientSignature, vendMachineSignature, purchaseCountOld, purchaseCountNew, message).
mapping purchaseTransaction of type PurchaseTransactions.
struct PurchasedItems(clientPurchaseAdrs).
mapping purchasedItem type of PurchasedItems.
event   NewpurchaseTransaction(clientPurchaseAdrs, vendingMachineAdrs, itemId, clientSignature, vendMachineSignature, purchaseCountOld, purchaseCountNew, message).
verify: signature of client.
if 1 then
function processItem(itemId,items[])
{
N ← length(items[])
    require (!(N≥ limit), "Limit reached, please recycle")
purchasedItem[clientPurchaseAdrs].push(itemId)
}
    emit NewpurchaseTransaction
end if
```

Algorithm 2 Adding recycle entry to client's record

```
contract RecyclingDepot.
Declare:
struct Transactions(clientRecycleAdrs, clientPurchaseAdrs, itemId, clientSignature, depotSignature, recycleCountOld, recycleCountNew, purchaseCountOld, purchaseCountNew, message).
mapping Transaction of type Transactions.
struct Items (itemId; owner; itemName; itemValue;)
mapping recycledItem type of Items.
event NewTransactions(clientRecycleAdrs, clientPurchaseAdrs, itemId, clientSignature, depotSignature, recycleCountOld, recycleCountNew, purchaseCountOld, purchaseCountNew, message).
verify: signature of client.
if 1 then
    function processItem(itemId, purchasedItem[])
{
  N ← length(purchasedItem[])
  for i ← 1 to N do
     if (purchasedItem[i]==itemId) then purchasedItem[i]=purchasedItem[length(purchasedItem[])-1];
        items.pop();
        emit NewTransactions
     else recycledItem[clientRecycleAdrs].push(itemId)
        emit NewTransactions
     end if
  end for
}
end if
```

Algorithm 3 Recyclables collection contract

```
contract RecyclingContract.
Declare:
collectionFee; isAgreementAccepted; isTransactionCompleted;
struct Transactions(isAgreementAccepted, collectionFee; numberOfItems; restaurantPurchaseAdrs; companyRecycleAdrs; restaurantSignature; companySignature; rstntPurchaseCountOld; rstntPurchaseCountNew; cmpnPurchaseCountOld; cmpnPurchaseCountNew; isTransactionCompleted).
mapping Transaction of type Transactions.
struct Items (itemId; owner; itemName; itemValue;)
mapping recycledItem type of Items.
mapping purchasedItem type of Items.
event AgreementAccepted(companyRecycleAdrs)
function acceptAgreement() {
require (msg.sender==restaurantPurchaseAdrs)
isAgreementAccepted=true;
companyRecycleAdrs=payable(msg.sender)
emit AgreementAccepted(companyRecycleAdrs); }
function executeTransaction() payable {
require (msg.sendr==restaurantPurchaseAdrs)
require (isAgreementCompleted==true)
require (isTransactionCompleted==false)
require (msg.value==collectionFee)
N ← length(purchasedItems[restaurantPurchaseAdrs])
for i ← 1 to N do
    purchaseValue = purchasedItems[restaurantPurchaseAdrs][i].itemValue + purchaseValue;
end for
i=0;
while (purchaseValue>0) do
    purchasedItems[restaurantPurchaseAdrs][i]=
purchasedItems[restaurantPurchaseAdrs][length(purchasedItems[restaurantPurchaseAdrs])-1];
    recycledItems[companyRecycleAdrs][length(recycledItems[companyRecycleAdrs])+1]=
purchasedItems[restaurantPurchaseAdrs][i];
    purchasedItems.pop();
    purchaseValue =purchaseValue- purchasedItems[restaurantPurchaseAdrs][i].itemValue;
    i++;
end while
isTransactionCompleted← true;
companyRecycleAdrs.transfer(msg.value);
emit TransactionCompleted }
```

Algorithm 3 Recyclables collection contract

```
contract RecyclingContract.
Declare:
collectionFee; isAgreementAccepated; isTransactionCompleted;
struct Transactions(isAgreementAccepated, collectionFee; numberOfItems; restaurantPurchaseAdrs; companyRecycleAdrs; restaurantSignature; companySignature; rstntPurchaseCountOld; rstntPurchaseCountNew; cmpnPurchaseCountOld; cmpnPurchaseCountNew; isTransactionCompleted).
mapping Transaction of type Transactions.
struct Items (itemId; owner; itemName; itemValue;)
mapping recycledItem type of Items.
mapping purchasedItem type of Items.
event AgreementAccepted(companyRecycleAdrs)
function acceptAgreement() {
require (msg.sender==!restaurantPurchaseAdrs)
isAgreementAccepted=true;
companyRecycleAdrs=payable(msg.sender)
emit AgreementAccepted(companyRecycleAdrs); }
function executeTransaction() payable {
require (msg.sendr==restaurantPurchaseAdrs)
require (isAgreementCompleted==true)
require (isTransactionCompleted==false)
require (msg.value==collectionFee)
N ← length(purchasedItems[restaurantPurchaseAdrs])
for i ← 1 to N do
    purchaseValue = purchasedItems[restaurantPurchaseAdrs][i].itemValue + purchaseValue;
end for
i=0;
while (purchaseValue>0) do
    purchasedItems[restaurantPurchaseAdrs][i]=
purchasedItems[restaurantPurchaseAdrs][length(purchasedItems[restaurantPurchaseAdrs])-1];
    recycledItems[companyRecycleAdrs][length(recycledItems[companyRecycleAdrs])+1]=
purchasedItems[restaurantPurchaseAdrs][i];
    purchasedItems.pop();
    purchaseValue =purchaseValue- purchasedItems[restaurantPurchaseAdrs][i].itemValue;
    i++;
end while
isTransactionCompleted← true;
companyRecycleAdrs.transfer(msg.value);
emit TransactionCompleted }
```

Algorithm 4 Untraceble recyclables

```
contract PaperWasteCollection.
Declare: companyAdrs; recyclceCompanyAdrs; paperWeight; paperVolume; credits; contractFulfilled;
constructor( _weight, _volume, _credits) {
paperWeight = _weight; paperVolume = _volume; collectionTime = Time; contractFulfilled = false; credits=_credits;
emit ContractCreated( paperWeight, paperVolume, collectionTime, credits); }
function submitBid(companyAdrs, companyBid, companyVol) public {
require (msg.sender != companyAdrs);
require(!contractFulfilled);
emit BidSubmitted(msg.sender, bid);
if (bid ¿= credits) then
    recyclceCompanyAdrs = msg.sender;
    contractFulfilled = true;
    emit ContractFulfilled(companyAdrs, recyclceCompanyAdrs, credits);
end if} }
event ContractCreated(companyAdrs, paperWeight, paperVolume, collectionTime, credits);
event BidSubmitted(recyclceCompanyAdrs, bid);
event ContractFulfilled(companyAdrs, address recyclceCompanyAdrs, credits);
function transferCredits()
require(contractFulfilled);
emit transferCredit(recyclceCompanyAdrs, companyAdrs, creditsToTransfer);
```

Algorithm 5 Unmatched records adjustment

```
contract AdjustRecords
Declare:
struct RecycleTransactions(clientRecycleAdrs; itemValue; clientSig; depotSig).
mapping recycleTransaction of type RecycleTransactions.
struct PurchaseTransactions(clientPurchaseAdrs; itemValue; clientSig; depotSig).
mapping purchaseTransaction of type PurchaseTransactions.
struct Items (itemId; owner; itemName; itemValue;)
 mapping  recycledItem type of Items.
 mapping  purchasedItem type of Items.
event New recycleTransactions(transactionId, clientRecycleAdrs, itemId, clientSig, depotSig).
event New purchaseTransactions(transactionId, clientPurchaseAdrs, itemId, clientSig, depotSig).
function deleteItems(recycledItems[], purchasedItems[] )
N ← length(recycledItems[])
for i ← 1 to N do
    recycleValue = recycledItems[i].itemValue + recycleValue;
end for
m ← length(purchasedItems[])
for j ← 1 to M do
    purchaseValue = purchasedItems[j].itemValue + purchaseValue;
end for
if (purchasedalue¿recycleValue) then
    j=0;
    while (purchaseValue¿recycleValue) do
        purchasedItems[j]=purchasedItems[length(purchasedItems[])-1];
        purchasedItems.pop();
        purchaseValue =purchaseValue- purchasedItems[j].itemValue;
        j++;
    end while
    for i ← 1 to N do
        recycledItems[i].pop();
    end for
else
    if (purchaseValue¡recycleValue) then
        i=0;
        while (purchaseValue¡recycleValue) do
            recycledItems[i]=recycledItems[length(recycledItems[])-1];
            recycledItems.pop();
            recycleValue ==recycleValue- recycledItems[i].itemValue;
            i++
        end while
        for j ← 1 to M do
            recycledItems[j].pop();
        end for
    else
        i=0;
        while (purchaseValue=recycleValue) do
            for j ← 1 to M do
                recycledItems[j].pop();
            end for
            for i ← 1 to N do
                recycledItems[msg.sender][i].pop();
            end for
        end while
    end if
end if
emit New purchaseTransactions
emit New recycleTransactions
```

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-7-1-(1)2024

Using Blockchain Technology to Improve the Integrity and Transparency of Procurement Processes between SMMEs and Government: A Systematic Literature Review

Edzai Kademeteme, Stella Bvuma
University of Johannesburg, South Africa

Correspondence: eamkademeteme@gmail.com
Received: 29 April 2023 **Accepted:** 06 August 2023 **Published:** 13 October 2023

Abstract

Fourth industrial revolution (4IR) technologies, such as blockchain, have the potential to improve public and private sector procurement processes. However, governments, including the South African (SA) government, have failed to recognize the significance of blockchain technology for several reasons, including corruption. The PRISMA methodology was used in this study to conduct a systematic literature review of the use of blockchain technology to improve the integrity and transparency of procurement processes between small-, medium- and micro-enterprises (SMMEs) and the SA government. The Scopus database was used to search for literature, and the final analysis included 12 articles that met the eligibility criteria. The 12 articles were analyzed using thematic analysis and the results demonstrated that 10 of the articles applied to this study as they discussed the use of blockchain in relation to integrity and transparency. The remaining two articles did not emphasize the use of blockchain technology in enhancing the integrity and transparency of the procurement processes. The common factors in the 10 articles that were found to impact integrity and transparency were as follows: handling of contracts, risks involved, security of the data, approaches used, management of the procurement process, transaction processing, the chain of events in the procurement process, access to critical data, the application process for securing contracts, quality of products, costs, and types of contracts. We believe that once blockchain technology has been implemented, SMMEs and the public will trust and be confident in the procurement processes as corruption would have been eliminated and tenders would be awarded fairly.

Keywords: *Fourth Industrial Revolution, 4IR, Blockchain Technology, SMMEs, PRISMA, Corruption, Public Procurement*

JEL Classifications: *H57, L14*

1. Introduction

Corruption and a lack of transparency have ravaged some governments and economies [1]. Corruption is considered one of the most significant threats to the economic security of any country or organization [2]. Several anti-corruption measures such as legislating, adopting rules and regulations making certain behavior illegal, and increasing punishments for illegal conduct [3] have been implemented to reduce or combat corruption. While these methods have reduced corruption to a certain extent, perpetrators often find ways to remain corrupt and use various strategies to either escape or postpone detection and punishment indefinitely. Therefore, much effort is needed to eradicate corruption. The impact of corruption on developing economies is devastating because these economies are already struggling [4]–[6]. South Africa (SA) is one such emerging and developing economy. According to Transparency International's 2021 Corruption Perception Index (CPI) report, SA is engulfed in corruption, with a CPI score of 44/100 and is ranked 70 out of 180 [7]. The CPI ranks 180 countries and territories worldwide based on the perceived levels of public sector corruption. The results are given on a scale of 0 (highly corrupt) to 100 (very clean).

Small, medium, and micro enterprises (SMMEs) are considered important to both developed and emerging economies [8]. In SA, SMMEs are important for economic growth and development, contributing approximately 36% to the total gross domestic product (GDP) [9].

They are considered fundamental to addressing issues such as economic growth, job creation, and poverty alleviation [10]. SMMEs have been credited with driving economic growth and development in developed countries around the world [11]. Governments frequently engage SMMEs to provide services through procurement processes. However, because of the high levels of corruption within governments, most SMMEs have failed to benefit from this trade relationship with governments [12], while some have benefited owing to the corruption [12]. Given the critical role that SMMEs and public procurement play in growing a country's economy, there is a need to fully support their transactional activities and procurement processes. Thus, several attempts and proposals have been made by researchers and governments regarding methods for eliminating corruption during procurement processes between governments and private service providers such as SMMEs [3], [13]. Attempts and proposals include the introduction of compliance measurements, regulatory frameworks, and severe punishments, among others. These attempts and proposals have reduced corruption to some extent, but despite concerted efforts to implement a broad range of anti-corruption measures, the problem of malfeasance persists [3]. Currently, there is no effective evidence-based prevention method to combat and stop corruption [13] when tenders are awarded to SMMEs.

This review article aims to explore the use of blockchain technology to improve the integrity and transparency of procurement processes between SMMEs and governments with a focus on SA. We focus on SA because its government departments continue to rely on a manual paper-based procurement system with few electronic features [14]. This has allowed for a high level of human interference, contributing to corruption, favoritism,

and inefficiency, demonstrating the country's readiness to fully implement e-procurement in its public sector [14]. Although the SA government has implemented numerous policy frameworks and systems to ensure fair, equitable, transparent, and cost-effective public procurement processes, the processes remain vulnerable to mismanagement and irregularities [15]. According to [16], poor procurement processes result in the appointment of incompetent contractors, and practitioners engage in unethical behavior, such as bribery, out of desperation for work [16]. Given the challenges that SA's public procurement processes face, the use of blockchain to manage these processes is likely to improve them by eliminating corruption and increasing efficiency.

The article is structured as follows: Section 2 introduces and describes blockchain technology; Section 3 presents the methodology followed, namely, a systematic literature review (SLR) through a literature search on the use of blockchain technology by governments and SMMEs to meet the aim of the study, and the results of the search; Section 4 presents the results of the thematic analysis conducted on the research literature identified; Section 5 comprises the discussion of the findings and their implications for theory and practice; and Section 6 presents the conclusions drawn and future research prospects.

2. Blockchain technology

Blockchain is a technology that uses a decentralized structure, distributed notes and storage mechanisms, a consensus algorithm, smart contracting, and asymmetric encryption to ensure network security, transparency, and visibility [17]. It is considered a collection of distributed databases that contain all public transactions, records, and digital events, which are shared among the participants [18]. Blockchain technology is a distributed ledger network in which nodes communicate with one another for trading data and transactions [19]. A blockchain is a distributed and decentralized technology comprising time-stamped blocks linked by a cryptographic hash. It has gained widespread acceptance as a solution to the underlying trust and security issues in information transparency and the prevention of tampering with data [20]. Blockchain applications are not only one technique but include cryptography, mathematics, algorithms, and economic models. They incorporate peer-to-peer networks and use distributed consensus algorithms to solve conventional distributed database synchronization problems [19].

Blockchain technology ensures security and transparency through the following processes:

1. The use of digitally distributed databases in which blocks are linked to one another in a linear fashion that cannot be changed.
2. A Merkle tree, which is a data structure that is used to encode blockchain data more efficiently and securely, is saved in the block and is used to validate the transaction. This determines whether a transaction is fraudulent or not.
3. Only when all participants in the supply chain agree on the transaction will a new block of information be added to the blockchain. This ensures that only valid transactions are recorded in the blockchain.
4. When a block is added to the blockchain, it can no longer be tampered with, and the transaction data are permanently recorded. This ensures the preservation of historical records.

If a government department adopts blockchain for contract awarding, we anticipate the process to be secure and efficient. For example, a contract will be stored on distributed databases to avoid it being tampered with because once it has been added, it cannot be altered.

Blockchain offers the following advantages: reliability, efficiency, fault tolerance, scalability, transparency, and traceability [18], [19], [21]. Every transaction is verified before being saved and once saved it cannot be reversed [18]. Such characteristics make transactions between SMMEs and governments transparent and secure. The ability of blockchain technology to record transactions on distributed ledgers opens up new avenues for governments to improve transparency, prevent fraud, and foster trust in the public sector [22]. Each transaction is validated using multiple computers. These systems, which are used to validate blockchain transactions, create a peer-to-peer network. They collaborate to ensure that any transaction is legitimate prior to it being added to the blockchain and thus prevent invalid blocks from being added to the chain [18]. Therefore, blockchain technology assists in the development of trust mechanisms for resolving transparency and security issues, as no single party in the supply chain can alter existing information [20].

In summary, blockchain technology offers the following advantages: information security, technological advantages, improvement of supply chain collaboration and trust, reduction of economic loss and product waste, and sustainable and transparent traceability management. With such advantages, top government officials will be less concerned about security and unethical practices within government because technologies such as blockchain prevent such practices. Therefore, governments should consider implementing such a technology to address issues of integrity and lack of transparency in public procurement processes.

This study examined published academic research on blockchain technology used by governments and SMMEs. The subsequent section presents the methodology followed to conduct a SLR through a literature search to better understand what has currently been done to implement blockchain technology in governments.

3. Methodology and results of the literature search

In terms of the methodology followed, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework [23] was used to explain the overall article selection and rejection process for the literature review on the use of blockchain technology to improve transparency and integrity in procurement processes. The PRISMA framework is illustrated in Figure 1.

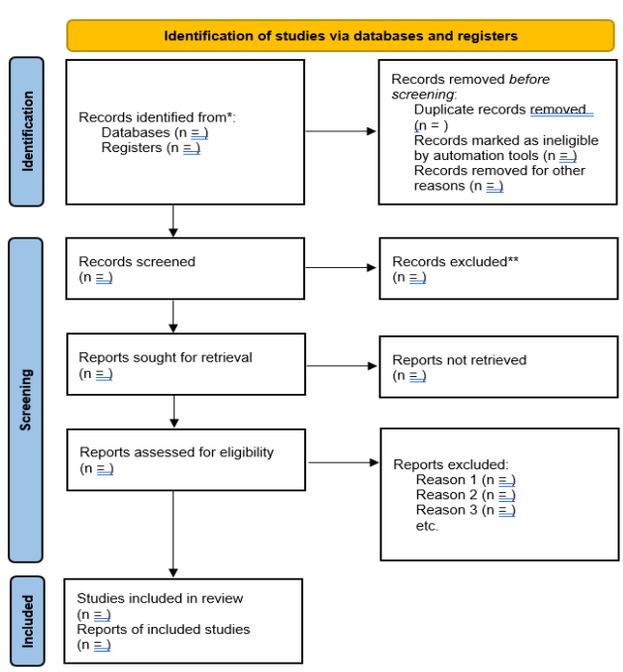


Figure 1. The PRISMA framework [23].

The PRISMA framework consists of three stages: identification, screening, and inclusion. The identification stage identifies the keywords that will be used to conduct the literature search and the source/s where the search will occur. The second stage, screening, details the criteria that will be used to select the best literature from the bulk search. The third stage, referred to as included, reports on the exact final literature that is included in the study after exclusion.

3.1 Identification stage

Following the PRISMA framework, during the identification stage, we decided to use the Scopus database as the source for the literature search. The Scopus database was chosen because the researchers have access to the database via their institution (university). During the identification stage, the following keywords and their various combinations were considered for the search: blockchain, blockchain technology, public procurement, corruption, transparency, procurement processes, SMMEs, SMEs, and governments. An initial search was conducted using the keywords "blockchain" and "block chain" to provide an idea of the overall view of publications that included these terms. A total of 28,581 articles were obtained. The identification stage requires that the output is screened before the actual screening stage. To achieve this, the papers published before 2013 were removed because according to our assessment, there was a sharp rise in the number of studies on blockchain technology from 2016. Furthermore, blockchain technology is a Fourth Industrial Revolution (4IR) technology that came to prominence in 2016 [24]. Finally, in terms of this preliminary screening, articles published in 2022 were removed because we were interested in full-year data only. Figure 2 illustrates the number of papers on blockchain published globally between 2016 and 2021.

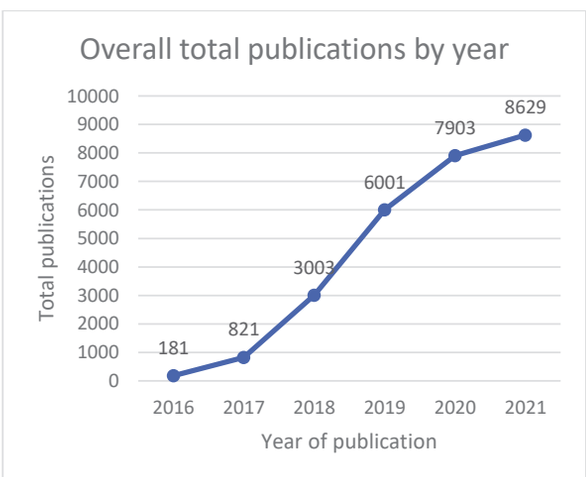


Figure 2. Papers published globally on blockchain.

After performing the preliminary cleaning, we were left with 26,538 papers published between 2016 and 2021. The number of papers published per year in the context of SA only are reflected in Figure 3.

Figure 3 distinctly shows that global research on blockchain technology has risen steadily, whereas in SA the rate of increase has been slow. To date, 26,431 papers have been published globally between 2016 and 2021, while only 107 have been published in the context of SA during the same period. The latter comprises 0.405% of all global publications. This is a low publication rate when compared with the global figure, indicating the need for research on blockchain in the context of SA to be increased significantly.

Figure 3 distinctly shows that global research on blockchain technology has risen steadily, whereas in SA the rate of increase has been slow. To date, 26,431 papers have been published globally between 2016 and 2021, while only 107 have been published in the context of SA during the same period. The latter comprises 0.405% of all global publications. This is a low publication rate when compared with the global figure, indicating the need for research on blockchain in the context of SA to be increased significantly.

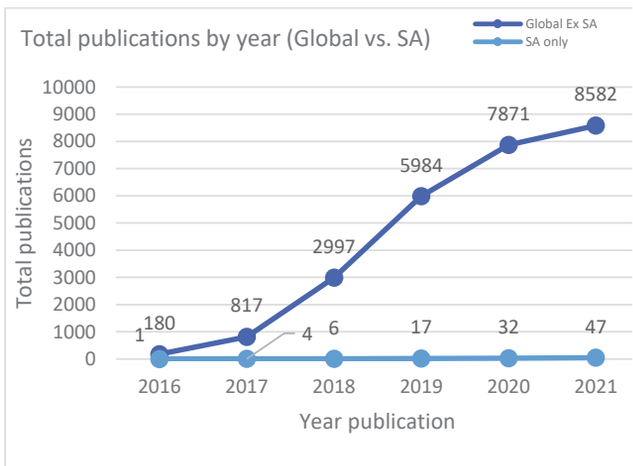


Figure 3. Papers published on blockchain globally vs. SA.

3.2 Screening stage

According to PRISMA, screening is the second stage and, in this stage, the final query in Table 1 was used. The query is explained as follows: papers on blockchain, conducted in the context of SA, published between 2016 and 2021, open access papers only, and articles written in English only. The output of the query was 12 articles.

Table 1. Search string and results obtained

Query Search String	Total articles included after applying the full search string
TITLE-ABS-KEY ((blockchain OR "block chain") AND (procurement OR government OR corruption OR "supply chain")) AND (LIMIT-TO (OA,"all")) AND (LIMIT-TO (AFFILCOUNTRY,"South Africa")) AND (LIMIT-TO (PUBYEAR,2021) OR LIMIT-TO (PUBYEAR,2020) OR LIMIT-TO (PUBYEAR,2019) OR LIMIT-TO (PUBYEAR,2018) OR LIMIT-TO (PUBYEAR,2017) OR LIMIT-TO (PUBYEAR,2016)) AND (LIMIT-TO (LANGUAGE, "English"))	12

3.3 Included stage

Following the screening stage, the included stage was performed. In this stage, the 12 articles obtained during the screening stage by executing the search query were analyzed. These 12 articles were exported to a CSV file format for further cleaning and analysis in Microsoft Excel. In Excel, we looked for duplicate articles and articles that are in the "In Press" publication stage. None of the papers were deleted as they did not meet the criteria for deletion. Further analysis in Excel was conducted using the total number of citations. Table 2 shows the details of the citation analysis for each of the 12 articles.

Table 2. Citation analysis by article title

Article	Author(s)	Title	Year of publication	Total number of citations
D3	Tandon, A., Kaur, P., Mäntymäki, M. and Dhir, A., 2021.	Blockchain applications in management: A bibliometric analysis and literature review	2021	21
D4	Grover, P., Kar, A.K. and Vigneswara Ilavarasan, P., 2018	Blockchain for businesses: A systematic literature review	2018	16
D2	Daramola, O. and Thebus, D., 2020.	Architecture-centric evaluation of blockchain-based smart contract E-voting for national elections	2022	8
D1	Danielle, N.E.L., 2020.	Allocation of risk in public-private partnerships in information and communications technology	2020	6
D9	Mageto, J. and Luke, R., 2020.	Skills frameworks: A focus on supply chains	2020	5
D6	Dietrich, F., Ge, Y., Turgut, A., Louw, L. and Palm, D., 2021.	Review and analysis of blockchain projects in supply chain management	2021	3
D10	Dietrich, F., Palm, D. and Louw, L., 2020.	Smart contract-based framework to increase transparency of manufacturing networks	2020	1
D5	Senou, R.B., Dégila, J., Adjobo, E.C. and Djossou, A.P.M., 2019.	Blockchain for child labour decrease in cocoa production in West and Central Africa	2019	1
D7	Gambo, N. and Musonda, I., 2021.	Effect of the Fourth Industrial Revolution on road transport asset management practice in Nigeria	2021	1
D8	Alsaed, Z., Khweiled, R., Hamad, M., Daraghmi, E., Cheikhrouhou, O., Alhakami, W. and Hamam, H., 2021.	Role of blockchain technology in combating COVID-19 crisis	2021	0
D12	Mulaji, S.S. and Roodt, S.S., 2021.	The practicality of adopting blockchain-based distributed identity management in organisations: A meta-synthesis	2021	0
D11	Smidt, H.J. and Jokonya, O., 2021.	The challenge of privacy and security when using technology to track people in times of COVID-19 pandemic	2021	0

It is good practice to eliminate studies that have never been cited. However, because the number of articles that satisfied our search criteria was low, it was decided to not remove articles that had not been cited. The next section provides the results of the thematic analysis of the 12 articles.

4. Thematic analysis results

The 12 articles were analyzed using the thematic analysis method. The thematic analysis process adopted by the study followed the guidelines of [25], which outline the five key steps for qualitative thematic data analysis: text familiarization, coding of the data, revision of the codes, creation of the themes, and revision of the final themes. These steps were followed to report on the key themes derived from the 12 articles in the inclusion criteria for the SLR process.

4.1 Text familiarization

In the text familiarization step, the articles were read and the persistent keywords that emerged when describing the effect of blockchain on the integrity and transparency of the procurement processes in government organizations were identified. Figure 4 shows the word cloud derived using the Atlas.ti analysis software to present the persistent keywords that emerged from the 12 articles.

4.2. Coding of the data

The keywords identified in the articles described the main objective of the studies. These words were captured and described as the main codes during the coding process of the thematic analysis and are defined in Table 3.

4.3 Revision of the codes

Each of the 12 identified articles highlights some perspectives using the coded keywords to address the aim of this study. Table 4 shows the categories of the articles and their consistency in using the keywords to describe how blockchain enhances the integrity and transparency of government procurement processes.

The analysis of the literature indicates that the codes were not consistently used in all the articles. For example, Election was used in only two articles (D2 and D4), Supply chain was used in three articles (D9, D10, and D12), Voting was used in four articles (D2, D4, D5, and D10), and Skill used in five articles (D1, D7, D8, D9, and D12). We cannot, therefore, conclude that Election, Supply chain, Voting, and Skill are significant in describing the effect of blockchain on the integrity and transparency of government procurement processes.

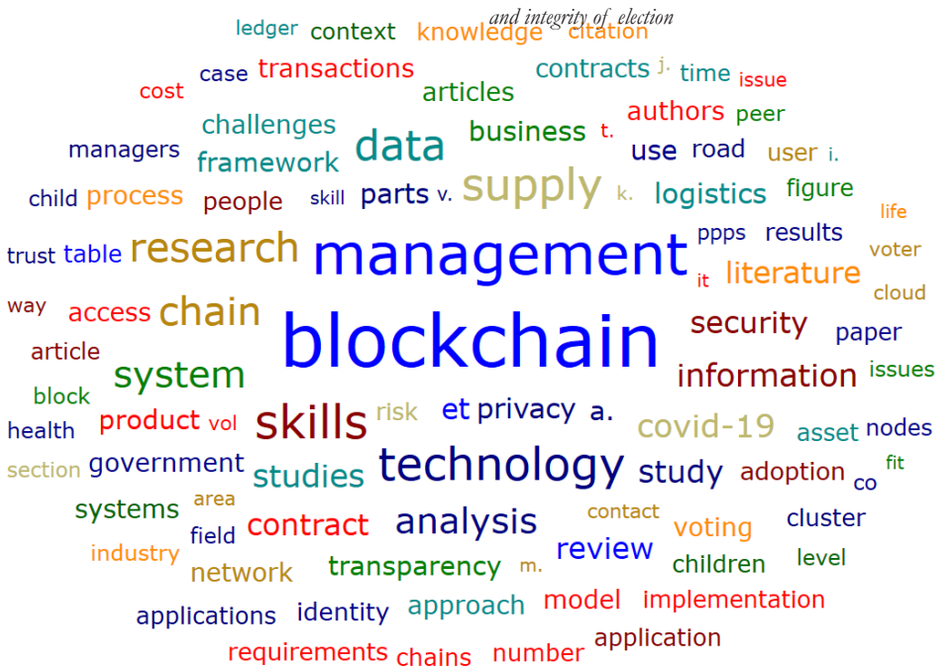


Figure 4. Keywords used to explain the use of blockchain to improve the integrity and transparency of supply chain processes.

4.4 Creation of the themes

The codes were analyzed in terms of the two key themes of the study, namely, integrity and transparency. Integrity refers to upholding ethical standards and the moral values of honesty, professionalism, and righteousness. It is a cornerstone for ensuring fairness, non-discrimination, and compliance in the public procurement process. Transparency is a core principle in public procurement. An open and transparent procurement process improves competition, increases efficiency, and reduces the threat of unfairness or corruption. The codes were grouped according to the key themes and are discussed next.

4.4.1 Integrity

The first group of codes dealt with describing how blockchain improves the integrity of the procurement process. Issues such as handling of contracts, risks involved, security of the data, approaches used, and management of the procurement process emerged as the main issues that influence the integrity of the procurement process. Figure 5 shows the codes linked to integrity.

The following texts from the identified articles highlight how blockchain technology enhances the concept of integrity of procurement processes in line with the identified codes:

"It provides a number of benefits. First, it reduces economic costs, time, and complexities in executing information exchange and administrative functions. Second, it reduces fraud, bureaucracy, and corruption via smart contracts. Furthermore, it offers increased automation, transparency, efficiency, integrity, security, and auditability. Finally, it contributes to increased public trust owing to effective record keeping and information availability." [D1:2 pp 9-11]

"The system used digital signatures to provide message authentication, cryptographic hashes to create hash chains, and provided resistance to coercion, the integrity of vote cast, voter authentication, voter confidentiality, and other quality attributes." [D2:27 p 5]

"Blockchain-based e-voting architecture can potentially address most of the challenges of traditional voting systems and conventional e-voting. These include issues of voter's authentication, verification of votes, protection of voter's privacy, the security of votes, results." [D2:42 p 1]

"In terms of business- or management-related issues, smart contracts are a critical element of blockchain architecture with significant implications. These contracts are employed to create and execute contractual transactions among inter-organisational parties in a trustless manner and subject to pre-determined rules or criteria." [D3:6 p 2]
"…data integrity enhances data accessibility and provides data compatibility, improves management practice for road transport assets, and components in life-cycle cost analyses enable the removal of outdated systems and unproductive assets. This considers both system and project optimisation report useful information periodically, ideally in real-time, facilitate iterative analysis processes that can be performed regularly." [D7:2 pp 4-5]

"Blockchain gives high efficiency to the e-government systems by decreasing the delays and reducing the service operations costs. In addition, it gives access to the automation feature with blockchain and the shared databases… If any counterfeiting endeavour happens, it will automatically be detected. When it comes to security, blockchain has a lot of ameliorating for data confidentiality and consistency. Data integrity and immutability are some of the benefits that are provided to e-Governments involving blockchain technology." [D8:37 p 11]

"Issues related to data integrity are most acute, as data tampering can have a huge impact on mission-critical services that depend upon reliable data… One of the fundamental steps in enforcing data integrity is safeguarding the digital system (such as a network, a website, a database, and an application) using the data through effective identification and authentication management. In this way, only authorised people can access the system and potentially use the data." [D12:13 p 1]

4.4.2 Transparency

The second group of codes dealt with describing how blockchain improved the transparency of the procurement process. Issues such as transaction processing, the chain of events in the procurement process, access to critical data, the application process for securing contracts, the quality of products, costs, and types of contracts emerged as the main ones that influence the transparency of the procurement process. Figure 6 shows the codes linked to transparency.

Table 3. Main codes from the 12 articles

Code	Comment
Transaction	An instance of buying and selling a commodity between the government and SMMEs.
Contract	A written agreement enforceable by law, which binds SMMEs and the government.
Supply chain	The network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product. A supply chain encompasses everything from the delivery of source materials from the supplier to the manufacturer through to the end user, which is the government.
Cost	A sum of money for a product before it can be acquired.
Voting	Used to express a wish to follow a particular course of action.
Product	An article or substance that is manufactured or refined for sale.
Management	The process of dealing with or controlling things or people.
Approach	A way of dealing with a situation or problem.
Application	The action of putting something into operation.
Election	A formal and organized choice by a vote of a person for a political office or other position.
Access	The means or opportunity to approach or enter a place.
Chain	A sequence of items of the same type forming a line.
Skill	The ability to do something well; expertise.
Security	The state of being free from danger or threat.
Risk	The term "business risk" refers to the possibility of a commercial business making inadequate profits due to uncertainties, for example, changes in tastes, changing preferences of consumers, strikes, increased competition, changes in government policy, obsolescence etc.

Table 4. Article categories and their consistency in the use of keywords

ARTICLE	Codes														
	Transaction	Contract	Supply chain	Cost	Voting	Product	Management	Approach	Application	Election	Access	Chain	Skill	Security	Risk
D1	X	X		X		X	X	X	X		X	X	X	X	X
D2	X	X		X	X		X	X	X	X	X	X		X	X
D3	X	X		X		X	X	X	X		X	X		X	X
D4	X	X		X	X	X	X		X	X	X	X		X	
D5	X	X			X	X	X	X	X		X	X		X	
D6	X	X				X	X	X	X		X	X		X	X
D7	X			X		X	X	X	X		X		X		
D8	X	X		X			X	X	X		X	X	X	X	X
D9	X	X	X	X		X	X	X	X		X	X	X	X	X
D10	X	X	X		X	X	X	X	X		X	X		X	X
D11						X	X	X	X		X			X	X
D12	X	X	X	X		X	X	X	X		X	X	X	X	X

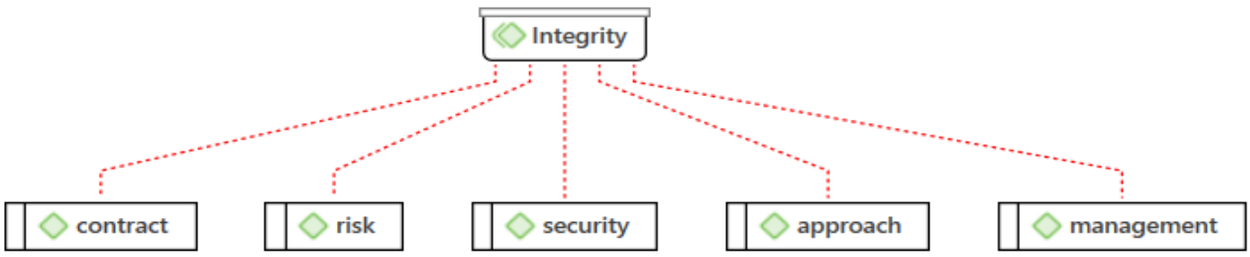


Figure 5. Codes linked to integrity.

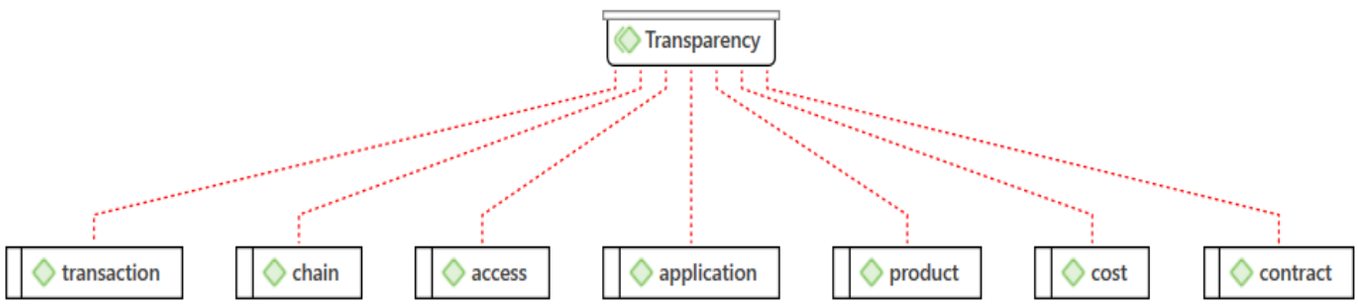


Figure 6. Codes linked to transparency.

The following text highlights the sentiments shared by the identified articles on how blockchain technology enhances the concept of transparency of procurement processes in line with the identified codes.

"Smart contracts can provide the public sector with the ability to ensure certainty and transparency in transactional processes. Over 46 countries across the globe have launched 200 blockchain initiatives. Smart contracts reduce transaction time and costs as the contracts execute themselves by integrating the Internet of Things (IoT) into the blockchain. Contractual fraud is easily detected, thus enhancing the security of contracts." [D1:1 pp 11-12]

"A smart contract is an executable code that enables untrusted parties in a blockchain to directly interact and perform transactions with one another without needing a centralised authority." [D2:2 p 4]

"The decentralised nature of blockchain, and its attributes of anonymity, and transparency make it a suitable approach to handle many of the difficulties associated with conventional e-voting systems." [D2:82 p 1]

"In terms of business- or management-related issues, smart contracts are a critical element of blockchain architecture with significant implications.

These contracts are employed to create and execute contractual transactions among inter-organisational parties in a trustless manner and subject to pre-determined rules or criteria." [D3:6 p 2]

"Indeed, blockchain is a technology that allows a decentralised environment to be created for the executions of transactions without any means of data alteration." [D5:1 p 1]

"…the increase of supply chain transparency is identified as the main objective of recent blockchain projects in supply chain management.

Therefore, most of the recent publications deal with simple supply chains and products. The few approaches dealing with complex parts only map sub-areas of supply chains." [D6:13 p 1]

"Implementation of smart contracts for converting all paper-based contracts that do not have a reliable system that can handle those contracts was delayed during the lockdown worldwide. The paper-based system is not efficient anymore. As such, governments and financial organisations have to do something to keep the businesses running." [D8:10 p 6]

"One of the best options to consider managing the supply chain is blockchain. It can connect all the stakeholders through one decentralised universal network, and securely shows the data of the silos." [D8:39 p 11]

"…with the continued need for SC transparency and sustained record keeping the emergence of blockchain technologies is likely to equip SC managers of the future with skills and knowledge that will create high SC visibility... The managers need not be equipped with the technical skills but should understand the applications and capabilities of the blockchain technologies to help design SCs that leverage the best technologies." [D9:92 p 13]

"The code of each smart contract is stored on the blockchain and can be identified by a unique address. Users can interact with a smart contract in present cryptocurrencies by sending transactions to the contract address. When a user causes a valid new transaction with a smart contract address as recipient, all participants on the mining network execute the contract's code with the current state of the blockchain and the transaction's content as inputs. The network then agrees on the output and the next stage of the contract by participating in a consensus protocol." [D10:2 p 2]

"By formulating logical requirements to create the identification numbers in smart contracts, the processes and their relations in the physical world can be mapped virtually on the blockchain. Thus, each asset receives a virtual identity. A complete integration of this approach in the whole manufacturing supply chain ensures the secure traceability, authenticity, and auditability of each assembled product and its components. Therefore,

transparency can be increased for all stakeholders and vulnerabilities that allow counterfeit parts to enter the supply chain can be reduced. The implementation of blockchain on a public platform provides full transparency for the customer, while the implementation on a private blockchain network only provides a restricted transparency." [D10:22 p 5]

4.5 Finalization of the themes

The two main themes of the study are integrity and transparency. The study identified 12 articles in the research literature that explain how blockchain technology enhances the integrity and transparency of the procurement processes of government organizations. A document network was created from the identified articles to categorize the articles according to their emphasis on integrity and transparency. This is depicted in Figures 7 and 8.

From the analysis of the documents above, it is evident that articles D7 and D11 did not emphasize addressing the use of blockchain technology with respect to enhancing the integrity and transparency of the procurement processes. Although the articles made the inclusion criteria for the SLR,

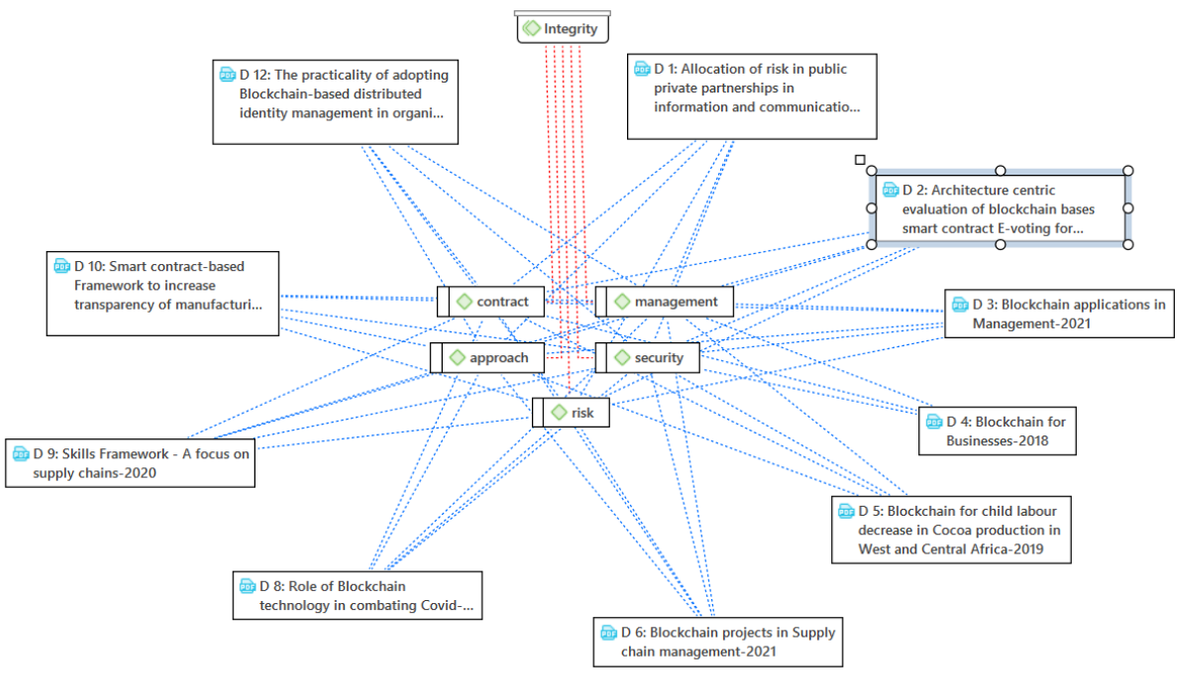


Figure 7. Articles explaining how blockchain enhances the integrity of the procurement processes.

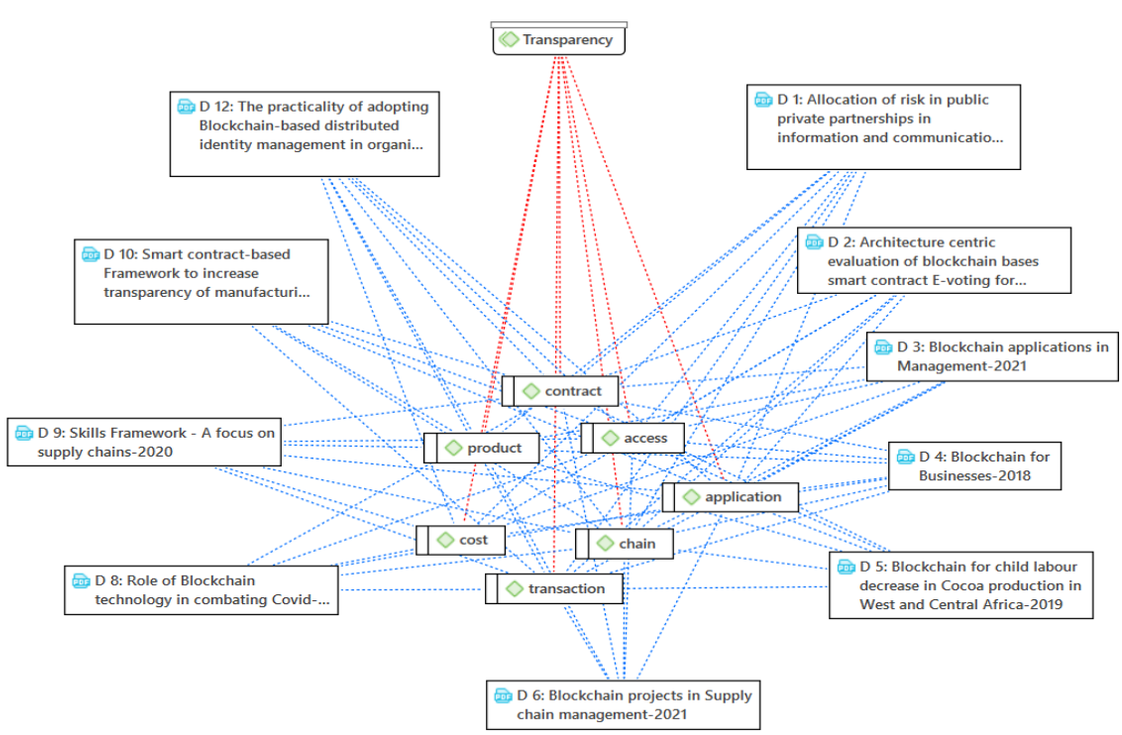


Figure 8. Articles explaining how blockchain enhances the transparency of the procurement processes.

they were not significant in terms of the effect of blockchain technology on government procurement processes.

5. Discussion

The results show that 10 of the 12 articles that satisfied the PRISMA criteria of selection were conclusive in answering the aim of the study. The 10 articles addressed issues of transparency and integrity when using blockchain technology. According to the results, the following are the main factors that drive the integrity of procurement processes when using blockchain: handling of contracts, risks involved, security of the data, approaches used, and management of the procurement process. The following are the main factors that drive transparency: transaction processing, the chain of events in the procurement process, access to critical data, the application process for securing contracts, the quality of products, costs, and the types of contracts. This finding implies that when the SA government intends to implement blockchain technology in their procurement processes, the abovementioned are the factors to consider in order to ensure that the system addresses these concerns and fosters integrity and transparency.

To improve the integrity of the procurement processes or the transactions between the SA government and SMMEs, the former must implement blockchain technology. Blockchain technology will improve integrity through the ways in which it handles contracts (smart contracts), secures data, and manages the procurement processes. According to [25] blockchain technology reduces fraud, bureaucracy, and corruption via smart contracts. Furthermore, it offers increased automation, transparency, efficiency, integrity, security, and auditability. Finally, it contributes to increased public trust owing to effective record keeping and information availability. Once the SA government has implemented blockchain technology, the citizens and SMMEs should be more trustful of the government. This should encourage them to transact with the government as they are guaranteed integrity and the award of tenders that are fair and fraud-free.

Data in traditional systems suffer from various challenges such as the lack of security, integrity, reliability, and convenience because they do not have a consistent structure for data security and reliable policies [26]. Therefore, in their study, the authors [26] propose a blockchain-based integrity and reliable information management system to address these challenges. The results of their study demonstrate the effectiveness and robustness of their proposed blockchain-based integrity and reliable information management system. This is in line with our findings that the integrity of procurement processes will be improved through the implementation of blockchain-based procurement systems because they will foster security, integrity, reliability, and convenience of the data (such as smart contracts) that are going to be stored in the blockchain system. Blockchain technology has also been applied to cloud computing systems to improve data security and trust (integrity) in computing or processing [27], [28]. While several models and solutions exclusive of blockchain have been proposed such as data integrity tests and secure multi-party calculations [27], they have not been successful in assuring users of data integrity and security. Therefore, the introduction of blockchain-based data integrity mechanisms has seen significant strides being made toward data integrity and security.

The use of blockchain will not allow users to tamper with contracts or the data saved into the blockchain [29]. According to [29], blockchain is a technology that allows a decentralized environment to be created for the execution of transactions without any means of data alteration. Furthermore, transparency will be emphasized using blockchain technology in that the way the technology handles and processes transactions, eliminates altering the already saved records. According to [30], smart contracts can provide the public sector with the ability to ensure certainty and transparency in transactional processes. Therefore, when all contracts between the SA government and the SMMEs are managed and processed via blockchain technology, transparency and integrity will be enforced.

6. Limitations and future work

This study, like any other, has limitations. First, this study is only theoretical, implying that empirical validation of the factors explored in the context of the SA public sector is required. Second, this review demonstrated a low publication rate of blockchain studies relative to global figures, indicating the need for significantly increased blockchain research in the context of SA.

7. Conclusion

Corruption has caused several economies to crumble and struggle owing to the devastating effect it has on the communities. This study conducted a SLR to theoretically investigate the use of blockchain technology to improve the integrity and transparency of procurement processes between SMMEs and the SA government. The Scopus database was used to search for relevant research literature and, following the PRISMA framework, 12 articles that met the eligibility criteria were identified. The 12 articles were analyzed using thematic analysis and the results demonstrated that 10 of the articles applied to this study as they discussed the use of blockchain in relation to integrity and transparency. The remaining two articles did not emphasize the use of blockchain technology in enhancing the integrity and transparency of the procurement processes. The common factors in the 10 articles that were found to impact integrity and transparency were as follows: handling of contracts, risks involved, security of the data, approaches used, management of the procurement process, transaction processing, the chain of events in the procurement process, access to critical data, the application process for securing contracts, quality of products, costs, and types of contracts. This finding implies that when the SA government implements blockchain technology in their procurement processes, these are the factors to consider to ensure transparency and integrity. We believe that once blockchain technology has been implemented in SMMEs, the public will trust and be confident in the procurement processes as corruption would have been eliminated and tenders would be awarded fairly.

Based on these findings, there is a need for further research. Further research should focus on empirically validating the factors identified in this study. Furthermore, the identified factors can be triangulated into a framework that informs the implementation of blockchain technology.

References

[1] O. N. Cordelia, N. H. Ngozi, and A. A. Ebuka, "Accountability and transparency in nation building: A Covid-19 experience in sub-Saharan Africa," Int. J. Public Policy Adm. Res., vol. 7, no. 1, pp. 23–33, 2020.

[2] L. M. Akimova, I. F. Litvinova, H. O. Ilchenko, A. L. Pomaza-Ponomarenko, and O. I. Yemets, "The negative impact of corruption on the economic security of states," Int. J. Manag., vol. 11, no. 5, pp. 1058–1071, 2020.

[3] M. D. Powell, "International efforts to combat corruption," in Proceedings of 2017 Annual Conference of the ASPA, Atlanta, Georgia, vol. 17, no. 21, pp. 4–5, 2017.

[4] A. Addo and P. K. Senyo, "Digitalization and government corruption in developing countries: Towards a framework and research agenda," in AOM Journals, 2020, vol. 2020, no. 1.

[5] B. A. Olken and R. Pande, "Corruption in developing countries," Annu. Rev. Econ., vol. 4, no. 1, pp. 479–509, 2012.

[6] P. Bardhan, "Corruption and development: A review of issues," J. Econ. Lit., vol. 35, no. 3, pp. 1320–1346, 1997.

[7] "Ramaphosa's 2022 Sona on corruption: Is that it?" https://www.dailymaverick.co.za/opinionista/2022-02-11-ramaphosas-2022-sona-on-corruption-is-that-it/ (accessed Feb. 18, 2022).

[8] G. Sabanidze, A. Kivenko, P. Benics, G. Kalkan, and A. Tick, "The importance of SMEs in economic development of developing countries," Manag. Enterp. Benchmarking 21st Century, pp. 91–104, 2021.

[9] M. Moos and W. Sambo, "An exploratory study of challenges faced by small automotive businesses in townships: The case of Garankuwa, South Africa," J. Contemp. Manag., vol. 15, no. 1, pp. 467–494, 2018.

[10] M. Herrington, P. Kew, and A. Mwanga, "GEM South Africa 2016-2017 report," Global Entrepreneurship Monitor, 2017.
[11] S. Bvuma and C. Marnewick, "Sustainable livelihoods of township small, medium and micro enterprises towards growth and development," Sustainability, vol. 12, no. 8, p. 3149, 2020.
[12] A. Mungiu, "Corruption: Diagnosis and treatment," J. Democr., vol. 17, no. 3, pp. 86–99, 2006.
[13] A. Ahmad, "Corruption as a contagious psychosocial disorder, a conceptual analysis," Duhok Med. J., vol. 14, no. 1, pp. 19–27, 2020.
[14] D. N. Maepa, M. F. Mpwanya, and T. B. Phume, "Readiness factors affecting e-procurement in South African government departments," J. Transp. Supply Chain Manag., vol. 17, pp. 874, 2023.
[15] T. M. Lukhele, B. Botha, and S. Mbanga, "Content analysis and ranking of irregularities in public sector construction procurement in South Africa," Int. J. Constr. Supply Chain Manag., vol. 12, no. 1, pp. 50–71, 2022.
[16] M. S. Soni and J. J. Smallwood, "Perceptions of Corruption in the South African Construction Industry," Int. J. Constr. Educ. Res., pp. 1–22, 2023.
[17] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," Transp. Res. part e Logist. Transp. Rev., vol. 142, pp. 102067, 2020.
[18] B. Vivekanadam, "Analysis of recent trend and applications in block chain technology," J. ISMAC, vol. 2, no. 04, pp. 200–206, 2020.
[19] S. V. Akram, P. K. Malik, R. Singh, G. Anita, and S. Tanwar, "Adoption of blockchain technology in various realms: Opportunities and challenges," Secur. Priv., vol. 3, no. 5, p. e109, 2020.
[20] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," J. Clean. Prod., vol. 260, pp. 121031, 2020.
[21] M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," Int. J. Prod. Econ., vol. 231, pp. 107831, 2021.
[22] F. R. Batubara, J. Ubacht, and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," in Proceedings of the 19th Annual International Conference on DG.O Research: Governance in the Data Age, pp. 1–9, 2018.
[23] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," BMJ, vol. 372, pp. 105906, 2021.
[24] K. Schwab, "The fourth industrial revolution," World Economic Forum, Geneva, 2016.
[25] N. E. L. Danielle, "Allocation of risk in public private partnerships in information and communications technology," Int. J. Ebus. Egovernment Stud., vol. 12, no. 1, pp. 17–32, 2020.
[26] N. Iqbal, F. Jamil, S. Ahmad, and D. Kim, "A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services," IEEE Access, vol. 9, pp. 8069–8098, 2021.
[27] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," Futur. Gener. Comput. Syst., vol. 102, pp. 902–911, 2020.
[28] H. Han, S. Fei, Z. Yan, and X. Zhou, "A survey on blockchain-based integrity auditing for cloud data," Digit. Commun. Networks, vol. 8, no. 5, pp. 591–603, 2022.
[29] R. B. Senou, J. Dégila, E. C. Adjobo, and A. P. M. Djossou, "Blockchain for child labour decrease in cocoa production in West and Central Africa," IFAC-PapersOnLine, vol. 52, no. 13, pp. 2710–2715, 2019.
[30] A. Tandon, P. Kaur, M. Mäntymäki, and A. Dhir, "Blockchain applications in management: A bibliometric analysis and literature review," Technol. Forecast. Soc. Change, vol. 166, pp. 120649, 2021.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
All authors contributed equally to the manuscript.

Funding:
None declared.

Acknowledgements:
I would like to thank the Department of Applied Information Systems at the University of Johannesburg.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-2-(8)2023

Designing a Blockchain-Based Customer Loyalty Programme using Design Science Research Method

Milad Behrouzi, Amir Albadvi, Parimah Emaadi Safavi
Tarbiat Modares University, Tehran, Iran

Correspondence: albadvi@modares.ac.ir
Received: 15 December 2022 **Accepted:** 08 July 2023 **Published:** 30 September 2023

Abstract

Loyalty programmes are crucial marketing tools for businesses to increase customer engagement and retention. These programmes, sponsored by enterprises, offer rewards, discounts, and other incentives to attract and retain customers. However, the lack of interoperability among loyalty programmes of different organisations can limit the customer's ability to maximise the value of their loyalty points. In this study, we proposed the design and implementation of a blockchain-based platform using the design science research (DSR) method as a candidate solution to overcome the limitations of conventional loyalty programmes. Using smart contracts, the design enables organisations to embed all necessary attributes for their desired customer loyalty programmes in accordance with their policies. The designed platform provides a decentralised, transparent, and secure environment for the exchange of loyalty tokens between various organisations and customers. Using expert opinion methodology, we discussed the technical considerations and implementation of the blockchain-based loyalty programme platform, as well as its potential impact on the customer experience. Our findings suggest that the proposed platform can improve the interoperability of loyalty programmes using a universal token that creates more value for businesses and customers. The research contributes to the field of loyalty programmes and blockchain technology by proposing a platform that enable businesses to develop more effective and data-driven loyalty strategies, while providing customers with better value for their loyalty points.

Keywords: *Blockchain Technology, Loyalty Programme, Marketing, Design Science Research*

JEL Classifications: *L14, M31*

1. Introduction

The advent of diverse computer technologies and networks has resulted in significant and expeditious transformations across all domains. Among the common practices experienced by individuals in their lifetime is the utilisation of loyalty programmes by organisations providing services or products. Such programmes aim to retain customers within the organisation and enhance their share of wallet [1].

In recent years, numerous organisations have begun to accumulate customer data to monitor and analyse their behaviour [2]. By studying this data, organisations try to design a loyalty programme to keep current customers satisfied and attract new customers.

Loyalty programmes include integrated systems of personalised customer marketing and marketing communications, offering tangible (such as discounts or gifts) or intangible (such as personalised service or information) rewards to the customer [3], [4].

Customers may be members of multiple loyalty programmes from various organisations that use disparate methods to provide and manage services, such as physical coupons, digital coupons, or specialised mobile applications. The absence of interoperability among loyalty programmes of various organisations leads to a situation where consumers face difficulty in effectively utilising the value of their loyalty points, given that each organisation offers its own system and rewards. Additionally, privacy concerns may dissuade customers from sharing personal information with every loyalty programme [5].

Blockchain technology is a distributed database comprising encrypted blocks of asset transactions that are sequentially ordered, digitally signed, and governed by a consensus model [6]. The technology's potential in addressing these loyalty programme challenges is noteworthy. By embedding the terms of loyalty programmes in a smart contract, blockchain enables organisations to determine the precise reward and profit amounts to be disbursed to their customers, without the need for trust, in a transparent manner. This contract is executed independently and is used to manage the transaction [7].

Providing a suitable blockchain platform for the exchange of these privileges between internal and external customers is possible by creating a token. Tokens are a form of incentive given to customers for participating in a loyalty programme. These tokens are stored on the blockchain and represent specific assets, such as currencies or products.

The blockchain platform offers a secure environment for the exchange of tokens between various organisations after mutual agreement. By employing tokens, integration and collective benefits of all loyalty programmes become feasible. Tokens are not limited to purchases but can also encompass the overall customer interaction with the brand or retailer, resulting in the integration of digital marketing [8].

By providing an integrated and trustless platform, blockchain can control the transfer and manage the number of customer assets in any organisation with the help of tokens in its platform [9]. Blockchain provides the basis for unifying the type of awards between organisations [10].

Furthermore, organisations can provide the possibility of transferring

their points with each other by agreeing between themselves and using a common platform, so that both the management and maintenance costs of their loyalty programmes are reduced and providing more valuable options to customers themselves should also provide ways to improve their level of satisfaction. For example, several hotels and airlines offer their points to their customers on the same platform using the same method [11].

As of now, the main disadvantages of using blockchain in this scope are the implementation of the structure and costs. Besides, due to the nature of blockchain, correcting a mistake is rather impossible or very costly. Some of these advantages and disadvantages are given in Table 1.

Table 1. The opportunities and limitations of blockchain-based loyalty programmes

Opportunities	Limitations
Transparency and Security: Blockchain technology provides a tamper-proof and transparent record of transactions, ensuring that loyalty points cannot be fraudulently altered or stolen.	**Technical Complexity**: Implementing blockchain technology can be technically complex and may require specialised expertise, increasing the costs and potential for errors.
Increased Efficiency: Blockchain technology can automate loyalty program processes, such as point issuance, redemption, and transfer, reducing administrative costs and improving customer experience.	**Lack of Standardisation**: As blockchain is a relatively new technology, there is a lack of standardisation, which can create interoperability issues and make it difficult to integrate with existing systems.
Enhanced Customer Loyalty: The use of blockchain technology can provide customers with a greater sense of trust and loyalty towards a brand, knowing that their loyalty points are secure and transparent.	**Technical Limitations**: Blockchain technology is still evolving and has limitations, such as the difficulty of modifying existing transactions and the risk of smart contract vulnerabilities.
Lower Costs: Blockchain can reduce the costs associated with loyalty programme administration, since it eliminates the need for intermediaries and reduces operational costs.	**Limited Scalability**: The current limitations of blockchain technology, such as transaction speed and storage capacity, may make it difficult to scale loyalty programmes with large customer bases.

In this article, we will explore the design and implementation of a blockchain-based platform for loyalty programmes via a design science research approach. We aim to explore blockchain potential to solve mentioned problems in loyalty programmes. Throughout this article, we discuss the benefits of using blockchain for loyalty programmes, the technical considerations in designing such a platform, gaining insights from experts, and the potential impact on the overall customer experience. By the end of this article, readers will have a better understanding of if blockchain technology can transform the loyalty programme landscape and create more value for both businesses and customers.

2. Methodology

Choosing the appropriate research model in the research process is vital in explaining its validity to the audience. Also, the introduction of the research model facilitates and expands future research. The methodology used in this study is the approach of design science research [12] as a research method used in information technology to develop and evaluate artefacts or practical problems. In this case, we utilised this methodology to leverage blockchain opportunities to optimise loyal points transfer among customers of various loyalty programmes [12, 13, 14].
In this method, we identified loyal points transfer problems and developed a technology solution to address these problems. The solutions developed are evaluated through gaining knowledge from a list of experts [15], and the findings are able to be used to refine the design or develop new solutions.

2.1 Design science research methodology

Design science research is a problem-solving paradigm that seeks to enhance human knowledge by creating innovative artefacts [14]. Using the DSR approach, the result of our work will be a product and a pragmatic view of the identified problem. Figure 1 illustrates the steps and processes underlying the design science research method [14].

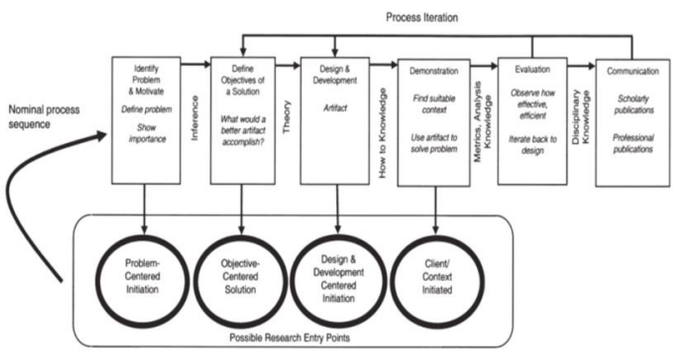


Figure 1. DSR process.

We benefited from six steps below in the design science research approach.

2.1.1 Problem identification and motivations

The first step in the design is to define the specific research problem and justify the value of a solution. In this study, our problem is t he lack of a safe and trustless method to grant, use, and exchange points obtained through customer loyalty programmes to customers and among organisations. Providing a safe and efficient platform for transferring privileges increases the efficiency of these loyalty programmes. As a result, productivity in loyal programmes would increase.

The purpose of customer loyalty programmes is to increase customer engagement with the organisation and to satisfy customers to allocate more significant portion of their wallet to the services or products of the organisations [16]. For that matter, there are many psychological methods which attract customers, leading to profitable outcomes for organisations [17, 18, 19, 20, 21, 22, 23, 24]. The key psychological method employed in our study is the status-based mechanism [20], which examines the perceived value by the customer through gifts and discounts [21]. By using the mentioned method, we identified problem and motivation for creating an artefact to enhance loyalty programme potentials.

2.1.2 Necessary factors for solving the problem

We can deduce goals by defining the problem and investigating solution possibilities. These objectives can be quantitative or qualitative and inferred from the problem specification. In this section, we select our blockchain platform according to the customer and organisation needs [25] and implement a smart contract that covers the rules of loyalty programmes through this platform. In the next step, we create tokens and transfer them to a wallet for easy transfer and proof of executing the artefact.

- Blockchain platform

Blockchain platforms vary in type, with some lacking smart contract support and being excluded from our selection. Others charge high fees

without offering a competitive advantage, citing technical reasons, support, or popularity. Our design employs the Binance Smart Chain platform, which offers cost-effective smart contract functionality to users.

- Wallet

In order to store tokens generated for the organisation and transfer tokens to users who have received a certain amount of them, it is necessary to store the tokens in a wallet under the supervision of the organisation so that the organisation can transfer them according to loyalty programme regulations. Automated transfer of digital currencies among customers and organisations necessitates the use of a digital wallet. The conversion of tokens to fiat currency or their offline transfer are regulatory measures that are employable and fall under the purview of organisational consensus.

- Unique token

The unique token is an intangible reward offered by organisations to users who use their service or purchase their product. Users earn points by adhering to the rules of the customer loyalty programme. The tokens are transferable within the platform, allowing customers to exchange them and use them for various benefits in the loyalty programme.

- Smart contract

A smart contract is a set of logical rules in the form of a cryptographic script that can be embedded within the blockchain [26], [27]. Upon implementation on the desired blockchain platform, the rules will become immutable and binding. Organisational considerations such as token transferability, creation, and burning may be incorporated into these contracts. Solidity, a programming language similar to JavaScript, is well-suited for building decentralised applications and is utilised for contract writing [9].

2.1.3 Design and development

In this phase, a DSR chrolo refers to any object that incorporates our research contribution. This involves identifying the intended functionality and design of the artefact.

We undertook the task of identifying various scenarios for our tokens and devising the execution mechanism within the network. The fundamental elements of the network comprise the token and the users' categories. As illustrated in Table 2, there are types of users in three different roles. These roles include the partner as a person who gives loyalty points to members of this loyalty programme, a member who receives points from their purchases and spends those points, and a manager who supervises the partners' affairs [11].

Table 2. User stories for the rewards points system

US_{01}	As a partner, I assign rewards points to members to encourage their loyalty as clients
US_{02}	As a member, I pay with the accumulated points to save money and enjoy the programme benefits
US_{03}	As a member, I see the balance of my points to know how many I have
US_{04}	As a member, I see a report of transactions
US_{05}	As a member, I approve the points charges, to be sure that other people do not spend them
US_{06}	As an administrator, I manage partners' data (registrations, cancellations, and changes) in the system and I see all the members.

Various transactions and user stories can occur within this network (see Table 3 [11]).

Upon reviewing the users' narratives, we identified the essential regulations that must be integrated into the smart contract. These rules pertain to the transfer, allocation, and expenditure of tokens. Although these rules could be inferred from studying existing loyalty programmes, we emphasised a scientific approach to this endeavour. So, we used the Remix website to write the smart contract to provide an online solidity-based coding platform. The final version of the smart contract code is shown in code 1.

The smart contract is assumed applicable for all transactions. Organisations adopt this mechanism based on their preferences. For instance, the organisation may consider each loyalty point as a token, or they may consider ten points equivalent to a single token. In case an organisation selects a specific policy for the conversion rate of points to tokens, it must be adhered to by its partner organisations. The organisations are required to engage in consultation and mutually agree on this ratio before making a final decision. To avoid potential mathematical complications in the future, it is recommended that each point be deemed equal to one token, as it allows for easy determination of the desired number of tokens.

Table 3. User stories

	Given	When	Then
TC_{01}	M1 has 1 point and P1 has 9999 points	P1 rewards M1	M1 has 2 points and P1 has 9998 points
TC_{02}	M' has 0 points and P1 has 9999 points	P1 rewards M'	M' has 0 points and P1 has 9999 points
TC_{03}	M1 has 1 point and P1 has 0 points	P1 rewards M1	M1 has 1 point, and P1 has 0 points and recieves a message warning that it does not have enough points
TC_{04}	M1 has 10 points and P1 has 0 points	M1 pays 1 point to P1	M1 has 9 points and P1 has 1 point
TC_{05}	M1 has 0 points and P1 has 0 points	M1 pays 1 point to P1	M1 has 0 points, and P1 has 0 points and recieves a message warning that it does not have enough points
TC_{06}	M1 has 10 points	M1 asks for his balance	M1 is notified that he has 10 points
TC_{07}	M1 has 10 points, and P1 has 10 points and recieves a message warning that it is collecting from a wrong member	P1 collects rewards given to M2	M1 has 10 points and P1 has 10 points
TC_{08}	M1 has 10 points and P1 has 10 points	P1 collects 1 point given to M1 and M1 provides his PIN	M1 has 9 points and P1 has 11 points
TC_{09}	There are three partners	Administrator inserts partner X with the number 1234567890	There are four partners
TC_{10}	There are three partners	Administrator inserts partner X with the number 12345	There are three partners

After setting up the smart contract, it was necessary to place the created

tokens in the wallet of the organisation benefiting from this blockchain to distribute them among its members. We utilised the user-friendly and cost-effective Metamask wallet for our operations. Additionally, we employed the Binance virtual test network to evaluate the efficiency of the smart contract, as elaborated in subsequent sections.

```
pragma solidity ^0.8.2;

contract Token {
    mapping(address => uint) public balances;
    mapping(address => mapping(address => uint)) public allowance;
    uint public totalSupply = 21000000 * 10 ** 18;
    string public name = "My Token";
    string public symbol = "TKE";
    uint public decimals = 18;

    event Transfer(address indexed from, address indexed to, uint value);
    event Approval(address indexed owner, address indexed spender, uint value);

    constructor(){
        balances[msg.sender] = totalSupply;
    }

    function balanceOf(address owner) public view returns(uint) {
        return balances[owner];
    }

    function transfer(address to, uint value) public returns(bool) {
        require(balanceOf(msg.sender) >= value, 'balance too low');
        balances[to] += value;
        balances[msg.sender] -= value;
        emit  Transfer(msg.sender, to, value);
        return true;
    }

    function transferFrom(address from, address to, uint value) public returns(bool) {
        require(balanceOf(from) >= value, 'balance too low');
        require(allowance[from][msg.sender] >= value, 'allowance too low');
        balances[to] += value;
        balances[from] -= value;
        emit Transfer(from, to, value);
        return true;
    }

    function approve(address spender, uint value) public returns(bool){
        allowance[msg.sender][spender] = value;
        emit Approval(msg.sender, spender, value);
        return true;
    }
}
```

Code 1. Smart contract.

2.1.4 Product display

This phase entails utilising the artefact in experiments, simulations, case studies, proofs, or other relevant activities. Our final product is a blockchain platform integrated with a smart contract that governs the loyalty programme. The provisions encoded within this smart contract are customised to cater to the requirements of loyalty programmes. This blockchain platform has the capability to allocate tokens to customers, receive tokens from other customers, and facilitate token transfers between two customers or among customers and organisations.

2.1.5 Evaluation

Evaluation assesses the effectiveness of the artefact in resolving the problem by comparing the intended solution with the observed outcomes of the artefact's implementation. This process can encompass diverse evaluation methodologies that align with the problem domain and the artefact's nature. Following this phase, the decision to revise the artefact's efficacy by revisiting the third step or to proceed with communication and leave any potential enhancements for future undertakings is determined.

To evaluate the implemented blockchain, we executed various network operations on the Binance virtual test network to assess its functionality. In the next step, we aimed to assess the practicality of the artefact and identify any potential obstacles in its implementation by soliciting expert opinions.

2.1.6 Communications

Here, all aspects of the problem and the designed artefact were communicated to the stakeholders. Depending on the research objectives and the audience, including professionals, appropriate forms of communication could be employed.

Finally, it should be noted that the design science research approach methodology has a back-and-forth behaviour. It is important to note that the outcomes reported in each section are the cumulative result of the entire process and not solely the consequence of a single stage. Each stage contributes to the final result and represents a crucial step towards achieving the desired objectives. Therefore, it is the combined effort and progress made throughout all stages that lead to the final outcome.

2.2 Expert opinion methodology

This method is employed to make predictions or estimates when there is inadequate information available to conduct statistical procedures [13]. This method operates innovatively and endeavours to solve obscure or unresolved problems. Knol et al. describe this method in seven steps [28]:

2.2.1 Determining uncertainties (identifying variable values)

In this section, we have discussed the importance of obtaining expert opinions and how it can help us in evaluating the feasibility and identifying potential challenges in implementing the proposed solution. Challenges addressed here include required infrastructures for implementing and examining the blockchain platform, technician training needs, and technical updates.

2.2.2 Scope and format of extraction

Here we created a questionnaire in a general format of questions. Various factors such as time and cost were taken into account to determine the appropriate method of gathering expert opinions, including interviews, questionnaires, face-to-face or telephone conversations, and opinion summarisation.

This study utilised interviews with multiple experts from diverse fields and incorporated a selection of their opinions. An eight-question survey was compiled, which was administered both in-person and online, and encompassed topics such as software, hardware, human resources, and future-proofing.

2.2.3 Identification and selection of experts

In the expert opinion method, it is important to define the criteria for identifying individuals who can be considered experts. An expert is a key person who:

- has significant knowledge of the problem area
- has a background in the discussed field
- is known (e.g., among colleagues) and competent in solving the problem
- is familiar with the assessment of possibilities.

Additionally, the expert's opinion should change over time as the expert receives new information and also the expert's opinions should be valid, transparent, science-based, and justifiable. Nevertheless, there are also criteria to recognise an expert:

- Tangible evidence of expertise (e.g., degree, publications, position)
- The fame
- Availability and willingness to participate
- Understanding the general problem area
- Neutrality
- Having no economic or personal stake in potential findings

2.2.4 Design of extraction manuals

The questions should have had a specific format and move towards a conclusion for the main purpose. These questions were in the form of statistical, probabilistic, and qualitative estimates.

2.2.5 Preparation of the extraction session

The meetings were held in person, by phone, or online depending on the person's time and availability.

2.2.6 Relying on the opinion or judgment of an expert

In order to use the opinions of experts, it was necessary to reach a consensus on those opinions if we have used several experts.

2.2.7 Summary, aggregation, and reporting of results

Finally, the collected answers were aggregated based on a scoring system.

3. Results

A customer journey map was created to illustrate the processes that customers and organisations undergo in this system. A customer journey map is a visual representation of the steps, activities, and situations a customer goes through to achieve a specific goal, including customer needs and emotions. The design processes were carried out so that the maximum level of automation follows the minimum level of human involvement. Figure 2 illustrates the journey map. As illustrated, the map considers the user experiences along with the chronological steps in system from the smart contract execution until the tokens have transferred to user's wallet.

3.1 Evaluation of transactions

Once the smart contract is implemented, it is essential to transfer the tokens generated by the contract to a designated account, such as the account of the organisation that initiated the creation of these tokens. The Remix site facilitates the interactive deployment of the smart contract code.

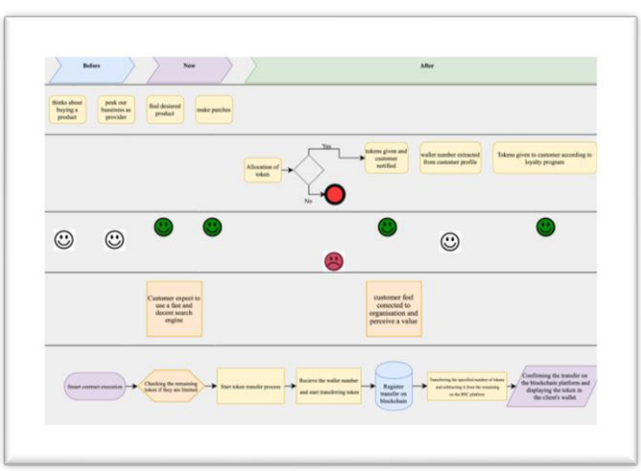


Figure 2. Customer journey map.

To transfer tokens from the deployed smart contract, we interacted on the blockchain using Remix. Then we used the "Deploy and run transactions" menu and entered the address of the desired Metamask wallet along with the number of tokens we wanted to transfer. The Metamask prompt opened automatically for session. Once the transaction was confirmed the tokens were transferred to the receiver's wallet.

To check the completion of the Binance blockchain platform transactions, we used the "BSC Scan" website. The results are shown in Figure 3.

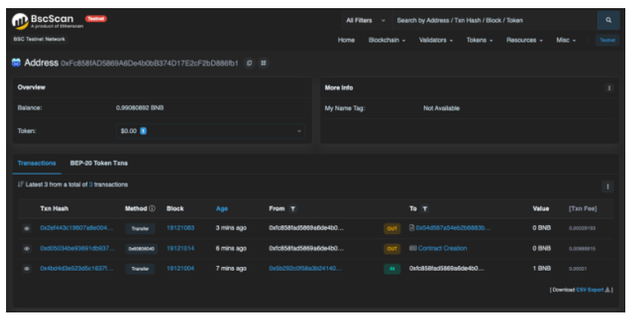


Figure 3. Token journey.

By choosing our token (TKN), we will be transferred to the information page of that token as shown in Figure 4.

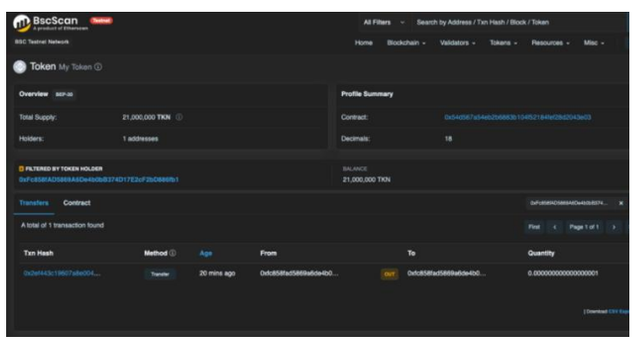


Figure 4. Proof of execution.

All information regarding the wallet address, methods, and time of the transfer shown in Figure 4 confirms the execution within the blockchain.

3.2 Evaluation using expert opinion

We created a questionnaire to obtain feedback from experts regarding the implementation of the project and potential challenges. The questionnaire also allowed experts to provide suggestions for improvement. The primary rationale for using expert opinions is to mitigate the high costs of implementing projects in organisations, the prolonged time required for large-scale project troubleshooting, and the increased risk of customer information loss for the organisation. Some of the questions and expert opinions are given in Table 4.

According to the opinion of respected experts, implementing this project is possible but facing challenges, like internal resistance and advertising costs, must be carefully addressed.

Regarding the software aspect, the experts generally agree that the system can work effectively with trained technicians. However, some experts suggest that a mechanism should be adopted for organisations that currently use traditional loyalty programmes, allowing their customers to transfer their points to the new blockchain-based platform.

According to the questionnaire, experts have confirmed the usefulness of the artefact for customers and observed a high potential for increasing customer satisfaction and wallet share due to the increase in interaction with the organisation.

4. Conclusion

After an extensive literature review, the decision was made to explore

Table 4. Expert opinions questionaire

Expert	Expertise Areas	Question 1: How do you rate the artifact deploy abiliy (1–10)?	Question 2: How do you evaluate the operational and training costs for deployment?	Question 3: How do you conclude with the advantages and disadvantages of the design?	Question 4: What are other considerable aspects and criterias?
1	Sales management	7	High	Advantages outweigh disadvantages	Measuring customer affinity beforehand
2	Data science/ eCommerce consulting	4	High	Advantages outweigh disadvantages	Investigating precise costs and long-term goals of cooperation
3	Financial management/ Customer loyalty programme design	8	High	Advantages outweigh disadvantages	Investigating customer prevalances and needed infrastructures
4	Social networks management/ Full stack developer	9	Very high	Advantages outweigh disadvantages	Evaluating clear regulations in terms of contracts and interoperability of programmes

blockchain technology to utilise their potential benefits in customer loyalty programmes. Using the DSR approach and expert opinions, we developed a model with defined conditions which involved collecting user stories and scenarios to identify network usage patterns, followed by writing a smart contract to meet the identified needs and deploying it on the Binance Smart Chain platform. The created artefact was then tested and its efficiency and effectiveness were confirmed through successful transactions. Additionally, we sought the opinions of experts in related fields through an expert opinion approach. Their feedback on the system's efficacy, potential challenges, and opportunities for commercial implementation was collected and summarised.

Our research indicates that blockchain technology offers valuable services that can enhance customer satisfaction, such as token-based point transfers, interoperability, and eliminating the need for paper coupons. The primary objective of such benefits is to capture a larger portion of customers' wallets, which aligns with the primary goal of loyalty programmes. This research aimed to enhance the productivity of loyalty programmes by leveraging blockchain technology.

Based on our research findings, it appears that replacing traditional loyalty systems with blockchain-based platforms is less complicated than previously believed. Complex organisational structures and financial barriers have previously hindered the implementation of this technology. Nevertheless, our proposed platform and smart contract implementation need minimal costs in the case of hardware. Furthermore, increased transparency in wallet transactions may encourage customers to utilise their loyalty points.

During the course of our study, we encountered several limitations, including the bureaucratic structures inherent in organisations, which currently impede the widespread adoption of this method. Additionally, the high costs associated with its implementation, adaption, and lack of cooperativity of organisations compelled us to limit our optimisation efforts after the communication phase of the design science research approach.

In conclusion, loyalty programmes based on blockchain technology have exhibited advantages for both users and organisations. The adoption of this platform allows organisations to collaborate and implement measures to enhance customer satisfaction. Furthermore, the transparency offered by blockchain technology can foster trust and confidence among users, leading to the expansion of economic relationships through the creation of a standardised token and its distribution in accordance with predefined guidelines. Consequently, conducting large-scale implementation would yield collateral benefits, such as the acquisition of significant data regarding customer behaviour, and optimise the overall customer experience. Therefore, further research focusing on the implementation and communication phases of the design process is necessary.

For references visit https://doi.org/10.31585/jbba-6-2-(8)2023

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
The authors designed and coordinated this research and prepared the manuscript in its entirety.

Funding:
None declared.

Acknowledgements:
Not applicable.

CONFERENCE PROCEEDINGS

6th Blockchain International Scientific Conference 19 April 2024, ISC2024, Singapore

1. The nature of DAO

Sinclair Davidson FBBA, *RMIT University, Australia*
Category: Oral Presentation

Abstract

Just as economics Nobel Laureate Ronald Coase famously asked, 'Why do firms exist?', this project asks, 'Why do DAOs exist?'. Blockchain technology overcomes transactional trust issues through decentralisation and the provision of a tamper-proof and transparent ledger. It does not, however, resolve governance trust issues. 'Who does what, to whose satisfaction?' remain open and important questions in DAOs just as they do in any and every other organisation. This paper forms part of a project that sets out to establish an intellectually coherent, consistent, and academically robust theoretical framework that locates DAOs within a theory of organisation that can then be used by both practitioners and policy makers. The practical outcomes of this research will include a theory of DAOs; a set of testable hypotheses based on those principles; and a set of recommendations to DAO users and policy makers.

Keywords: *Decentralised Autonomous Organisation, Organisation costs, Open Source, Property Rights*

JEL Classification: *D23, D71, D86, L22, L86*

2. Decentralised Finance (DeFi) in 2034: Impact on Financial Services and Needed Competencies for its Professionals

Daniel Liebau, *Erasmus University, The Netherlands*
Category: Oral Presentation

Abstract

The significance of blockchain-based Decentralized Finance, or DeFi, is rising. In late 2021, crypto-native actors pushed total value locked (TVL), a common measure for the size of this market, above USD 150 billion. The ability to swap digital assets against each other and to give borrowers access to capital without intermediaries, only using smart contracts, were decentralized innovations. Then, these unregulated markets collapsed to ca. USD 40 billion in TVL after the bank run on the Terra LUNA network. But regulators worldwide, including MAS in Singapore, started investigating DeFi primitives and how to use them to resolve some of the critical issues in current Finance. Even the Bank of International Settlements (bis) investigated to understand related risks. It is, therefore, timely to ask what capabilities will be needed by finance professionals and their organizations of any size to remain competitive a decade from now – in 2034. I collect unique survey data amongst participants of my executive education course titled "Decentralized Finance (DeFi): A New Financial Ecosystem" to understand required competencies as they are perceived by experienced financial services professionals in (investment) banks, asset managers, insurers, and regulators. Research results are relevant for policymakers and talent development leaders alike.

Keywords: *Blockchain, Decentralized Finance, Innovation, Technology Change, Competencies*

JEL Classification: *G1, J2, O3, L1*

3. Navigating Cryptocurrencies' Next Frontier: The Revolution Towards Decentralizing Physical Infrastructure

Jincheng Zheng, Chongwu Xia, Swee-Won Lo, David Lee Kuo Chuen - *Singapore University of Social Sciences*
Category: Oral Presentation

Abstract

Decentralized Physical Infrastructure Networks (DePIN) integrates blockchain, cryptocurrencies, and the Internet of Things (IoT) to develop traditional industries and the new digital economy. This article outlines DePIN's concept, mechanisms, applications, and future trends, as well as current noteworthy challenges. The LASIC principle is used to measure the feasibility of DePIN, offering valuable insights to investors and practitioners in the assessment of a sustainable business model within the DePIN ecosystem. This article also compares various public blockchains that are used as the DePIN settlement layer and proposes the criterias for cultivating a prosperous DePIN ecosystem.

Keywords: *Decentralised Autonomous Organisation, Organisation costs, Open Source, Property Rights*

JEL Classification: *D23, D71, D86, L22, L86*

4. Token Classification Framework By Consideration Of Origins Of Value And Mechanisms Of Manifestation Thereof

Vasily D Sumanov, Simon Polanski, *PowerPool, Cyprus*
Category: Oral Presentation

Abstract

This paper presents the original Value Capturing Theory (VCT) for digital assets (tokens) study and classification, focusing on the intrinsic value of tokens and acknowledging the significance of demand-side considerations. Traditional classification frameworks overlook these aspects, often assessing tokens based on a wide range of properties without positing a hierarchical structure. In contrast, the VCT introduces a novel framework that classifies tokens based on their value-creating roles in coordinating agent behavior and the primary pathways through which value is realized in the system. In particular, a hierarchical three-level model is developed, wherein a token is attributed several origins of value, and interacting origins of value are grouped by a common pathway they are realized through (termed the Value-Capturing Mechanism). Specific technical implementations of these pathways are recognized. In addition, a method of systematic token design is proposed, and criteria for recognizing novel Value-Capturing Mechanisms are given. Application of the novel framework is demonstrated for both token design for a model system and the decomposition of an extant token according to its origins of value and Value-capturing Mechanisms.

Keywords: *classification framework, token value, value-capturing mechanisms, origins of value, token engineering*

JEL Classification: *D46*

5. Architectural Design of a Blockchain-Powered Carbon Trading System: A Case Study of the South African Carbon Market

Timileyin P Abiodun, *University of Johannesburg, South Africa*
Category: Oral Presentation

Abstract

To achieve carbon neutrality by 2050 and reduce greenhouse gas emissions to a range of 350 to 420 megatons of carbon dioxide equivalent, South Africa introduced a carbon taxation system in June 2019. However, in just three years, it has become evident that the system faces significant challenges, with less than 6% of the estimated tax returns reaching the government. This issue raises concerns about possible corruption and manipulation within the system. To address these challenges, this study presents a comprehensive framework for a carbon trading and taxation system, leveraging blockchain technology. The unique perspective of designing this framework from the government's perspective ensures efficient monitoring and oversight. Notably, the proposed system operates automatically, eliminating the need for third-party intermediaries. This study also identifies a crucial research gap and lays the foundation for future studies. It plans to empirically implement the system as a decentralised application (dApps) using the Ethereum blockchain network, complemented by ReactJs for the user interface, Node-Red to interface with IoT sensors, and Provable to authenticate and validate data that is being injected into the blockchain network. In summary, this research aims to address the shortcomings of the current carbon taxation system in South Africa through a novel, government-centric approach powered by blockchain technology. The proposed system's potential to enhance transparency and efficiency justifies further exploration in future studies.

Keywords: *Blockchain, Blockchain Technology, South Africa, Greenhouse Gas, Carbon Taxation, Carbon Market, Carbon Trading System, Carbon Finance, Carbon Footprint.*

6. Some Simple Institutional Cryptoeconomics of Shared Security

Darcy W.E. Allen, Chris Berg, Sinclair Davidson, *RMIT Blockchain Innovation Hub, RMIT University, Australia*
Category: Oral Presentation

Abstract

Security is an economic good that is costly to produce. Entrepreneurial blockchain communities face a 'make or buy' decision to acquire that security. Many complex factors determine whether a project either (1) makes security (e.g. bearing the setup and maintenance costs of a validator set) or (2) buys security from another blockchain or service provider (e.g. a larger blockchain with more economic weight). In recent years several prominent shared security models have emerged including Interchain Security in Cosmos, Eigenlayer in Ethereum, Babylon for Bitcoin and Parachains in Polkadot. These models involve the purchase of security over a blockchain's organisational boundary, with different contracting structures. In this context, this paper outlines some simple institutional cryptoeconomics of shared security models. We apply institutional economics theory to dissect shared security models, identifying potential contracting hazards that stem from contract incompleteness, asymmetric information and asset specific investments. By applying existing understandings of contract theory to the frontiers of shared security, this paper informs the design of more robust and sustainable shared security models in blockchain ecosystems.

Keywords: *Shared Security, Institutional Economics, Incomplete Contracting, Blockchain Governance*

7. Towards Confidential Chatbots: A Scalable Decentralized Federated Learning Framework

Hongxu Su[1], Cheng Xiang[1] and Bharath Ramesh[2]
[1]*National University of Singapore* - [2]*Western Sydney University*
Category: Oral Presentation

Abstract
The development of cutting-edge large language models like ChatGPT has sparked global interest in the transformative potential of chatbots to automate language tasks. However, alongside the remarkable advancements in natural language processing, concerns about user privacy and data security have become prominent challenges that need immediate attention. In response to these critical concerns, this paper presents a novel approach that addresses the privacy and security issues in chatbot applications. We propose a scalable and privacy-preserving framework for chatbot systems by leveraging the power of decentralized federated learning (DFL) and secure multi-party computation (SMPC). Our DFL framework leverages blockchain smart contracts for participant selection, orchestrating the training process on user data while keeping the data local, and model distribution. After each round of local training by the participants, the blockchain network securely aggregates the model updates using SMPC, ensuring that participants' raw model parameters are not exposed to others. Iterative training rounds are executed through the blockchain network, with participants updating the model collaboratively using SMPC. Experiments show that our approach achieves comparable performance to centralized models while offering significant improvements in privacy and security. This paper presents a novel solution to privacy and security challenges in chatbots and we hope our approach will foster trust and encourage broader adoption of chatbot technology with privacy at the forefront.

Keywords: *Privacy-Preserving Learning, Decentralized Federated Learning, Tiny Language Models (TinyLMs), Secure Multi-party Computation (SMPC), Blockchain Technology*

JEL Classification: C88 - *Other Computer Software - Our paper discusses the development or application of specific software related to chatbots.*

8. Empowering Families in the Genomic Era: A Decentralized Data Trust Approach for Ethical Genomics Management

Daniel Uribe, *GenoBank.io™, USA*
Category: Oral Presentation

Abstract
The field of genomics is at a pivotal juncture, facing challenges in data privacy and the ethical handling of genetic information. Existing genomic data management systems often lack transparency, are inefficient, and do not comply with stringent data protection laws like GDPR or CCPA. Addressing these issues, we propose an innovative AI-governed web3 Genomics Data Family Trust framework, rooted in the principles of DeSci (Decentralized Science). Utilizing the ERC721 standard on EVM-compatible chains, such as the Avalanche C-Chain, our system embeds BioNFTs (Ricardian Contracts) in compliance with local data laws. This approach ensures enhanced transparency and traceability, bolstered by security through client-side encrypted GenoVaults. Additionally, BioWallets enable effective management of genomic assets, with AI oversight ensuring governance standards.

A critical aim of this decentralized trust is to foster integration with AI platforms like BioGPT and other advanced GPT and LLMs. This integration supports the acceleration of genomics and clinical data interpretation, consistent with initiatives like FDA 3060 (a) (Clinical Decision Support Software).By embracing DeSci, the platform not only empowers individuals and families with control and secure sharing of their genomic data but also facilitates their participation in groundbreaking genomic research. The adaptability of the system to various genomic data management scenarios underscores its potential to transform genomic research, aligning with the ethos of Decentralized Science to promote open, transparent, and collaborative scientific inquiry.

Keywords: *DeSci, Genomics, Data Privacy, AI Governance, BioNFTs, Smart Contracts, ERC721, GDPR, CCPA, BioGPT, FDA 3060(a), DeSci, Web3, BioDAO, LabNFT, BioWallet, Biosamples*

JEL Classification: C88 - *K24, O34, I18*

9. Assessing the readiness for blockchain technology in the South African public sector

Beatah Sibanda, *North-West University, South Africa*
Category: Oral Presentation

Abstract

The rise in recent technological developments through the Fourth Industrial Revolution has impacted how businesses and governments globally operate, requiring a shift in strategies and governance systems. These technological advances have altered production, management, and governance systems, allowing businesses and governments to respond with agile and complex approaches. A study into one of these technologies reveals that blockchain could enhance the effectiveness and efficiency of operations in the public sector through its transparency-enhancing measures. While governments globally have adopted or are considering blockchain, South Africa still needs to catch up. This study assessed the readiness of the South African public sector to adopt blockchain technology. The population for the study comprised officials in 15 provincial departments in Gauteng province, South Africa. The study adopted a sequential-exploratory approach using the QUAL-QUANT design. If blockchain has the potential to enhance transparency and accountability in the public sector, it is worth assessing if South Africa is ready to accept this technology by obtaining the perceptions of those charged with governance. Although the study's findings suggest that blockchain could be instrumental in improving public sector governance, South Africa may need more time to accept blockchain technology as several deterrents that could hinder adoption were identified, such as resistance to change, change management, and outdated infrastructure. These could, however, be mitigated by skills development and training and the acquisition of the appropriate infrastructure to support blockchain. The study proposes a framework for adopting blockchain technology in the South African public sector to enhance good governance.

Keywords: *Auditor-General South Africa, Blockchain technology; corporate governance; accountability; transparency; public sector.*

JEL Classification: *H1*

10. Models Of Crypto Projects And Their Properties

Oleksandr Letychevskyi, *Heriot-Watt University Edinburgh, Scotland*
Category: Oral Presentation

Abstract

The research concerns the general abstract model of the crypto project. The algorithmic components of the crypto project, which are defined in the smart contract and their varieties for different services, are highlighted. Typical algorithms for such services as a cryptocurrency exchange, services related to the Internet of Things, education, Internet services and trade are considered. In addition to the algorithmic components, the market component that depends on the external environment, the influence of various external factors, such as the actions of other companies, the statements of celebrities, changes in sales and purchases depending on price changes, is investigated. To predict the scenario of the crypto project, the types of neural networks are considered, which are also included as a component of the crypto project model. Taking into account the algorithmic and market component of the crypto project, the properties of reliability, equilibrium, impossibility of centralization and resistance to malicious actions are investigated. This study is a generalization of the experience of formalization of token economy projects and is an important stage for the creation of a system of analysis and prediction of crypto project scenarios. The presentation will also include demonstrations and comparisons of software systems used in similar analytical studies, including the platform created by the author and his team.

Keywords: *smart contract, algebraic modelling, token economy, economical equilibrium, formal methods, neuron networks*

JEL Classification: C680

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?

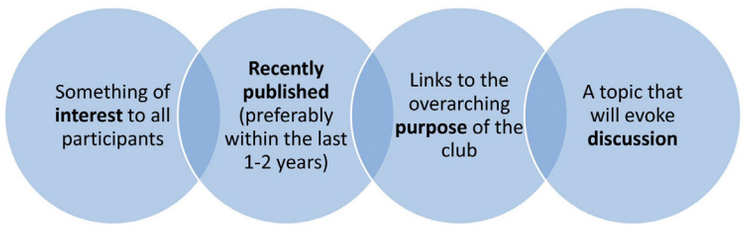
5:35 PM | Crypto Governance and Cryptocurrency Exchanges
Sabino Correa, London Business School, UK
Author of the 2020 JBBA Paper:
Crypto Governance: Analysing Platforms for Crypto Assets Trading

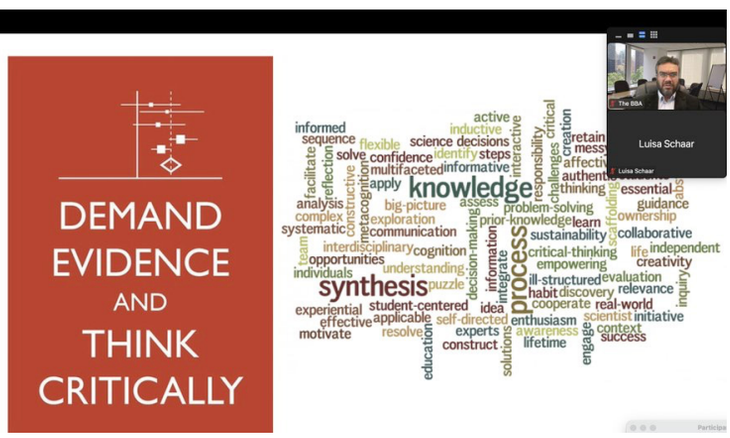
5:50 PM - 6:00 PM: Open Forum AMA & Close

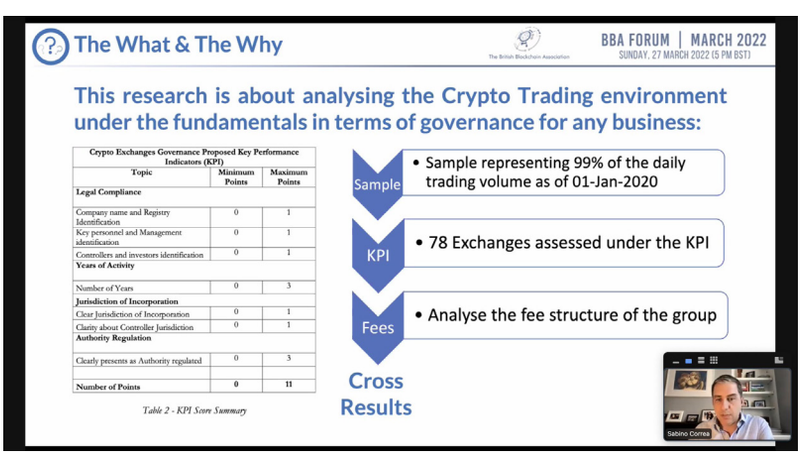
SPEAKERS FROM*

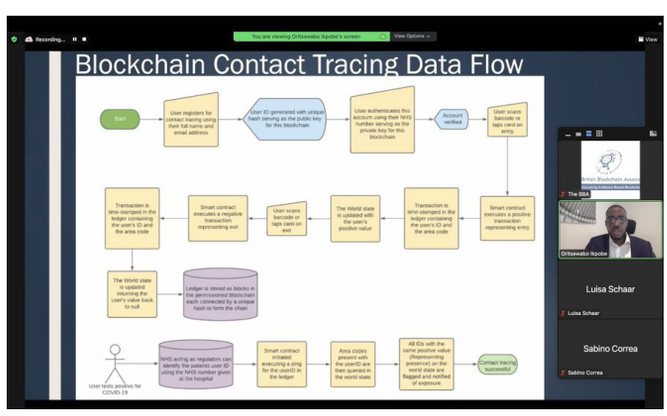
*DISCLAIMER: The views, opinions and factual statements expressed during this webinar are the personal views of the speaker only and do not necessarily represent the official policy, position or views of their organisations.

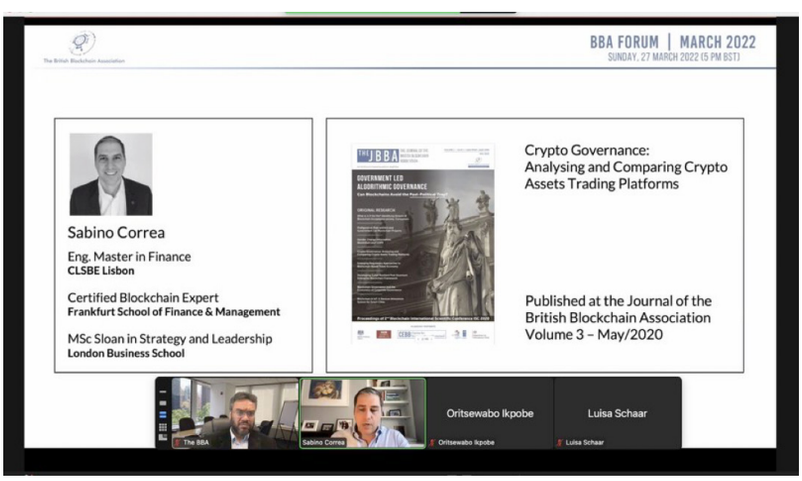
Blockchain and Crypto-assets Journal Club:











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

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

JBBA University Network

(Universities actively involved in blockchain research and/or offers at least one post-graduate teaching module/ Cert/ Diploma/ MSc/ PhD on Blockchain / DLT and/or Cryptocurrencies. The JBBA is indexed at these universities)

Stanford University · University of Birmingham · UCL · Harvard University · University of Pittsburgh · University of Arkansas · Wisconsin · Johns Hopkins University · The Hong Kong Polytechnic University · University of Oxford · Georgetown University · University of Maryland · University of Glasgow · Trinity College Dublin, The University of Dublin · Cardiff Metropolitan University · Edinburgh Napier University · Tel Aviv University · Singapore Management University · University of Zurich · Hochschule Luzern · Carnegie Mellon University · Imperial College London · Oilscoil Teicneolaiochta an Atlantaigh, Atlantic Technological University · Illinois · Massachusetts Institute of Technology · UCLA · Texas, The University of Texas at Austin · NUS National University of Singapore · University of Cumbria · University of Cambridge · Haute École de Gestion Hochschule für Wirtschaft School of Management Fribourg Freiburg · Maastricht University · Trinity Western University · St. Mary's University School of Law · Penn · LSE The London School of Economics and Political Science · 東京工業大学 Tokyo Institute of Technology · 서울대학교 Seoul National University · University of Nicosia · The Open University · Capitol Technology University · UNSW · New York University · Bowie State University · Princeton University · Universidad del Rosario · IT University of Copenhagen · King's College London · Columbia University · King Abdulaziz University · University of Sydney · University of Portsmouth · RMIT University · City University of London · L-Università ta' Malta · Monash University · The University of Chicago · University of Copenhagen · NTNU Norwegian University of Science and Technology · UBC The University of British Columbia · University of Surrey · George Mason University · UCSB · University of Reading · Alma Mater Studiorum Università di Bologna · Epoka University · The University of Hong Kong · Universidad Europea Madrid · Varna University of Management · ASU Arizona State University · Warwick · Université Laval · Tsinghua University · ITBA · Duke University · University of Southampton · Frankfurt School of Finance & Management Bankakademie | HfB · The Chinese University of Hong Kong · Portland State University · SUSS Singapore University of Social Sciences · Ben-Gurion University of the Negev

List curated by
The British Blockchain Association
(Correct as of March 2024)

The British Blockchain Association
Advocating Evidence Based Blockchain

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

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 2024)

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

ENGAGE WITH
THE BRITISH BLOCKCHAIN ASSOCIATION
AND THE JBBA

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

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

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

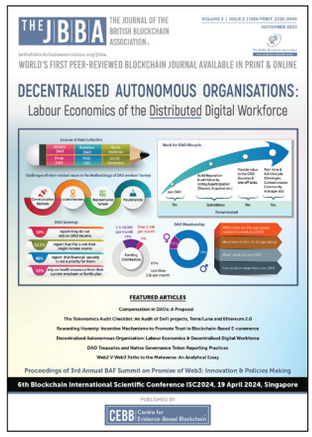
Subscribe to JBBA RSS feed to keep track of new content and receive Alert notifications each time something new is published in the JBBA.

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

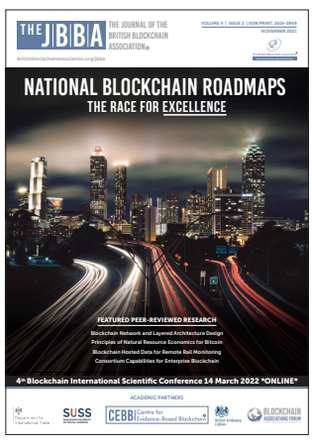
Volume 5 - Issue 2
November 2022

Volume 6 - Issue 1
May 2023

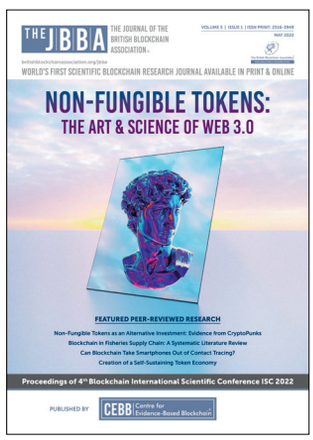


Volume 6 - Issue 2
November 2023

Volume 4 - Issue 1
May 2021



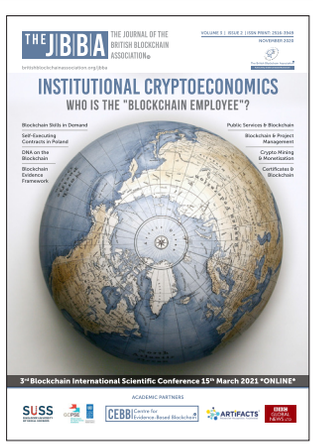
Volume 4 - Issue 2
November 2021



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®