



ENTERPRISE BLOCKCHAIN IS STRATEGIC VALUE CREATION POSSIBLE?

PEER-REVIEWED RESEARCH

Strategic Value Creation
through Enterprise Blockchain

Medical Tourism, Tokens
& Blockchain Networks

Blockchain, Hedge Funds and
Zero Knowledge Proofs

Identity of Things: SSI of IoT devices

Evidenced Based Blockchain
for Agri-Farming

ITO: The Sponsored
Token Technology

Blockchain is dead!
Long live Blockchain!

Industrial Symbiosis Networks &
Blockchain-based B2B Marketplaces

Proceedings of 3rd Blockchain International Scientific Conference ISC 2021

ACADEMIC PARTNERS





The British Blockchain Association[®]

Advocating Evidence Based Blockchain

JOIN NOW

MEMBERSHIP BENEFITS

Find Solutions



Get access to all the resources you need to succeed in your next venture

Get Educated



Stay informed with the latest news, education and cutting edge research

Network



Become a part of a global network of Centre for Evidence Based Blockchain (CEBB)

Influence



Be a part of an association that champions the future landscape for blockchain

Promote



Gain awareness for your blockchain based venture and help elevate your own profile

Reduce Costs



Get member only discounts and perks on valuable products and services

WORKING IN COLLABORATION WITH:



FEATURED MEMBERS



Join Now at britishblockchainassociation.org/membership

britishblockchainassociation.org



TABLE OF CONTENTS

Editorial Board	12
Editorial	15
Testimonials from Authors & Readers	16

PEER-REVIEWED RESEARCH

Strategic Value Creation through Enterprise Blockchain <i>Kristi Yuthas, Yolanda Sarason, Asad Aziz</i>	18
Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices <i>Tim Weingärtner, Oskar Camenzind</i>	26
Piece of Cake: Assuring Specific Qualities of Product in Farm Lifecycles with DLT – Can Evidenced-Based Practice be supported by Participatory Action Research Methods? <i>Hannah Rudman</i>	32
ITO: The Sponsored Token Technology <i>Tianqi Cai, H. J. Cai, David Kuo Chuen Lee, Dong Yang, Kai Wang</i>	38
Industrial Symbiosis Networks in Greece: Utilising the Power of Blockchain-based B2B Marketplaces <i>Stavros T. Ponis</i>	47
The Relation between Tokens and Blockchain Networks: The Case of Medical Tourism in the Republic of Moldova <i>Marc Pilkington</i>	53
Blockchain is dead! Long live Blockchain! <i>Joshua Ellul</i>	62
Investment Compliance in Hedge Funds using Zero Knowledge Proofs <i>Komal Kalra, Shubham Sabai, Sandeep Kumar Shukla</i>	71
CONFERENCE PROCEEDINGS ISC2021	78

3RD BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE

15 MARCH 2021, #ISC2021, UK

OPENING KEYNOTE

CEBB | Centre for Evidence-Based Blockchain

The British Blockchain Association



Dr Naseem Naqvi FBBA
Host, The British Blockchain Association
London, UK



Blockchain Association
Evidence Based Blockchain

ISC2021



Hester Peirce SEC
Commissioner, SEC, SEC
USA, USA



U.S. SECURITIES AND EXCHANGE COMMISSION

Speech

Paper, Plastic, Peer-to-Peer



Commissioner Hester M. Peirce

March 15, 2021

Remarks at the British Blockchain Association's Conference

"Success Through Synergy: Next generation Leadership for Extraordinary Times"

Thank you to the British Blockchain Association for including me in today's conference. I will begin with my standard disclaimer that the views that I represent are my own and not necessarily those of the Securities and Exchange Commission or my

THE JBBA | THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

The British Blockchain Association
Advocating Evidence Based Blockchain

CEBB | Centre for Evidence-Based Blockchain

3rd Blockchain International Scientific Conference #ISC2021

OPENING KEYNOTE: Dr Naseem Naqvi, President, The BBA

- Blockchain sits at the junction of technical, social, legal and political paradigms – There is a need for interdisciplinary harmonisation, both within the bounds of the individual branches of DLT and the stakeholders.

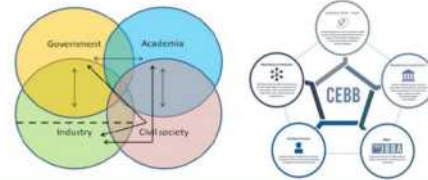
THE JBBA | THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

The British Blockchain Association
Advocating Evidence Based Blockchain

CEBB | Centre for Evidence-Based Blockchain

3rd Blockchain International Scientific Conference #ISC2021

OPENING KEYNOTE: Dr Naseem Naqvi, President, The BBA



BBA's 3rd Blockchain International Scientific Conference #ISC2021 (Online) March 15, 2021 (Countries and Institutions)



CEBB | Centre for Evidence-Based Blockchain

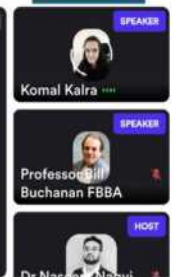
The British Blockchain Association
Advocating Evidence Based Blockchain

ISC2021



Komal Kalra is Presenting

- Hedge Funds
- Zokrates Architecture
- Design Overview
- Protocol Workflow
- Results



Blockchain Research Abstracts Presentation 2

CEBB | Centre for Evidence-Based Blockchain

The British Blockchain Association
Advocating Evidence Based Blockchain

Yuvraj Rajendra is Presenting

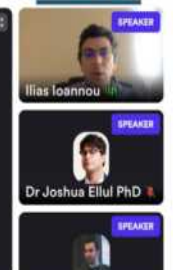


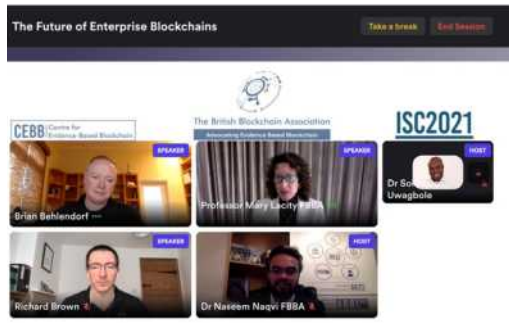
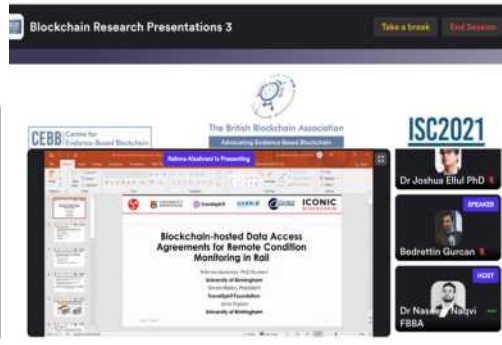
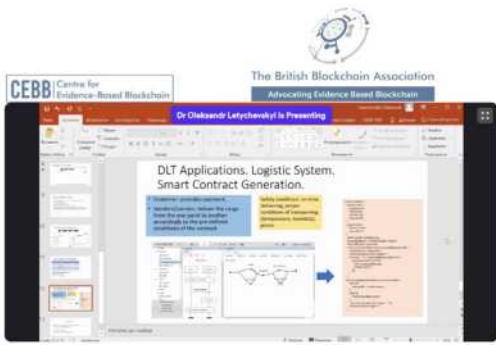
Blockchain Research Presentations 3

CEBB | Centre for Evidence-Based Blockchain

The British Blockchain Association
Advocating Evidence Based Blockchain

ISC2021

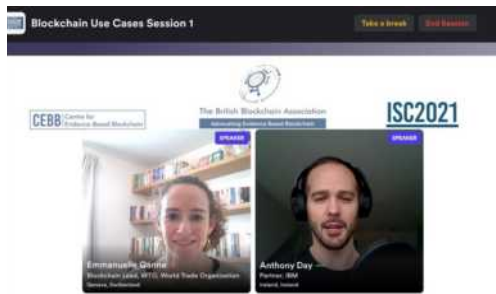




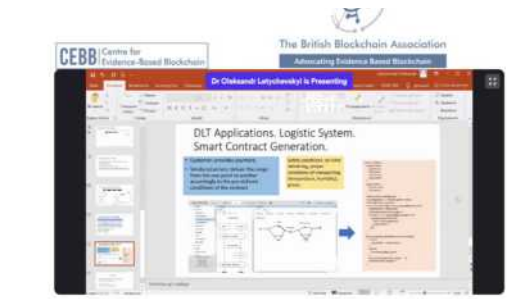
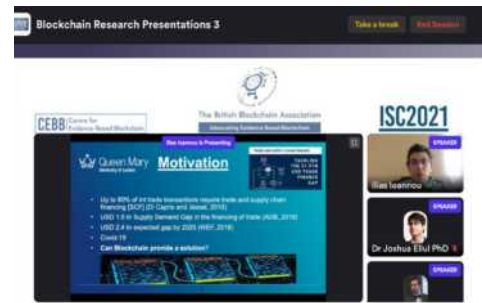
2nd Prize:
Dr Oleksandr Letychveskyi, Ukraine (19)
Professor Dr Tim Weingartner, Switzerland (19)



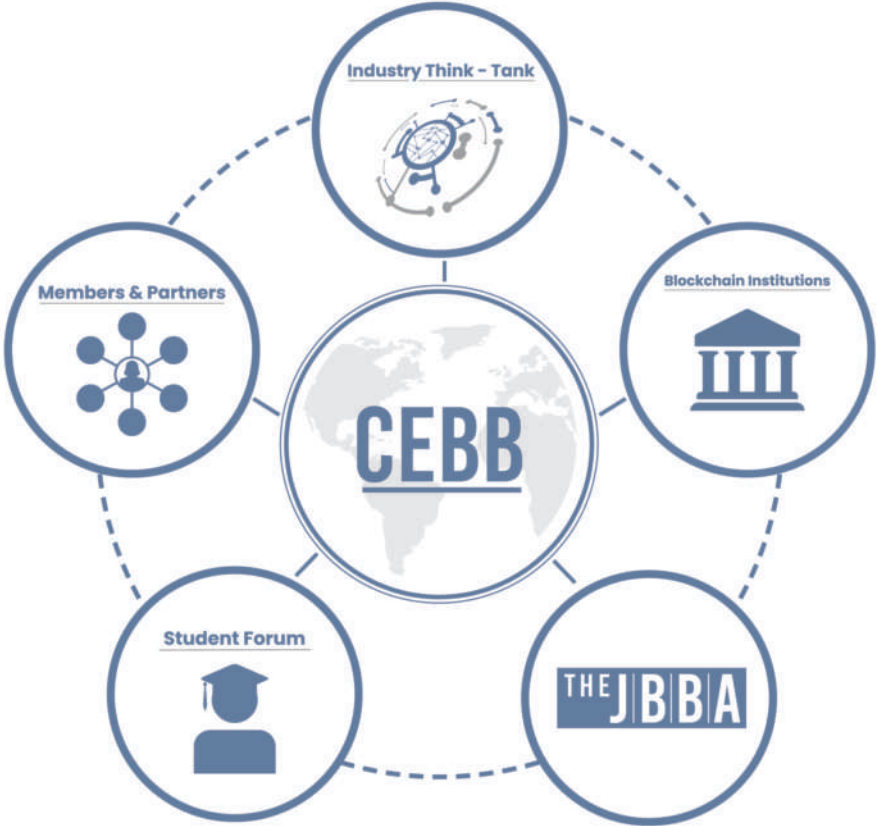
3rd Prize:
Yuvraj Rajendra of IIT Allahabad, India (14)
Dr Joshua Ellul of University of Malta, Malta (14)



1st Prize:
Dr Stanton Heister and Professor Dr Kristi Yuthas (21)
Portland State University, USA



Bridging the Blockchain Research and Practice Gap



MEMBERS



JOIN CEBB

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

WHAT IS CENTRE FOR EVIDENCE BASED BLOCKCHAIN?

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

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



Follow us on:



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

INTRODUCING JBBA VIDEO ABSTRACTS!



JBBA has become the World's First Blockchain Research Journal to create Video Abstracts for its Authors!

- By featuring the people behind the science, video abstracts will add value and visibility to the work of our authors
- They help convey the significance of scientific results in a personalised way, beyond the concise text of articles
- Video abstracts make the paper more accessible and discoverable, and enhances its reach and global impact

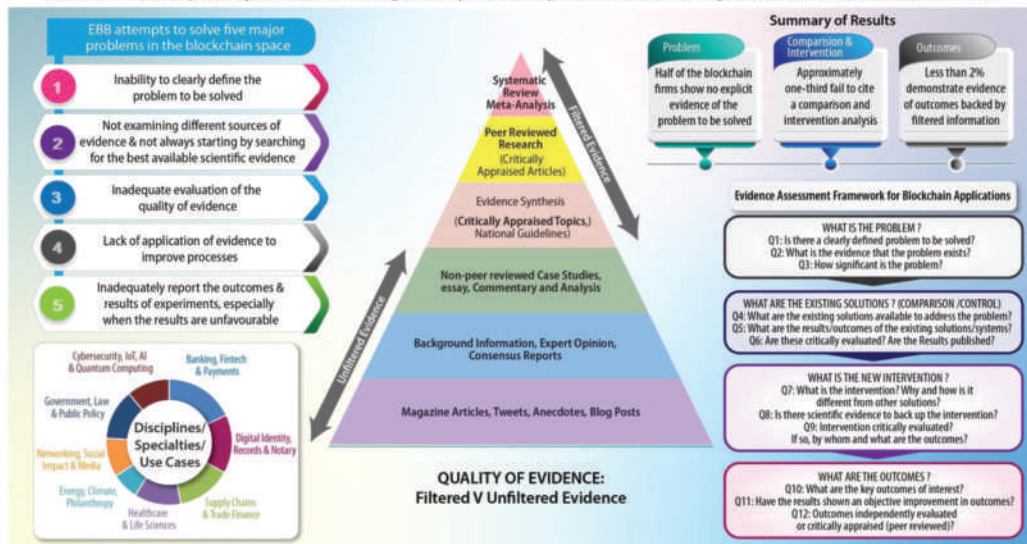
For more info, visit <https://www.youtube.com/c/TheJBBA>

JBBA INFOGRAPHICS

PRODUCED BY CENTRE FOR EVIDENCE BASED BLOCKCHAIN (CEBB)

Evidence-Based Blockchain (EBB): Findings from a Global Study of Blockchain Projects and Start-up Companies

EBB is conscientious, explicit and judicious decision making based on professional expertise and evidence from organisations, stakeholders and scientific research



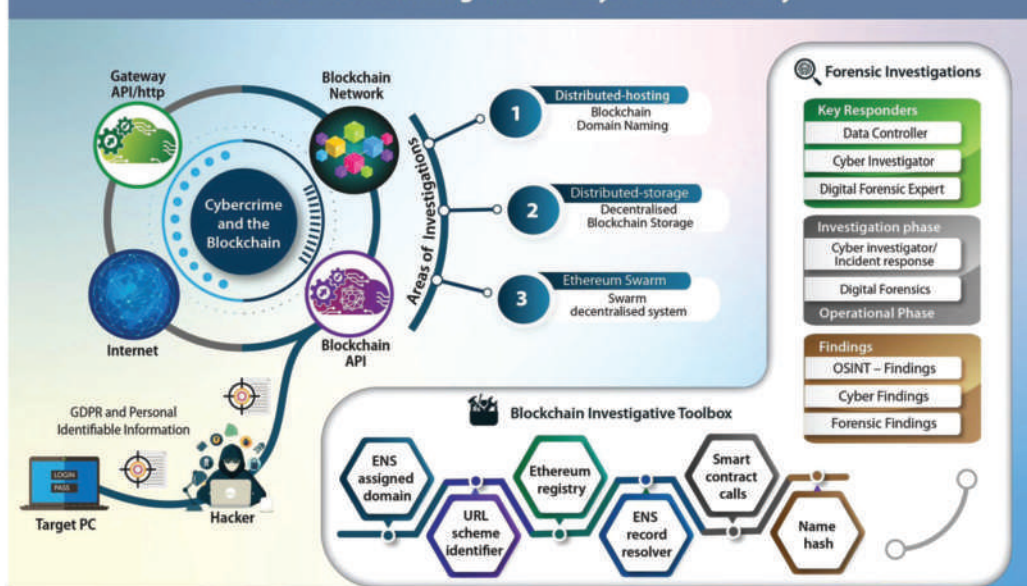
Naseem Naqvi, Mureed Hussain
DOI: 10.31585/jbba-3-2-(8)2020



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

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

Blockchain Investigations - Beyond the 'Money'

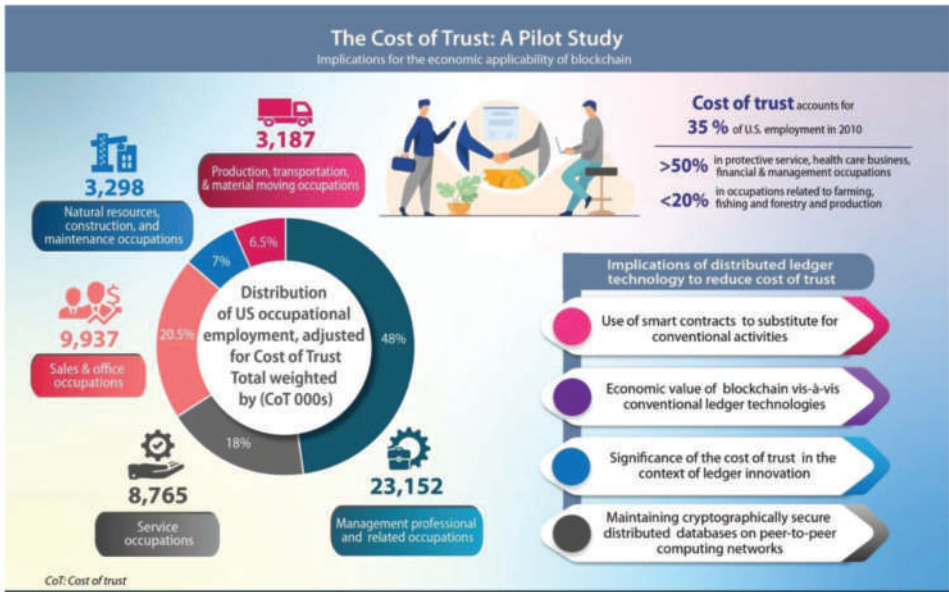


Simon F. Dyson (2019)
DOI: 10.31585/jbba-2-2-(6)2019



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

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

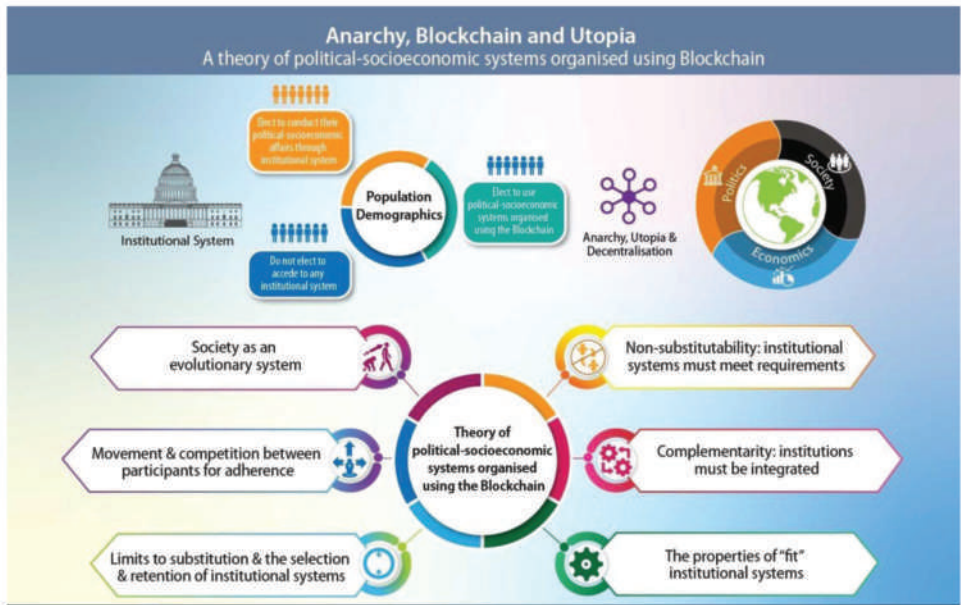


Mikayla Novak et al (2018)
DOI: 10.31585/jbba-1-2-(5)2018

THE JBBA
THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

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

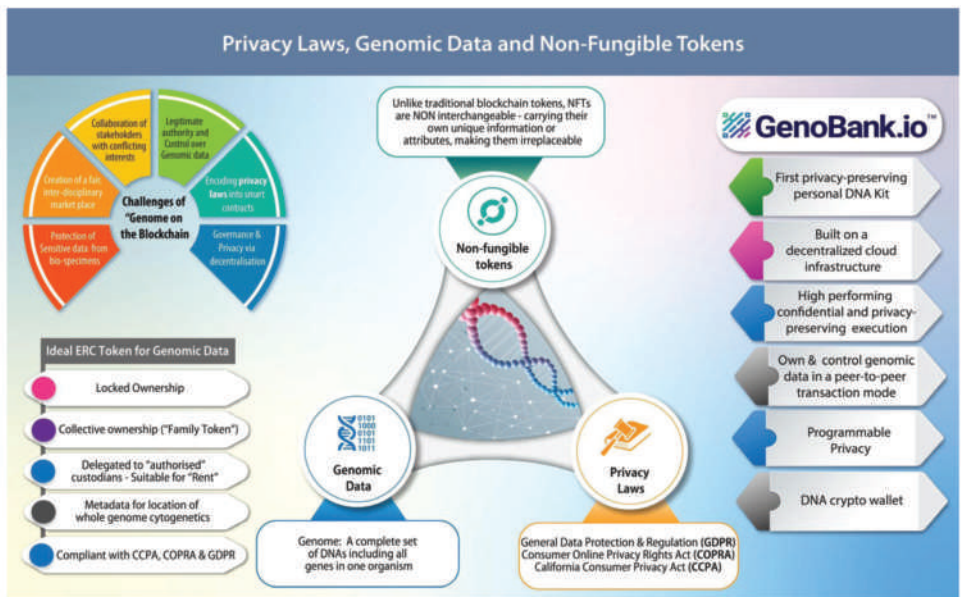


Brendan Markey-Towler (2018)
DOI: 10.31585/jbba-1-1-(1)2018

THE JBBA
THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

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



Daniel Uribe and Gisele Waters (2020)
DOI: 10.31585/jbba-3-2-(5)2020

THE JBBA
THE JOURNAL OF THE
BRITISH BLOCKCHAIN
ASSOCIATION

Centre for Evidence Based Blockchain
britishblockchainassociation.org
@Brit_blockchain

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

For more info, visit <https://jbba.scholasticahq.com/for-authors>

EDITORIAL BOARD

Editor-In-Chief:

Dr. Naseem Naqvi
 FBBA FRCP M Acad Med MSc (Blockchain)
 Centre for Evidence Based Blockchain, UK

Associate Editor-In-Chief:

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

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

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

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

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

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

Contributing Editors:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

External Reviewers:

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

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

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

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

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

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

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

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

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

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

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

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

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

Dr Hossein Sharif PhD
(Blockchain, AI, Cryptocurrencies)
University of Newcastle, UK

Dr Wajid Khan PhD
(Big Data, E-Commerce)
University of Hertfordshire, UK

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

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

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

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

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

Demelza Hays MSc
(Cryptocurrencies)
University of Liechtenstein, Liechtenstein

Alastair Marke FRSA MSc
(Blockchain and Climate Finance)
Blockchain Climate Institute, UK

Jared Franka BSc
(Cryptocurrency/ Network Security)
Dakota State University, USA

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

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

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

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

Simon Dyson MSc
(Healthcare, IT, Security)
NHS Digital, UK

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

Professor Dr David Galindo PhD
(Applied Cryptography & Blockchain)
University of Birmingham, UK

Managing Editor:

Mr. Joseph Gautham
(Academic publishing)
Deanta Global, Dublin, Ireland
[Editorial@thejbba.com]

Publishing Consultant:

Mr. John Bond
Riverwinds Consulting, USA

Sponsorships and Academic Partnerships:

Ms Tracy Smith
Editorial@thejbba.com

Type-setting, Design & Publishing

Mr. Zeshan Mahmood
admin@britishblockchainassociation.org

WHY JBBA?

- » We publish in real-time, online, as well as in **PRINT - THE HARD COPIES ARE DISTRIBUTED WORLDWIDE**
- » Print copies are available at some of the largest libraries in the world including **BRITISH LIBRARY** and over 100+ more **AROUND THE GLOBE**
- » Our authors and readers rate the JBBA as **OUTSTANDING**
- » We create **INFOGRAPHICS** of published research papers
- » 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** (Directory of Open Access Journals)
- » We have a **JBBA YOUTUBE CHANNEL**
- » JBBA papers are quoted by Government Officials, Policymakers, Regulators and High Profile Organisations - **CREATING A GLOBAL IMPACT**

EDITORIAL

I am delighted to present to you the **seventh** issue of the Journal of the British Blockchain Association – The JBBA. This is now the journal's third full issue and the second special conference edition that has been published during a global pandemic. Now in its fourth year, I am pleased to see that the journal continues to accomplish its mission of serving the blockchain community with robust, peer-reviewed research on distributed ledger technologies.

It would be an understatement to say that the Blockchain is transforming the societal fabric of our lives. At the same time, policymakers and regulators are under increasing pressure to support innovation, while ensuring that the policies are safe, cost-effective, consumer-centred, business-friendly and based on best available evidence. Perhaps it was not surprising to hear this comment from SEC Commissioner, Hester Peirce, at our Blockchain International Scientific Conference ISC2021: *“Evidence-based rule making is not yet the norm in Crypto regulation space”*.

UK Research and innovation (UKRI) defines academic impact as *“demonstrable contribution that excellent social and economic research makes in shifting understanding and advancing scientific method, theory and application across and within disciplines.”* The readers will find such high-impact research papers in this issue, many of them were presented at the ISC2021, namely:

1. Strategic Value Creation through Enterprise Blockchain
2. Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices
3. Piece of Cake: Assuring Specific Qualities of Product in Farm Lifecycles with DLT - Can Evidenced Based Practice be supported by Participatory Action Research Methods?
4. ITO: The Sponsored Token Technology
5. Industrial Symbiosis Networks in Greece: Utilising the Power of Blockchain-based B2B Marketplaces
6. The Relation between Tokens and Blockchain Networks: The Case of Medical Tourism in the Republic of Moldova
7. Blockchain is dead! Long live Blockchain!
8. Investment compliance in Hedge Funds using Zero Knowledge Proofs

There is a global crisis of trust, one which has reached epidemic proportions. Societal trust, the currency on which we construct the fabric of our lives – has eroded. It is now prudent that the policies, benchmarks and frameworks in blockchain must be based on trustworthy, reliable and reproducible information. We must implement evidence-based information that comes from robust peer-reviewed research. There must be a strategic intent and senior level buy-in to identify sources of evidence, develop and test blockchain pilots and deploy interventions based on high-quality evidence. The use of resources must be constantly and dynamically optimised in line with emerging data. This should apply to all stages of quality management of blockchain interventions: quality assurance, quality control and quality management.

UK's Walport Report recommended that distributed ledger technology pilots *“should be co-ordinated in a similar fashion to the way that clinical trials are implemented, reported and assessed, in order to ensure uniformity and maximize the rigour of the process.”* I am glad the JBBA has been providing a platform to global blockchain research community to fulfil these objectives of advancing better science.

The theme of this issue is Enterprise Blockchains – blockchains that have provided us with a hope to build a trusted decentralised economy, however technology cannot accomplish this on its own. To restore lost trust, we must also educate and reform the human components of the enterprise

DLT ecosystems. Blockchain sits at the junction of technical, social, legal and political paradigms – hence there is a strong need for interdisciplinary harmonisation, both within the bounds of the individual branches of DLT and the stakeholders. We must foster blockchain ecosystems where there is freedom for innovation and a sense of accountability. Building decentralised ecosystems is easy; building decentralised accountability is hard. Accountability is the price we pay for self-sovereignty.

The trustable sources of information are more important now than ever before. We are overwhelmed with accessible information, but, unfortunately, not always of examined and scrutinized quality. Scientific consensus and peer-reviewed data is the cornerstone for disseminating trustworthy and reliable knowledge; for which I believe our editors and reviewers carry a tremendous responsibility.

To conclude this editorial, I would like to thank all the authors for submitting their research to the JBBA, the reviewers and the editors for their tireless volunteer service and our readers and well-wishers around the globe for the continuous support of the journal.

With best wishes

Dr Naseem Naqvi FRCP FBBA

Editor in Chief

President, The British Blockchain Association

Chair, Centre for Evidence Based Blockchain (CEBB)

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

“ Within an impressively short time since its launch, the JBBA has developed a strong reputation for publishing interesting research and commentary on blockchain technology. As a reader, I find the articles uniformly engaging and the presentation of the journal impeccable. As an author, I have found the review process to be consistently constructive.

Dr. Prateek Goorba PhD, Blockchain Researcher and Economist

“ We live in times where the pace of change is accelerating. Blockchain is an emerging technology. The JBBA's swift review process is key for publishing peer-reviewed academic papers, that are relevant at the point they appear in the journal and beyond.

Professor Daniel Liebau, Visiting Professor, IE Business School, Spain

“ The JBBA submission process was efficient and trouble free. It was a pleasure to participate in the first edition of the journal.

Dr. Delton B. Chen PhD, Global4C, 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

“ Very professional and efficient handling of the process, including a well-designed hard copy of the journal. Highly recommend its content to the new scientific field blockchain is creating as a combination of CS, Math and Law. Great work!

Simon Schwerin MSc, BigChain DB and Xain Foundation, Germany

”

“ JBBA has quickly become the leading peer-reviewed journal about the fastest growing area of research today. The journal will continue to play a central role in advancing blockchain and distributed ledger technologies.

John Bond, Senior Publishing Consultant, Riverwinds Consulting, USA

”

“ 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

”

“ The overarching mission of the JBBA is to advance the common monologue within the Blockchain technology community. JBBA is a leading practitioners journal for blockchain technology experts.

Professor Dr. Kevin Curran PhD, Ulster University, Northern Ireland

”

“ 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 Rennick 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 the future

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

”

Strategic Value Creation through Enterprise Blockchain

¹Kristi Yuthas, ²Yolanda Sarason, ²Asad Aziz

¹School of Business, Portland State University, USA

²College of Business, Colorado State University, USA

Correspondence: yuthask@pdx.edu

Received: 29 December 2020 **Accepted:** 06 March 2021 **Published:** 20 March 2021

Abstract

Blockchain and other distributed ledger technologies have enormous potential for creating business value but have not yet been widely adopted. Enterprise blockchain systems are recognised as solutions to existing operational problems or ‘pain points’ but their potential for delivering value through strategic opportunities is not well understood. Drawing from literature on strategic alliances and the resource-based view of the firm, we identify avenues through which blockchain systems can contribute to a firm’s strategic capabilities and, as a result, to its sustained competitive advantage. We provide a framework for understanding how participation in blockchain solutions can enable companies to build upon existing strategic capabilities, strengthen collaborative capabilities and develop blockchain-specific capabilities. The framework can be useful to firms and service providers for incorporating strategic outcomes into the evaluation of blockchain investment opportunities.

Keywords: *enterprise blockchain, consortium, ecosystem, strategic alliances, resource-based view, competitive advantage, strategic capabilities*

JEL Classifications: *0020M15 IT Management*

1. Introduction

Blockchain and other distributed ledger technologies provide databases or ledgers that are shared among multiple parties. Transactions stored in these ledgers are validated, timestamped and secured. Once recorded, they cannot be changed or deleted. Shared ledgers can improve data transparency, efficiency and collaboration among participants. While initially created for the transfer of cryptocurrency, blockchain use has increased exponentially since its introduction [1]. Enterprise blockchains have emerged as the means through which multiple partners that are known to each other collaborate in storing records and conducting transactions using a shared ledger. These partners agree to certain rules, such as who has visibility into each record. These shared rules provide benefits such as helping facilitate the management and sharing of sensitive information such as customer and financial data, without breaching privacy laws [2].

Despite blockchain’s potential for strategic impact, its adoption has not lived up to what some refer to as its hype [3]. Research on 517 blockchain projects finds that many projects fail to address clearly defined and significant problems and lack evidence to support the use of blockchain solutions [4]. In this article, we examine an important factor that may contribute to the incomplete evidence supporting blockchain use. In general, blockchain has been viewed as a solution for improved operational outcomes [5] rather than a potential source of strategic value. While the operational benefits of blockchain are becoming more widely recognised, blockchain’s potential to support strategic capabilities and competitive plans is not well understood. We address this gap by providing a framework that can be used to systematically evaluate strategic outcomes of blockchain projects.

We begin by describing foundational elements of enterprise blockchains. We discuss the processes currently used to assess blockchain, processes

which focus on operational improvements and overlook strategic benefits. We then introduce constructs from the academic literature on strategic alliances and the resource-based view (RBV) of the firm that are relevant for the enterprise blockchain context and provide the basis for understanding the strategic opportunities presented by these systems. Finally, we present a framework and examples that identify and categorise ways companies can build strategic capabilities through participation in blockchain consortia.

2. Key Elements of Enterprise Blockchains

The term blockchain refers to a specific type of distributed ledger system in which transactions are stored in blocks analogous to tabs in a spreadsheet arranged in a temporal sequence [6]. Although many no longer use blocks to store data, distributed ledger systems are commonly referred to as blockchains, a term that will be used throughout this paper. Blockchains can be “permissioned” or “permissionless”. Permissionless blockchain systems such as the Bitcoin blockchain are open to all users. Without obtaining permission, anyone can establish an identity and execute transactions over the platform, and anyone can participate in maintaining the network by downloading the software used to validate and store transactions. Bitcoin and Ethereum are the most well-known examples of permissionless blockchains.

Blockchains used by enterprises are typically permissioned. These blockchains are developed and maintained by a known group of participants who have established their identities and have agreed to abide by the rules that govern the blockchain. Governance agreements determine the rights and responsibilities of each blockchain participant. Data stored on the chain are associated with the identities of the participants who attested to its validity. Data are typically encrypted and visible only to those participants or parties to which access has been granted, such as supply chain partners, auditors, or regulators.

Core elements of interest in an enterprise blockchain are distributed ledgers, digital assets, and smart contracts. Distributed ledgers are used to store transactions that are executed by blockchain participants, such as information about the transfer of goods from one party to another. These transactions can be written to the blockchain by transacting parties or by Internet of Things (IoT) devices such as Radio-Frequency Identification (RFID) chips. Ledgers can be used to store basic transactions, as in a traditional database, and they can also store digital assets and smart contracts.

Digital assets such as cryptocurrency, software or music, can be secured and ownership can be validated on a blockchain. “Digital twins” that provide digital representations of physical assets, such as deeds, titles, patents or ownership shares can also be stored and transferred using a blockchain system. Blockchains provide the ability to ensure that only one copy of a digital asset, such as a bitcoin or car title, is valid, so that if it is sent to another party, the sender’s copy is no longer valid. This enables assets of value to be securely transferred between blockchain participants without the need for banks or other trusted brokers.

Smart contracts, which are programs containing if-then logic, can be stored on the blockchain and executed automatically as predefined conditions are met. For example, a shipping contract can be programmed so that when a set of RFID chips cross to a loading dock, a receiving report is generated and digitally signed, authorising a digital payment.

Blockchain’s unique features provide several benefits in an enterprise context. Every piece of information stored in a blockchain is linked to the identities of the parties that initiated and validated the data, which establishes legitimacy and origin. This provides accountability and ensures that information can be traced to a validated source. Entries in a ledger are timestamped and immutable, which establishes an audit trail and provides transparency into the provenance of assets.

3. Identification and Evaluation of Blockchain Solutions

When an enterprise explores potential benefits of blockchain solutions, the objective is typically to achieve operational improvements such as cost avoidance, risk reduction, and improved customer experience. The exploration process involves identification of potential use cases—specific uses for blockchain systems that can produce these operational benefits. This is a technology-driven process in which corporate use cases are matched with technological capabilities to determine whether blockchain is a fit.

Like information technology (IT) projects that follow an analysis-design-implementation approach, analysis of potential blockchain use cases generally begins with problem identification. Guidance provided to companies usually centres around solving current and known problems, often referred to as pain points or frictions. McKinsey [7], for example, asserts that “Organizations must start with a problem. Unless there is a valid problem or pain point, blockchain likely won’t be a practical solution.” The World Economic Forum [8] states, “Good use cases must solve real problems for organizations. Great use cases solve real problems at a cost that is significantly lower than the benefits the adoption brings.” PwC advises firms considering embarking on a blockchain to begin by assessing what the firm is trying to accomplish, which “starts with pain points that are tested against key criteria, to determine if blockchain is a good fit or if other technologies are better placed.” [9] IBM, which has been ranked as the leading service provider in the blockchain space [10], guides companies considering blockchain solutions to focus on current problems and why and for whom they are problems. At the ecosystem level IBM suggests focusing on friction, which “at the industry level, provides a Founders Handbook for evaluating enterprise blockchain solutions. The Handbook begins by focusing on problems with three essential questions for identifying potential use cases: “1. What’s the problem with the way we

do things today? 2. Who is this a problem for? 3. Why is this a problem?” [11].

IBM’s approach extends the analysis to examine problems in the interactions between companies. In a white paper [12], IBM states “Blockchain technology...has the potential to obviate intractable inhibitors across industries.” The paper further argues that as frictions are reduced, enterprises and entire industries will be restructured. While these goals are expansive, IBM focuses on known operational problems. IBM’s Founders Handbook [11] also suggests focusing on friction, “Based on your professional experience within your industry, identify a specific process currently creating friction among multiple parties in the same ecosystem. We recommend focusing on a use case with the greatest amount of friction.” Klein et al. [13], who provide a use-case identification framework based on extensive research, also base their recommendations on the current state of the ecosystem. They argue that “Blockchain technology offers great potential for cost, time and efficiency improvements of existing business models.”

Traditional use-case analyses prioritise blockchain solutions to operational problems and emphasise well-understood benefits associated with these solutions. Blockchains are effective in addressing the lack of trust between trading partners by providing the ability to track the provenance of transactions and digital assets and ensuring the immutability of records. They can also reduce friction in inter-company workflows through the use of smart contracts and automated value-transfer mechanisms which can reduce costs directly or through disintermediation.

Current approaches have made strides in exploring and addressing existing operational problems, The Centre for Evidence-Based Blockchain advances this project by providing a comprehensive framework for evaluating whether the outcomes of a blockchain intervention are superior to existing solutions for solving important problems [4]. Despite the increasing sophistication in identifying beneficial use cases, there are currently no frameworks that provide guidance for envisioning or evaluating the strategic opportunities and innovations that blockchains could enable. As a result, the cost of implementing a new and unfamiliar blockchain solution is weighed against operational returns such as reduced costs and operational efficiencies but not against strategic benefits.

Some blockchain proponents have begun to recognise that blockchain can support certain strategic goals. McKinsey [7], for example, notes that “Blockchain appeals to industries that are strategically oriented toward modernization. These see blockchain as a tool to support their ambitions to pursue digitization, process simplification, and collaboration”, and points to the reputational value of being an innovator. Others have pointed to the role of blockchain in reinventing processes and products [14].

In the right circumstances, the capabilities addressed by McKinsey and Accenture could contribute to an enterprise’s competitive advantage. The strategic potential of blockchain solutions extends far beyond these examples, however, and a more complete analysis could uncover new possibilities.

4. Strategic Alliances and Competitive Advantage

To unpack how participation in an enterprise blockchain can create strategic value for a firm, we draw upon the academic literature on strategic alliances through the lens of RBV. RBV [15] presents a view of firms as collections of resources. According to RBV, to the extent that the resource endowments of a firm are Valuable, Rare, Inimitable, and Organisational to be accessible – these resources form the basis of the firm’s sustainable competitive advantage. For this paper, it is sufficient to identify RBV as a perspective that can help firms identify what resources they have, or need to access, to be successful. RBV, however, does not provide guidance on how a firm is to go about accessing those resources. Looking at strategic

alliances as a means to access resources provides the linkage to blockchain consortia – blockchain consortia are a type of strategic alliance. A strategic alliance is a voluntary arrangement among firms that exchange or share resources, or collaborate in the development of products, services or technologies [16]. Alliances can also be cooperative arrangements between two or more firms to improve their competitive position and performance by sharing resources [17], [18], [19]. The RBV perspective portrays firms as collections of heterogeneous resources [20], [21], [22]. Resources that can be sources of competitive advantage are rare, valuable and are difficult to imitate or substitute [21]. Within this perspective, there has been an increasing focus on dynamic capabilities, as bundles of resources that over time can lead to competitive advantage [23], [24]. Capabilities are a special type of intangible resources, they are organizationally embedded, non-transferable, and firm-specific resources whose purpose is to improve the productivity of the other resources possessed by the firm [25]. They may include company expertise in quality, product or service, innovation, customer service or price leadership [26]. For example, Apple Inc. is seen as having strategic capabilities in their design methodology, systems integration and their understanding of consumer behaviour; Tesla is seen as having superior engineering expertise in battery-powered motors and power trains [27].

The research on strategic alliances using an RBV lens has focused on how alliances reinforce and build capabilities that can uncover sources of competitive advantage [28]. There are different avenues through which alliances can create competitive advantage [29]. One avenue is when the alliance builds on an existing capability. For example, if a firm's competitive advantage centres on customer service, an alliance that builds on this capability can facilitate the firm's competitive advantage. Another avenue is when there are complementary capabilities among the partners. If one firm has expertise in R&D and another firm in marketing and distribution, for example, a strategic alliance can build on each firm's capabilities and give either, or both, an advantage in their respective marketplaces. A third avenue is when new capabilities are created because of the alliance. For example, when partners can enter a new market, each has the potential to build capabilities in new markets. This was common when traditional brick and mortar businesses entered online sales through alliances. Once the alliance was established, the brick and mortar businesses were able to develop their own capabilities around online selling.

Blockchain consortia can be understood as forms of strategic alliances, with the same potential for improving competitive advantage for alliance partners. Our framework illustrates how participation in blockchain consortia can lead to competitive advantage through these three avenues.

5. Blockchain-Based Strategic Capabilities Framework

Enterprise blockchain solutions can provide the basis for strengthening and building a range of capabilities that contribute to long-term competitive advantage. As enterprises evaluate blockchain opportunities they should look beyond operational benefits to determine whether and how participation can affect firm strategy. In Table 1, we present a framework that identifies several ways blockchain solutions can enhance strategic capabilities. Blockchain participants can: 1) strengthen and leverage their existing capabilities; 2) share and build complementary capabilities and 3) build blockchain-specific capabilities.

The Blockchain-Based Strategic Capabilities Framework illustrates a wide range of strategic capabilities that can potentially be affected by blockchain solutions. Companies exploring blockchain solutions can use this framework as they evaluate whether these solutions offer opportunities for building and improving strategic capabilities.

A. Strengthen and Leverage Existing Capabilities

Some firms use blockchain to strengthen existing capabilities. They

accomplish this through 1) building on existing value propositions; 2) extending networks; and 3) gaining access to new markets.

1) *Build upon value propositions:* Atit Diamonds' use of blockchain supports its existing strategy. Its Rock Solid Diamond Collection is positioned as conflict-free and sourced using environmentally sensitive techniques [30]. Atit participates in the Everledger network, which uses blockchain to trace diamonds from their origin to the final consumer. A distributed ledger records information about the origination, processing and transport of the diamonds. These diamonds are distributed for sale to consumers who value these ethical practices. Through the blockchain ledger, distribution partners can provide customers and industry analysts the information needed to verify that its diamonds are sourced from conflict-free zones and have been processed and transported in an environmentally sensitive manner.

2) *Network reach:* The size and scope of a company's network of trading partners can be an important component of strategic advantage in some companies and industries. For example, the Japanese *Keiretsu*, a network of companies with obligational relationships characterized by goodwill, allows members of the network to lower business risk and to rely on information available to the *Keiretsu*. These trusted relationships developed over long periods of time, and have allowed networks of companies, such as those associated with *Mitsubishi* and *Sumitomo* to dominate Japanese industry.

Building reliable networks is challenging, especially when there are cultural, economic and institutional differences across firms. The ability to establish trust through blockchain solutions can help networks of firms establish relationships like those that characterize *Keiretsu*, but at a faster rate.

REX homes is a blockchain-based real estate brokerage company that uses smart contracts to establish relationships [31]. It does not participate in the private multiple listing service (MLS) owned and managed by the National Association of Realtors. Instead, REX homes use a blockchain to provide free and open access to real estate listings, which encourages clients, owners and brokers to participate in the network and increases its reach [31]. Network participants also benefit. Real estate owners can provide trustworthy inspection, maintenance and utility records and potential buyers can provide validated identity and financial data on the blockchain ledger. REX's blockchain-based business model has driven explosive growth in the volume of real estate transactions closed by REX [32].

3) *Access to markets:* Through their participation in blockchain, firms may gain access to new customers that become aware of their offerings as a result of interactions with other members of the consortium. A company might also access new markets, for example as a result of consolidating data or sharing processes with other consortium participants.

A blockchain initiative being piloted by the Municipal Transport Company of Madrid (EMT) allows passengers to access all the city's mobility services through a central location. Previously, travellers needed to register with each transport company and purchase tickets from those companies. Using a blockchain-based app, a traveller registers once, and purchases tickets that combine train, bus, motorcycle, scooter and bicycle routes into a single ticket. Because less-used modes of transport such as bicycles and scooters show up in suggested routes, customers who typically travel only by bus or train may begin to use alternative modes, creating opportunities for alternate transport services. Thus, participation in the consortium provides access to new customers and markets for these service providers.

B. Sharing Complementary Capabilities

As with all types of strategic alliances, competitive advantage is possible when blockchain partners can accomplish more together than they can separately. Pooling participants' valuable resources and abilities enable consortium partners to develop complementary capabilities to confer an

Table 1: Blockchain-Based Strategic Capabilities Framework

Build upon existing capabilities – Consortium participants can strengthen their existing capabilities.		
VALUE	CAPABILITY	EXAMPLE
Value proposition	Participants can strengthen their capability to verify claims made in their value proposition	Everledger gives diamond producers the ability to trace a diamond's true provenance and certify its value, increasing customer trust in the diamond's quality and origin in a conflict-free zone.
Network reach	Participants can expand their network of trading partners with verifiable information	REX Homes is a blockchain-based multiple listing service for commercial real estate. Real estate owners can provide trustworthy inspection, maintenance and utility records. Buyers can provide validated identity and financial data, increasing transaction efficiency.
Access to markets	Participants can gain access to new markets and customers	Municipal Transport Company of Madrid (EMI) allows transit passengers to use a single app to access all of the city's mobility services. As a result, partners gain access to new customers who had not previously booked with them.
Share complementary capabilities – Consortium participants can enhance capabilities through sharing complementary resources with partners.		
VALUE	CAPABILITY	EXAMPLE
Access to resources	Participants can leverage partners' resources	Consortium partners of The Port of Rotterdam allow the port to monitor the movement of goods. The Port can dynamically allocate resources such as slips, cranes and personnel to improve efficiency for transportation partners and enhance its own logistics advantage.
Access to data	Participants can gain access to new data housed on distributed ledgers shared by partners	The Insurwave marine insurance project allows Maersk, an intercontinental shipper, to purchase tailored insurance products based on real-time weather and route data gathered by Maersk's vessels and shared with insurers.
Shared risk	Participants can hedge against uncertainty through effective use of blockchain resources	MediLedger provides a track and trace system that enables pharmaceutical companies to enhance the security of opioids and other pharmaceuticals, to reduce counterfeits and enhance patient safety. This increases regulatory compliance and reduces risk for participants.
Strengthened relationships	Participants build relational capital that supports non-blockchain collaboration	The Pistoia Alliance collaborated on a multi-pharma partnership for decentralized identity management. Later, partners sponsored blockchain hackathons for potential joint investment opportunities.
Build blockchain-specific capabilities – Consortium participants can build new capabilities related to blockchain participation.		
VALUE	CAPABILITY	EXAMPLE
Smart contract expertise	Participants can gain expertise in using contracts to manage idiosyncratic business processes and agreements	GrainChain uses smart contracts to manage transactions between grain purchasers and farmers. The contracts escrow ownership and payments, with payments determined by complex calculations based on the weight of the shipment, moisture, chemical composition, timing and other variables.
Consortium and use case expertise	Participants can gain experience and resources that enable them to identify strategic use cases and join or found consortia	Henkel has experimented with numerous blockchain pilots and implementations. The company has developed deep consortium-related expertise and now participates in a diverse portfolio of blockchain projects.
New relationships and collaborations	Participants can develop relationships with consortium partners that enable subsequent blockchain collaborations	PharmaLedger's consortium members have been developing and testing blockchain use cases. Through their work on early projects, the consortium has established ethical and legal frameworks that now support eight use cases.

advantage on the individual partners. Blockchain solutions can promote synergistic capabilities through: 1) access to resources, 2) access to data and 3) the ability to share the risk of uncertainty. Each section includes examples from existing firms.

1) Access to resources: Companies can benefit from accessing resources through agreements with partners. A manufacturer, for example, may benefit from the advanced logistical capabilities of consortium partners, by offering greater precision and reliability in filling blanket purchase orders through dynamic routing processes. By enhancing communication, business agreements and data security, blockchain solutions allow partners to share resources safely. Partners can leverage these resources in ways that create value.

A blockchain consortium co-founded by The Port of Rotterdam,¹ designed to move beyond antiquated and fragmented record-keeping systems, allows participants to benefit [33]. Prior to this consortium, a single purchase order for a product being shipped globally can be typed over one hundred times in various siloed administrative systems. Tracking a shipment can require phone calls to several partners along the route. In the blockchain pilot, carriers allow the port access to logistics resources and information. Access to partners' shipping plans and planning algorithms can facilitate the dynamic allocation of personnel, boat docking slips, cranes, and equipment needed to move cargo. The Port can thus enhance its existing advantages in logistics and port management. Tighter coupling between shippers and ports allows more efficient resupply, loading, and crew management operations – resulting in value created for the shippers through higher levels of asset utilisation.

2) Access to data: Blockchain solutions can be used to implement data-sharing agreements among members in the shared ledger. Pooling data can provide partners with information that was previously unavailable. When combined with a partner's unique resources and capabilities, it can form the basis for new value creation, and this value may exceed the risk partners previously associated with sharing private data.

Maersk, a founder of the well-known TradeLens shipping information platform, participates in a blockchain that provides access to tailored insurance products. The industry is currently fragmented, with different insurers providing insurance for vessels, cargo, port access and other shipping elements, and reinsurers and retrocession insurers managing secondary insurance needs. Maersk has joined the Insurwave marine insurance project which uses smart contracts to streamline the insurance process [34]. Sharing vessel information through the Insurwave consortium has enabled Maersk to purchase tailored insurance products. Insurers provide products based on real-time risk data gathered by Maersk's vessels as they transport goods through various locations and weather conditions. These products, designed to meet its precise needs, enable Maersk to cost-effectively hedge against uncertainty associated with weather and other marine transport risks and to manage its trade more efficiently.

3) Share Risk among Partners: Participation in an enterprise consortium allows a firm to work with partners to share and reduce risk. Key to this is the ability of blockchain to verify information instantaneously for consortium partners as well as regulators, auditors and other parties that monitor compliance.

The Medilegger project was designed to help pharmaceutical industry participants comply with the demands of the Drug and Supply Chain Security Act, intended to ensure that pharmaceutical products sold in the US are legitimate and that trading partners are appropriately licensed and authorized [35]. Participants in Medilegger can enforce business rules and ensure compliance without exposing private data. The consortium allows partners to adapt to evolving regulations and share compliance and safety risks.

4) Strengthen collaborative relationships: Participants in blockchain consortia develop relational capital through common goals, close interaction, and reciprocity required for effective governance [36]. These relationships can improve operational performance of the partners and can provide the basis for taking advantage of mutually beneficial opportunities in the future [37].

The Pistoia Alliance, in an enterprise consortium made up of large pharmaceutical companies, participated in a use case analysis workshop to identify potential blockchain projects. The alliance has since developed the Informed Consent blockchain project which is designed to demonstrate the benefits of using blockchain-based decentralized identity methods to improve the security and consistency of processes for providing and revoking consent. The project enables patients to own and control their own personal data and to grant and revoke consent in clinical trials [38].

Participating in projects like these builds collaborative strategic relationships between these companies as they work together toward the development of common policies and processes for governing the shared blockchain solution. Subsequent to their informed consent collaboration, partners jointly sponsored a blockchain hackathon to identify solutions to communicable disease. The Pistoia Alliance has launched a seed fund through which they make joint investments in promising projects [39].

C. Building New Capabilities Around Blockchain Technologies

Companies participating in blockchain consortia can build new capabilities around a blockchain competency. These meet the definition of capabilities as organisationally embedded, non-transferable firm-specific resources. We suggest that these blockchain capabilities are the most overlooked potential sources of competitive advantage when firms focus on the operational improvements delivered by blockchain. Firms may use these new capabilities as the foundation for development of strategic capabilities and then position the company to participate in additional strategic alliances more easily, including blockchain consortia. We illustrate how new capabilities can be built around: 1) specific tools such as smart contracts or 2) around general capabilities around blockchain implementation or blockchain management.

1) Smart contract expertise: Smart contracts are programs, run on the blockchain, that implements policies and contract obligations in software. They can execute, control and archive events as specified in legal contracts or agreements. These programs can respond in close to real time to triggering events. Smart contracts can be as simple or as complex as the agreements between contracting parties. As companies become more experienced in developing smart contracts, they can manage increasingly complex and idiosyncratic agreements effectively. Further, knowing that such agreements can be codified may enable new agreements that could only be executed through smart contracts.

Developing expertise in smart contracts can minimize the risks of contract failures due to security vulnerabilities and coding errors [40]. Ricardian contracts, which create machine-readable equivalents to prose contracts, can help alleviate some contracting problems [41]. Companies that develop the technological resources to effectively design secure and accurate contracts can extract greater value.

GrainChain uses smart contracts to manage payments and transfer of goods between farmers, trucking companies, grain silos, grain purchasers and banks [42]. Where contracts once had to be manually calculated and adjusted according to the amount and nature of grain delivered, this process is automated through smart contracts. When a truckload of grain is received at a silo, it is weighed and classified on a variety of quality and chemical attributes. Smart contracts use test results to price delivery according to previously executed agreements between the farmer and purchaser. Once the delivery and its characteristics are recorded, payment can be issued immediately to the farmer—a vast improvement from a

process that could take weeks and was error-prone.

2) *Consortium-related managerial expertise*: Participating in blockchain consortia requires companies to participate in blockchain governance, which determines the rules and procedures participants must follow when interacting with the blockchain. Through this process, firms learn how to become effective consortium participants. Firms also gain experience forming relationships across the network, which is significant because blockchain allows for linkages with new partners as the network grows. To capture value, participants must learn how to manage and prioritize these linkages.

Experience with one blockchain solution can be used to more effectively identify use cases that will result in value creation and capture and seek out or build solutions for these use cases. The consortium-related capabilities a company develops through participation in one consortium can carry over to these new solutions. Furthermore, an experienced company can evaluate the implications of a blockchain's functions, governance mechanisms and the effects on the company as well as its strategic relationships over time.

Henkel, a large consumer goods company, has taken an active learning approach to the development of blockchain-related capabilities [43]. The blockchain innovation team uses "discovery workshops" to identify and evaluate potential use cases throughout the company and its institutional capability in blockchain is growing steadily. The company also participates in the development of standards and certifications that build greater confidence in, and accelerate the adoption of blockchain solutions. It also participates in trade organisations and events that enhance learning and foster cross-industry cooperation.

blockchain-related relational capital that provides the foundation for future blockchain collaborations that draw upon and build capital around relationships that enables value-capture for collaborators through joint blockchain projects.

PharmaLedger, a consortium of pharmaceutical companies and public and private entities engaged in healthcare solutions. The 29 participants worked collaboratively to develop a platform to support the design and development of blockchain solutions that would support innovation across the ecosystem. Consortium partners have formed and strengthened relationships that enable the creation of value through blockchain collaborations. Through this effort, the group has developed ethical and legal frameworks and an industry digitisation strategy, and a marketplace for health data. [44] These artifacts are the tangible products of the relational capital developed through collaboration and have paved the way for the consortium to develop eight healthcare-related use cases in its three-year tenure. [45]

6. Conclusion

Despite its promise, blockchain has not yet achieved its potential. While the operational benefits of blockchain adoption are widely recognized, strategic benefits are not well understood, even among technical and strategic leaders involved in their implementation. We present memberships in blockchain consortia as forms of strategic alliances and use RBV to motivate the introduction of strategic alliances as a tool to access resources that can be the basis of competitive advantage. We illustrate how strategic value can be created through three avenues. The first is by joining alliances and building relationships that enhance and contribute to existing capabilities.

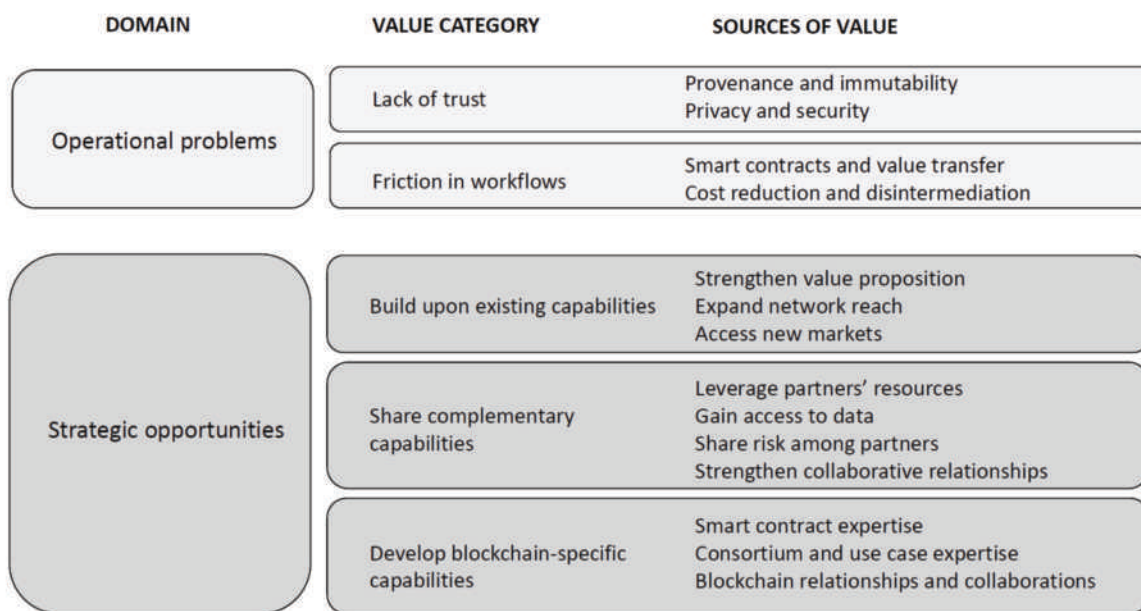


Figure 1: Blockchain Strategic Opportunities and Unexplored Sources of Value

Henkel's pilot blockchain project focused on more effective tracking and exchange of transport pallets. The company has since participated in a variety of unrelated blockchain consortia including PlasticBank, a social enterprise that recycles ocean plastic, and TaxChain, which captures value-added taxes (VATs) through cross-border supply chains. Henkel has developed deep consortium-related blockchain expertise and now has "one of the most diverse blockchain portfolios in the enterprise space" [43].

3) *Blockchain relational capabilities*: Blockchain expertise can be developed by individual firms, but collaborators in blockchain projects can develop

The second by sharing and building complementary capabilities with partners through access to resources and data as well as sharing risk among partners. The third by building blockchain capabilities through gaining smart contract expertise developing more managerial expertise around implementing blockchain solutions. The domain of strategic opportunities by blockchain allows firms and consortia to create value through multiple sources. Figure 1 summarizes the contributions of this paper in explicating these opportunities.

Embedded in the RBV is the concept of capabilities as sources of

competitive advantage that are built over time and difficult to imitate or substitute. This implies first-mover advantage potential, even as blockchain is still nascent. Firms that aggressively build these capabilities can not only be part of the conversation but also have the potential to shape the conversation around implementation of blockchain consortia. Dale Chrystie, FedEx's blockchain strategist, refers to the urgency of developing capabilities as "not yet, but don't be late for the game" [46]. Firms deciding not to invest in blockchain face the risk of being locked out of the new competitive landscape as industries will be fundamentally disrupted and changed.

As blockchain solutions are adopted, assumptions about firm boundaries will be challenged. Many theories in strategic management, including RBV, are rooted in economic theories that focus on firm-level behaviour and performance. Adoption of a stakeholder perspective, in contrast, necessitates conceptualising performance beyond the firm level [15]. The adoption of blockchain can lead to shrinking or expanding firm boundaries [6]. As we focus more broadly on ecosystems, questions about transactions being "within" or "outside" a firm's boundary are less important than questions about how bundles of exchanges can generate social and economic wealth [47]. A Transaction Cost Economics view of blockchain may be helpful for future scholarly work.

Effective deployment of enterprise blockchain solutions can facilitate the development of trust, cooperation and risk-sharing among firms that otherwise may only consider each other as competitors. This allows firms to think beyond a binary view of competition and cooperation and embrace "coopetition" [48], [49], [50]. Blockchain encourages the kind of openness and collaboration associated with trade or standards organisations or with open-source software development projects in which long-term collaboration among partners is more typical.

As blockchain solutions become ubiquitous, traditional relationships, business models and entire industries will be disrupted. We agree with the World Economic Forum [51] that blockchain has the potential to revolutionize how companies compete and collaborate, and that strategic value can be captured by companies that begin the process of building strategic capabilities through blockchain.

Your organization or industry cannot sit on the sidelines for 3-5 years waiting for the technology to mature. If the blockchain solutions are relevant to your business, you should start preparing a non-technical and technical foundation progressively for the eventual mainstream operations. [51, p. 8]

References:

- [1] L. Pawczyk, J. Holdowsky, R. Massey, and B. Hansen, "Deloitte's 2020 global blockchain survey, from promise to reality," Deloitte, 2020. [Online]. Available: https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf [Accessed: 26 Feb 2021].
- [2] K. Gilbert, "The complete guide to blockchain business networks," ConsenSys, New York, NY, USA, APR. 2020. [Online]. Available: <https://consensys.net/insights/the-complete-guide-to-blockchain-business-networks> [Accessed: 26 Feb 2021].
- [3] T. Felin, K. Labkani, "What problems will you solve with blockchain?" MIT Sloan Management Review, vol. 60, no. 1, pp. 32-38, Sept. 2018.
- [4] N. Naqvi, M. Hussain, "Evidence-based blockchain: Findings from a global study of blockchain projects and start-up companies," The Journal of The British Blockchain Association, Sep 1:16795, 2020.
- [5] Forrester Consulting, "The Total Economic Impact™ of IBM blockchain," Jul. 2018. [Online]. Available: <https://www.ibm.com/downloads/cas/QJ4XA0MD> [Accessed: 26 Feb 2021].
- [6] H. Treiblmaier, "The impact of the blockchain on the supply chain: a theory-based research framework and a call for action," Supply Chain Manage.: Int. J., vol. 23, no. 6, pp. 545-559, Sept. 2018, doi: 10.1108/SCM-01-2018-0029.
- [7] M. Higginson, M. C. Nadeau, K. Rajgopal, "Blockchain's occam problem," McKinsey & Company, New York, NY, USA. <https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem> [Accessed: 29 Nov 2020].
- [8] C. Mulligan, J. Z. Scott, S. Warren, J. P. Rangaswami, "Blockchain beyond the hype," World Economic Forum, Cologny, Switzerland, White Paper, 2018. <https://www.weforum.org/whitepapers/blockchain-beyond-the-hype> [Accessed: 26 Feb 2021].
- [9] S. Davies and S. Likens, "Make the blockchain business case: evolution, not revolution," PwC, 2017. <https://www.pwc.com/gx/en/industries/technology/blockchain/blockchain-in-business/make-the-business-case.html> [Accessed: 1 Dec 2020].
- [10] S. Gupta, S. Duncan, T. Mondal, M. Madhur, "HFS top 10 enterprise blockchain services 2020," HFS Financial, Fort Collins, CO, USA, 2020. <https://www.hfsresearch.com/research/hfs-top-10-enterprise-blockchain-services-2020> [Accessed: 26 Feb 2021].
- [11] IBM, *The founder's handbook: An introduction to building a blockchain solution*, 3rd ed. Somers, NY, USA: IBM Corporation, 2020.
- [12] J. Cuomo, et al., "Fast forward: Rethinking enterprises, ecosystems and economies with blockchains," IBM Corporation, Somers, NY, USA, 2016. <https://www.ibm.com/downloads/cas/QP4AE4GN> [Accessed: 26 Feb 2021].
- [13] S. Klein, W. Prinz, W. Gräther, "A use case identification framework and use case canvas for identifying and exploring relevant blockchain opportunities," in Proc. 1st ERCIM Blockchain Workshop 2018, in Reports of the European Society for Socially Embedded Technologies: vol. 2, no. 5, W. Prinz and P. Hoscicka, Eds. May 2018, doi: 10.18420/blockchain2018_02.
- [14] S. Warren, et al., "Get the full picture," Accenture, Dublin, Ireland, 2019. <https://www.accenture.com/us-en/insights/blockchain/wef-building-value> [Accessed: 26 Feb 2021].
- [15] J. B. Barney, "Firm resources and sustained competitive advantage," *Journal of Management.*, vol. 17, no.1, pp. 99-120, Mar. 1991, doi: 10.1177/014920639101700108.
- [16] R. Gulati, "Alliances and networks," *Strategic Management Journal.*, vol. 19, no. 4, pp. 293-317, Dec. 1998, doi: 10.1002/(SICI)1097-0266(199804)19:4<293::AID-SMJ982>3.0.CO;2-M.
- [17] M. A. Hitt, M. T. Dacin, E. Levitas, J. L. Arregle, and A. Borza, "Partner selection in emerging and developed market contexts: Resource-based and organizational learning perspectives," *Academy of Management Journal*, vol. 43, no. 3, pp. 449-467, June 2000, doi: 10.2307/1556404.
- [18] J. C. Jarillo, "On strategic networks," *Strategic Management Journal*, vol. 9, no. 1, pp. 31-41, Jan./Feb. 1988, doi: 10.1002/smj.4250090104.
- [19] R. D. Ireland, M. A. Hitt, and D. Vaidyanath, "Alliance management as a source of competitive advantage," *Journal of Management*, vol. 28, no. 3, pp. 416-446, June 2002, doi: 10.1016/S0149-2063(02)00134-4.
- [20] B. Wernerfelt, "A resource-based view of the firm," *Strategic Management Journal*, vol. 5, no. 2, pp. 171-180, Apr. 1984, doi: 10.1002/smj.4250050207.
- [21] J. B. Barney, "Firm resources and sustained competitive advantage," *Journal of Management*, vol. 17, no.1, pp. 99-120, Mar. 1991, doi: 10.1177/014920639101700108.
- [22] M. A. Peteraf, "The cornerstones of competitive advantage: a resource-based view," *Strategic Management Journal*, vol. 14, no. 3, pp. 179-191, Mar. 1993, doi: 10.1002/smj.4250140303.
- [23] D. J. Teece, G. Pisano, and A. Shuen, "Dynamic capabilities and strategic management," *Strategic Management Journal.*, vol. 18, no. 7, pp. 509-533, Aug. 1997, doi: 10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.
- [24] M. Peteraf, G. Di Stefano, and G. Verona, "The elephant in the room of dynamic capabilities: Bringing two diverging conversations together," *Strategic Management Journal*, vol. 34, no. 12, pp. 1389-1410, Dec. 2013, doi: 10.1002/smj.2078.
- [25] R. Makadok, "Toward a synthesis of the resource-based and dynamic-capability views of rent creation," *Strategic Management Journal*, vol. 22, no. 5, pp. 387-401, May 2001, doi: 10.1002/smj.158.
- [26] G. Hooley, A. Broderick, and K. Möller, "Competitive positioning and the resource-based view of the firm," *Journal of Strategic Marketing*, vol. 6 no. 2, pp. 97-116, June 1998, doi: 10.1080/09652549800000003.
- [27] F. Rothaermel, *Strategic Management*, 5th ed. New York, NY, USA: McGraw Hill, 2020.
- [28] R. Gulati, N. Nohira, and A. Zabeer, "Strategic networks," *Strategic*

Management Journal, vol. 21, no. 3, pp. 203-215, Mar. 2000, doi: 10.1002/(SICI)1097-0266(200003)21:3<203::AID-SMJ102>3.0.CO;2-K

[29] Y. L. Doz and G. Hamel, "Alliance advantage: The art of creating value through partnering." Cambridge, MA, USA: Harvard Univ. Press, 1998.

[30] Retail Technology Innovation Hub, "Everledger and Shairu & Atit Diamonds announce blockchain jewellery first." Retail Technology Innovation Hub. <https://retailtechinnovationhub.com/home/2020/4/22/everledger-and-shairu-amp-atit-diamonds-announce-blockchain-jewellery-first> [Accessed: Feb 26 2021].

[31] REX Homes, "About Us." <https://www.rexhomes.com/about> [Accessed: 26 Feb 2021].

[32] REX Homes, "Real Estate Innovation Supporting California's Housing Market Recovery in 2020." PR Newswire. <https://www.prnewswire.com/news-releases/real-estate-innovation-supporting-californias-housing-market-recovery-in-2020-301108149.html> [Accessed: 26 Feb 2021].

[33] Port of Rotterdam, "How Rotterdam is using blockchain to reinvent global trade," Port of Rotterdam. <https://www.portofrotterdam.com/en/news-and-press-releases/how-rotterdam-is-using-blockchain-to-reinvent-global-trade> [Accessed: 26 Feb 2021].

[34] N. Morris, "EY Maersk blockchain marine insurance platform goes live." Ledger Insights. <https://www.ledgerinsights.com/blockchain-marine-insurance> [Accessed: 26 Feb 2021].

[35] Medilegger, "Leaders from 24 companies in the US pharmaceutical supply chain collaborate to submit the MediLedger DSCSA pilot project final report to the FDA, proposing blockchain for an interoperable track and trace system for US prescription drugs," PR Newswire, <https://www.prnewswire.com/news-releases/leaders-from-24-companies-in-the-us-pharmaceutical-supply-chain-collaborate-to-submit-the-medileggers-dscsa-pilot-project-final-report-to-the-fda-proposing-blockchain-for-an-interoperable-track-and-trace-system-for-us-prescription-301008871.html> [Accessed: 26 Feb 2021].

[36] Dyer, J.H., & Singh, H. (1998). The relational view: Cooperative strategy and sources of interorganizational competitive advantage. *Academy of Management Review*, vol. 23 no. 4 pp. 660-679. <https://doi-org.proxy.lib.pdx.edu/10.5465/amr.1198.125>.

[37] Yu, Y., & Huo, B. (2019b). The impact of relational capital on supplier quality integration and operational performance. *Total Quality Management and Business Excellence*, vol. 30 no. 11-12, pp. 1282-1301. <https://doi-org.proxy.lib.pdx.edu/10.1080/14783363.2017>.

[38] Pistoia Alliance. <https://www.pistoiaalliance.org/projects/current-projects/informed-consent-blockchain/> [Accessed: 26 Feb 2021].

[39] Pistoia Alliance. <https://www.pistoiaalliance.org/blog/learnings-from-judging-the-code2care-hackathon-the-winners-ideas-and-themes-and-most-importantly-focusing-on-the-patient/> [Accessed: 26 Feb 2021].

[40] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (sok)." In *International conference on principles of security and trust*. Springer, Berlin, Heidelberg, 2017.

[41] J. Hazard and H. Haapio, "Wise contracts: Smart contracts that work for people and machines," Trends and communities of legal informatics. *Proceedings of the 20th international legal informatics symposium IRIS*. 2017.

[42] PYMNTS, "Blockchain tackles farming's cash flow bottlenecks." PYMNTS. <https://www.pymnts.com/news/b2b-payments/2020/grainchain-blockchain-farming-cash-flow-risk> [Accessed: 01 Dec 2020].

[43] A. Day, Producer, "Blockchain in consumer goods with Rodolfo Quijano from Henkel," *Blockchain Won't Save the World: Season 1 Episode 20*, July 28, 2020. [Podcast]. Available: <https://www.blockchainwontsaveit.world/> [Accessed: 01 Dec 2020].

[44] PharmaLedger <https://pharmaledger.eu/about-us/the-project/> [Accessed: 15 Feb 2021].

[45] PharmaLedger <https://pharmaledger.eu/wp-content/uploads/PharmaLedger-2020-End-Year-Press-Release.pdf> [Accessed: 15 Feb 2021].

[46] REIMAGINE 2020 - Global Blockchain Education, REIMAGINE 2020 v1.0 - Dale Chrystie - FedEx. (May 21, 2020). [Online Video]. <https://www.youtube.com/watch?v=0kuUnMxapZ4> [Accessed: 01 Dec 2020].

[47] S. A. Alvarez, U. Zander, J. B. Barney, and A. Ajuah, "Developing a theory of the firm for the 21st century," *Academy of Management Review*, vol. 5, no. 4, pp. 711-716, Nov. 2020, doi: 10.5465/amr.2020.0372.

[48] W. Hoffmann, D. Lavie, J. J. Reuer, and A. Shipilov, "The interplay of competition and cooperation," *Strategic Management Journal*, vol. 39, no. 12, pp.

3033-3052, Dec. 2018, doi: 10.1002/smj.2965.

[49] D. Lavie, "The competitive advantage of interconnected firms: An extension of the resource-based view," *Academy of Management Review*, vol. 31, no. 3, pp. 638-658, July 2006, doi: 10.2307/20159233.

[50] B. J. Nalebuff and A. M. Brandenburger, "Co-opetition: Competitive and cooperative business strategies for the digital economy," *Strategy Leadership*, vol. 25, no. 6, pp. 28-34, June 1997, doi: 10.1108/eb054655.

[51] N. Hewett, S. Deshmukh, S. Furiya, F. Jee, A. Albabil, "The World Economic Forum's blockchain deployment toolkit," *World Economic Forum, Cologny, Switzerland*, 2020. [Online]. Available: <https://widgets.weforum.org/blockchain-toolkit/modules> [Accessed: 26 Feb 2021].

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

All authors made substantive contributions to the manuscript.

Funding:

Publication of this article in an open access journal was funded by the Portland State University Library's Open Access Fund.

Acknowledgements:

We appreciate the insights provided by Stanton Heister and Skye Lininger of Portland State University's Business Blockchain Certificate Program.

¹ This solution was developed through its Blocklab subsidiary which was co-founded by The Port of Rotterdam and the City of Rotterdam.

Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices

¹Tim Weingärtner, ²Oskar Camenzind

¹Blockchain Lab, Lucerne University of Applied Sciences, Switzerland

²Building Technologies Division, Siemens Schweiz AG, Switzerland

Correspondence: Tim.Weingaertner@hslu.ch

Received: 31 December 2020 **Accepted:** 20 February 2021 **Published:** 24 February 2021

Abstract

Identity is a crucial property of Internet of Things (IoT) devices. Due to rapid growth and high numbers of similar devices, reliable identification of those devices is a problem. The origin and history of an IoT device is especially important in security-relevant environments.

Our research addresses this issue by proposing an approach based on blockchain and decentralised identifiers (DID). It is inspired by the concepts of self-sovereign identity (SSI) and bootstrapping of remote secure key infrastructures (BRSKI). Devices are equipped by the manufacturer with an identity stored in a trusted execution environment (TEE) and secured by a blockchain. This identity can be used to trace back the origin of the device. During the bootstrapping process on the customer side, the identity registration of the device is updated in the blockchain. This process is performed by a so-called registrar. Smart contracts prevent unsolicited transfer of ownership and track the history of the device. Besides proof of origin and device security our concept can be used for device inventory and firmware upgrade.

A prototype implementation was realised to validate the concept. All six use cases have been implemented and tested using an Ethereum blockchain infrastructure. JSON Web Tokens (JWT) have been used as signed artefacts to transfer information between the stakeholders. This enables an asynchronous communication needed for example in an environment with no direct internet access. Such an infrastructure can be provided by an independent association and can be used by all manufacturers. Depending on the environment a registration of devices can be optional or mandatory.

Keywords: *enterprise blockchain, consortium, ecosystem, strategic alliances, resource-based view, competitive advantage, strategic capabilities*

JEL Classifications: *0020M15 IT Management*

1. Introduction

The rapidly growing number of devices used for the Internet of Things (IoT) is raising concerns about the origin and history of these devices. Security issues regarding IoT devices lead to new concepts about bootstrapping and administration. Identity becomes a crucial property of IoT devices. So far there are primarily proprietary solutions. In a multi-provider environment those kinds of approaches have major disadvantages since the customer himself is responsible for administration.

In this paper we propose a new approach applying concepts from self-sovereign identity to IoT devices ensuring their identity and history. Derived from [1] we call our approach a “Manufacturer Authorized Signing Authority Blockchain Infrastructure” (MASA-BI). As the name implies, the system is based on the blockchain technology to ensure immutability, autonomy and unified interfaces.

First, we will give a short introduction into the topic of identity and self-sovereign identity summarizing the major concepts used here. The related work shows the already existing approaches and illustrates the previous knowledge our approach is based on. Our approach consists of six use cases (UC1–UC6) which are arranged around two main application areas. The analysis of advantages and disadvantages as well as a final conclusion completes the paper.

2. Identity

When speaking of identity, the first thing that comes to mind is the identity of a person. *Webster*¹ defines identity as “the distinguishing character or personality of an individual”. Beside the psychological aspects of identity, we use it to distinguish persons from each other. The identity check uses attributes of an entity to verify if a person is the one, he or she claims to be. Those attributes can be physical or non-physical. Physical or physiological attributes which define an identity are fingerprints, face, iris structure, voice, DNA, smell, speech, location as well as possession or access to physical objects like identity card, mobile device, notes, etc. Non-physical attributes which define our identity mainly depend on our brain like knowledge, abilities, memories, experiences, relationships, feelings, wishes, behavior or secrets. For an identity check we compare those attributes with previously stored data. Most of the time we use a combination of different attributes. At the airport, the identity card a person possesses is checked against his appearance. In addition, biometrical data like face lineaments are compared. When a password is requested the knowledge of an individual is checked, sometimes in combination with a message to the mobile phone which should be in possession and access of this person. The attributes can be classified by their difficulty to copy, steal, or guess them.

The identity of a “thing” has some similarities to those of a person even though a thing can be copied. For example, each specimen of a certain sensor is identical if we do not get on an atomic level. We can give them an identity by adding individual attributes like a serial number. If a sensor has

a memory chip, its “experiences” can make it different to a similar device.

But why do things need an identity? If we want to move into the direction of a digital twin - the digital copy of a physical object - identity is crucial [2]. Each data point which is detected in the real world has to be assigned to the corresponding position of the digital twin. Errors or fraud have to be excluded. Otherwise, the digital twin is just an anonymous copy.

Securing this identity is a big challenge today and there is a lot of research going on in this area [3]. Since all digital data can be copied easily one has to take steps to avoid this and protect the identity of a device. Most common, secured elements are used, that make it hard to impossible to access those data. To avoid the copying of data at the interface level the data has to be signed by the device. It has to be kept in mind that the needed processing power for the cryptographic calculations of the signing process has to be provided by the device.

2.1. Self-sovereign identity

Self-Sovereign Identity (SSI) allows a person to create her own identity and get a verification or proof by a trusted third party such as the government. Although SSI is independent of blockchain technology it is often used together. Blockchain has seen a rise in importance as a technology to store data in an immutable way there therefore to guarantee and confirm identity. Systems like uPort² or Sovrin³ together with Hyperledger Indy are just some examples of existing solutions. Since no personal data is stored on the blockchain, the compliance to GDPR (General Data Protection Regulation) is assumed [4]. There is still some doubt about it and clear guidelines from the regulators are demanded [5].

With the concept of self-sovereign identity using Decentralized Identifiers (DIDs) [6] it is possible to store identities and verifiable claims on the blockchain. The DID is a globally unique identifier which does not need an explanation since its DID scheme links to a specific method explaining how the DID is resolved and links to a DID document describing all details. The DID document is fully self-describing and contains information about the entity the DID is about. This includes cryptographic information or service endpoints. For GDPR compliance reasons it is important that neither DID nor DID document contain person-related information.

A DID looks like:

did:ethr:0xe34eac30c498d9e26865f64fcaa57dbb935b0d7a
and consists of three parts separated by a colon:

1. String “did” for the URL scheme
2. DID method⁵
3. Specific identifier

While the DID represents the identity of the entity, additional verifiable claims describe qualities or properties of the entity [7]. Those claims have to be issued by a trusted party which itself is represented by an identity (DID). Verifiable claims can be stored on a blockchain to ensure immutability and independence from the availability of the issuer. The uPort in [8] shows an example of such an ecosystem. While claims are stored for example in a smart contract on a blockchain, JSON Web Tokens (JWT) can be used to transfer and interchange verifiable claims off-chain [9][10].

JWT consists of three parts separated by dots [11]:

1. Header, with information about the signing algorithm
2. Payload, containing the claim
3. Signature, which is the signed header and payload

To reduce the size, the header and the payload are Base64Url encoded. The claim itself contains information about the issuer and the date of

issuing, the subject or entity the claim is about, the audience the claim is intended for and optionally an expiration time. Further optional fields are possible. Examples and libraries for JWT can be found on jwt.io⁶.

3. Related work

Self-sovereign identity of persons is discussed in several research papers [12][13][14][15]. Some of them cite the ten key properties of self-sovereign identity from C. Allen [16]:

1. Existence of the entity in the real world
2. Control from the entity over its identity
3. Access to the own data
4. Transparency about the systems and algorithms used
5. Persistence and long-liveness of the identity
6. Portability of the identity to guarantee independence of systems
7. Interoperability of the identity through open standards
8. Consent of the entity to share or use their identity
9. Minimalisation of data that is disclosed through a claim
10. Protection of the entities’ rights

Al-Bassam describes in his paper [17] a smart contract-based identity system where each entity is represented by an Ethereum address. His SCPKI system focusses on persons or organisations as entities which control their identity over the private key to their Ethereum address. A claim or proof is reduced to a Boolean value in the attributes of an identity.

Self-sovereign identity is seen by Der et al. [18] as one of the essential enablers for a digital revolution. In the outlook of their paper the usage of self-sovereign identity for things is mentioned as future research area. Conceptual questions like “How can a non-human entity recognize and characterize its own identity”, are raised.

A first overview about self-sovereign identity for Industrial Internet of Things (IIoT) is presented by Bartolomeu et al. [19]. Their paper provides a review of several use-cases and challenges Self-Sovereign Identity face in the context of IIoT. One application mentioned is the authentication of devices. It is mentioned that most solutions rely on a centralised instance and blockchain-based SSI is one possibility to overcome this drawback.

4. Giving a device an identity during manufacturing

As described above, a device has to “receive” an identity to act as a unique digital twin. Since this identity is not linked to physical uniqueness it is an artificial act. Therefore, this is security wise a critical moment and should be done during manufacturing and in a secured environment. There are several possibilities to include a secured environment on a chip to store this identity in a save way. Trusted Execution Environments (TEE) represent one solution for it. Shepherd et al. [20] give an overview of actual technologies. Companies like Intel, LEGIC⁷ or Riddle & Code⁸ provide products to store private keys in a secure element on a chip. In our approach we leave this intentionally to the manufacturer.

We propose a system containing a smart contract *DIDManufacturerInventory* which manages the identities of IoT devices. Our prototype is based on the Ethereum blockchain and its signature system since this infrastructure offers the broadest development environment. The implementation can be easily ported to another blockchain environment that offers similar features. While each device holds its address and the access to it as private key the proposed smart contract acts as proof of origin of the device. In our proposal the device manufacturer generates a private key and an Ethereum address (derived from the public key) according to the Ethereum address requirements [21] and stores this in a secure area on the device. Either way, once this identity is created on the device as required, or if the device is used in a secure environment, we assume that the device eventually contains its private key, which cannot be accessed from outside the device.

Since the private key grants access to the blockchain the device now has a) access to its address on the Ethereum blockchain and b) can sign messages with its private key. The access to the blockchain is not required for our approach since we want to avoid high resource consumption.

In a first step the manufacturer generates his own Ethereum address and registers to the DIDManufacturerInventory once. This is the first use case which has been implemented in our prototype (UseCase1 = UC1). We intentionally decided not to require proofs for the identity of manufacturers to reduce the hurdle of participating in such a system. At a later stage this can be introduced easily. With his account address the manufacturer can register as many devices as wanted. Each device receives its own Ethereum address as describe above. The device registration process is the second use case (UC2). It stores the public key of the device in the smart contract. For data privacy reasons a manufacturer can possess more than one address on the blockchain (UC1). Besides this, no identifying data is stored on the blockchain. During UC2 trusted public keys of MASA nodes have to be stored on the device. We will see later on the purpose of this measure.

5. Bootstrapping a device in a new environment

The second part of our proposal is related to the registration in the client environment. Once the device is shipped and installed at the premises of the customer the bootstrapping process begins (see Figure 1). The registrar has the role of an onsite registration authority. Usually, one registrar per site is foreseen and a 1:1 relation between device and registrar will hold for most cases. Nevertheless, it is also possible to use several registrars which we will see in UC6.

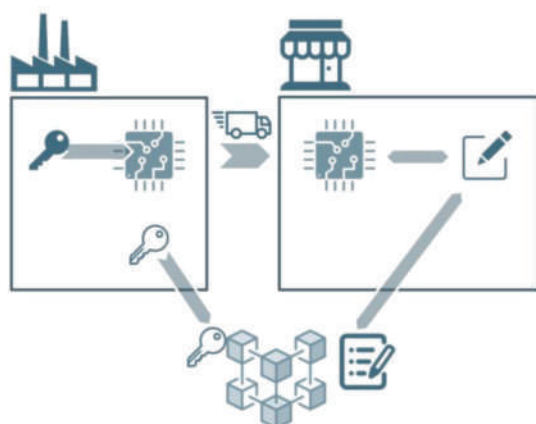


Figure 1: Overall process from manufacturing to registration in the client environment.

UC3 represents the initial registration use case of the registrar in the smart contract DIDInventory. This process is very similar to the registration of a manufacturer (see UC1) and is as well self-sovereign. Due to design reasons, we separated the identity distribution during manufacturing (UC1 and UC2) from the bootstrapping at client environment (UC3–UC6) by two separate smart contracts. It can be decided at a later stage if one blockchain for both environments should be used or if they are to be kept separately. We discuss the advantages and disadvantages in section 7.

After the registrar is authorised as such, the bootstrapping of the device can start (UC4). This process is derived from BRSKI [1]. It can be initiated by the device looking for a registrar through first boot up, via a manual action like pressing of a button, or by accessing the device with an initial call. The bootstrapping process UC4 contains 10 steps (see Figure 2):

1. **Device** informs the surrounding that it is active or is initially called.

2. **Registrar** sends its identity (public Ethereum address) to the device.
3. **Device** includes the registrar's identity in a JSON Web Token JWT1 and signs this token with its private key and sends it to the registrar.
4. **Registrar** includes JWT1 into a new JSON Web Token JWT2 and signs this token with the registrar's private key.
5. **Registrar** calls the DIDInventory smart contract as message sender and passes the device address. This step is needed since the blockchain should not handle JWTs due to their length and the resulting gas costs. DIDInventory registers the assignment between device and registrar with a tentative state.
6. **Registrar** submits JWT2 to a MASA-BI node which is a server application connected to the blockchain.
7. **MASA-BI** node checks the validity of JWT2 and the registration in DIDInventory (step 5). If both are valid the MASA-BI node proofs the assignment in DIDInventory. Afterwards DIDInventory changes the state to active.
8. **MASA-BI** node generates a JSON Web Token JWT3 with a confirmation about the assignment, signs it with its private key and sends it to the registrar.
9. **Registrar** forwards JWT3 to the device.
10. **Device** verifies the signature of the MASA-BI node with its built-in list (in secured environment) and if ok adds the registrar to its trust list.

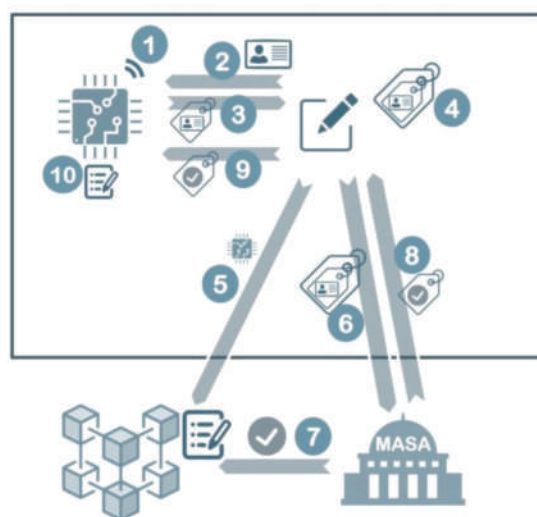


Figure 2: Bootstrapping process UC4.

As extension the use of a nonce can be applied to enhance security (see [1]). Furthermore, the JWTs could be provided with an expiration time to reduce the risk of a replay attack.

Since the DIDInventory holds the assignment the registrar can always check this using the read function. This function is restricted to the individual registrar. We are aware that at the actual prototype using the transaction history everybody can possibly read this assignment. It is our intention to improve this in a second version with the actual developments going on regarding Zero Knowledge Proof and Ethereum 2.0.

Bootstrapping variations

Further use cases are exceptional cases and are based on UC4:

UC5: Assignment of a device that is out of reach of an internet connection
UC4 assumes that the device, the registrar and the MASA node are connected. If the device is placed in a shielded environment where no direct internet connection is possible the registrar can act as a transportation medium. In this case the registrar has to move from the shielded environment of the #

device to an environment where an internet connection is possible. The expiration of the JWTs has to be chosen accordingly.

UC6: Transfer of a device from registrar A to registrar B

There might be the need for a change in registrars. This can be the case due to change in ownership or responsibility like change of tenants or due to additional registrars. In our approach this case is handled by a two-phase process. In a first phase the assigned registrar A reports a new registrar B to DIDInventory. In the second phase UC4 is applied to registrar B and DIDInventory handles the transfer. We use a special type attribute in the JWT payload to indicate the device that no reset of its settings should be performed. The first phase of UC6 can also be used as backup of a registrar and is time-independent from the second phase.

6. Prototype implementation

We used the Ethereum blockchain for a technical implementation of the prototype with Solidity as developing language for the smart contracts. The use cases have been implemented separately so they can be easily transferred to an infrastructure with multiple devices. In a first step we realised a software prototype with all use cases as single components in a Javascript Node environment with a React frontend. This test environment allowed a step-by-step verification of the described use cases and validation of all sent and received information (see Figure 3).

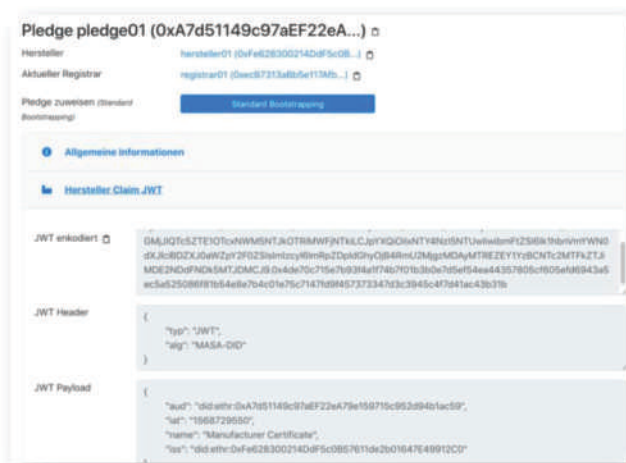


Figure 3: Frontend screenshot of the software prototype.

In a second prototype, we are building a hardware-based system with separate components for device, registrar and MASA-BI. To experiment with different hardware configurations and transmission protocols we use Arduino and Nordic NRF52840.

One of the important aspect of using Ethereum is the cost for transaction and execution of individual steps. If the mainnet of Ethereum would be chosen, the cost of about 4Mio Gwei⁹ per registration would arise. This would result in costs of 2,57 CHF¹⁰ which is too much for an industry usage. Therefore, we suggest the set-up of an own Ethereum¹¹ network run by different manufacturers and organised as association. This would allow the usage of a Proof of Stake consensus mechanism and the independence from highly volatile crypto prices.

7. Strengths and weaknesses of such a system

The proposed system offers a variety of benefits for both manufacturers and customers. These are not only based on the usage of blockchain technology but also on the application of the chosen identity solution using DIDs. Nevertheless, there might also be some drawbacks. We analyzed strengths and weaknesses from a stakeholder perspective. This analysis is without claim to completeness.

7.1. Benefits for the manufacturer

Device inventory

Today most manufacturers have to keep track of their produced devices by an own infrastructure. The first part of our solution (UC1 and UC2) can substitute this with an immutable and distributed ledger offering an audit trail on all devices. Since we designed the system that those use cases could also be separated in an own blockchain infrastructure, any concerns about showing numbers of devices produced can be dispelled. It has to be mentioned that if there is a separation between the identity providing and bootstrapping no further verification about the device origin is possible in DIDInventory during bootstrapping.

MASA-BI ecosystem

Our vision is an open, community-oriented ecosystem for the MASA-BI infrastructure. This community-supported MASA-BI would facilitate an open and transparent market. For start-ups this would also make it easy to participate in a secured device distribution. From this open ecosystem all market participants could benefit. To ensure the open character and to prevent a takeover by one market player, an association or foundation as legal form is suggested.

Security

Device security today is mainly based on certificates from CAs (Certified Authorities). Assaults on those CAs and disclosure of root certificates result in a massive security issue for all devices trusting in those certificates. Self-sovereign identity of devices and the proposed blockchain-based approach reduce this risk significantly.

Proof of origin

Since the devices are registered during manufacturing, a proof of origin and trusted supply chain can be guaranteed. If devices are traded on a secondary market the history of those devices can be retraced. For some environments like critical infrastructures second-hand devices are not allowed. Our approach is a way to detect such misuse. Even if a device is used and not assigned to a registrar, a factory reset can be enforced. In addition, the exact manufacturing date can be reconstructed from the registration time on the MASA-BI.

Firmware update

Finally, the system could be extended to a registration of the registrar at the manufacturer. This identification should be separated from the MASA-BI due to GDPR reasons. A direct link between the manufacturer and the registrar could simplify sending firmware or factory updates regarding the specific device versions. Linking registration to MASA-BI and registration with the manufacturer is one way to increase the registration rate of devices.

7.2. Possible drawbacks for the manufacturer

Transparency about production

In a full extension where device registration at manufacturer site (UC2) and bootstrapping (UC4) are handled by the same permissionless blockchain, it will be possible to draw a conclusion about the number of produced devices. For some manufacturers this might be a problem. The further development using zero-knowledge proofs or permissioned blockchains can eliminate this obstacle. Nevertheless, some manufacturers could be restrained.

Costs

Registration of devices at the MASA-BI is associated with costs. The prototype is using the Ethereum blockchain where Gas has to be paid for writing transactions. On a large scale these costs can sum up to a significant amount, especially with recently rising Gas costs. There are several possibilities to solve this drawback. The infrastructure could be provided by an independent association or the nodes of the blockchain used can be financed by different manufacturers. With this approach of a permissioned blockchain infrastructure a new way of pricing can be implemented.

7.3. Benefits for the customer

Easy registration

The registration process for new devices should be as convenient as possible. The proposed system facilitates this reduction in complexity. Since there is no constraint to follow the registration, the benefits for the customer should nudge him to use the system. This feature is very much dependent on the usability of the registrar software. Therefore, special attention must be paid to this.

Security of device origin and counterfeit discovery

Especially for commercial usage the origin of a device is decisive (see 7.1 – Proof of origin). Due to a transparent tracking, the proposed system allows to detect irregularities in the supply chain. Not only do manufacturers benefit from this, customers benefit as well, as the tracking of devices is possible without involving manufacturers.

Fallback scenario if registrar is changed

To enhance convenience, all situations where a registrar is involved have to be considered. UC6 already addresses these aspects. We are working on further processes to cope with this scenario. Again, usability and security are the main focus.

Keep configuration even if complete system is handed over to another provider.

In an environment where a service provider is responsible for the setup and configuration of a system, a handover to the operator is required. UC6 addresses this handover and raises the convenience level. This is a great opportunity since today installations have to be set up in a new way if a handover happens.

7.4. Possible drawbacks for the customer

Transparency about device ownership

Our proof of concept uses Ethereum as blockchain technology. The open character of this blockchain allows conclusions about the ownership of devices registered. This might be a similar drawback for the manufacturer (see 7.2). Further development in blockchain technology as well as access restriction to data can cope with this drawback.

Need for having a registrar

The implementation of the proposed system requires the usage of a registrar for each installation site. For smaller sites this might be a dissuasive effort. Therefore, it is required that the effort for setting up and operating a registrar is reduced to the minimum. Nevertheless, a customer will only use this kind of system if the benefits mainly and the convenience level are high.

7.5. Summary as SWOT

<p>Strength</p> <ul style="list-style-type: none"> - open ecosystem - security - proof of origin - easy registration 	<p>Weaknesses</p> <ul style="list-style-type: none"> - costs, if public blockchain - registration process needed - registrar needed
<p>Opportunities</p> <ul style="list-style-type: none"> - use as inventory - manage firmware upgrades - easy handover of installation 	<p>Risks</p> <ul style="list-style-type: none"> - transparency over devices

8. Conclusion

We presented a concept for a device registration system based on blockchain technology. This system allows the allocation and management of device identities which are independent of manufacturer-provided systems. Therefore, our proposal of a self-sovereign identity management is immutable and independent of the failure of any single player. The usage of already existing signing technologies in combination with JSON Web Tokens and the concept of DIDs allows a fast and lean implementation. Due to the application of secured hardware the access to the identity can be kept on the device. Just like identity for humans, the identity of things will be an essential feature for future applications.

References:

[1] M. Pritikin, M. Richardson, T. Eckert, M. Bebringer and K. Watson "Bootstrapping Remote Secure Key Infrastructures (BRSKI)" <https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-30> [Accessed March 25, 2020]

[2] T. Weingärtner "Tokenization of physical assets and the impact of IoT and AI." https://www.enblockchainforum.eu/sites/default/files/research-paper/convergence_of_blockchain_ai_and_iiot_academic_2.pdf, 2019, [Accessed March 25, 2020]

[3] X. Zhu and B. Youakim "A Survey on Blockchain-based Identity Management Systems for the Internet of Things." in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018.

[4] P. Koblhaas "Zug ID: Exploring the First Publicly Verified Blockchain Identity" <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702>, 2017 [Accessed March 25, 2020]

[5] A. Third, K. Quick, M. Bachler and J. Domingue "Government services and digital identity" https://www.enblockchainforum.eu/sites/default/files/research-paper/20180801_government_services_and_digital_identity.pdf [Accessed December 30, 2020]

[6] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grand and M. Sabadello "Decentralized Identifiers DID (v1.0)" <https://w3c.github.io/did-core/> [Accessed December 30, 2020]

[7] N. Otto, S. Lee, B. Sletten, D. Burnett, M. Sporny and K. Ebert "Verifiable Credentials Use Cases; W3C Working Group Note 24 September 2019" <https://www.w3.org/TR/vc-use-cases/> [Accessed December 30, 2020]

[8] J. Shane "Welcome to uPortlandia!" <https://medium.com/uport/welcome-to-uportlandia-2302e0d2ceb1> [Accessed December 30, 2020]

[9] L. Lesavre, P. Varin, P. Mell, M. Davidson and J. Shook "A taxonomic approach to understanding emerging blockchain identity management systems". arXiv preprint arXiv:1908.00929 DOI 10.6028/NIST.CSWP.01142020, 2019.

[10] J. G. Faisca and J. Q. Rogado "Decentralized semantic identity" in Proceedings of the 12th International Conference on Semantic Systems, 2016, pp. 177-180.

[11] "Introduction to JSON Web Tokens" <https://jwt.io/introduction/> [Accessed March 25, 2020]

[12] A. Mühle, A. Grüner, T. Gayvoronskaya and C. Meinel "A survey on essential components of a self-sovereign identity". Computer Science Review, 30, 2018, pp. 80-86.

[13] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen and N. Zarin "Self-

sovereign identity solutions: The necessity of blockchain technology". *arXiv preprint arXiv:1904.12816*, 2019.

[14] Q. Stokkink and J. Pouwelse "Deployment of a blockchain-based self-sovereign identity" in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1336-1342.

[15] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan and S. Wang "An identity management system based on blockchain" in 2017 15th Annual Conference on Privacy, Security and Trust (PST), 2017, pp. 44-4409

[16] C. Allen "The Path to Self-Sovereign Identity" <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>, 2016 [Accessed March 25, 2020]

[17] M. Al-Bassam "SCPki: A smart contract-based PKI and identity system" in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017, pp. 35-40.

[18] U. Der, S. Jähnichen and J. Sürmeli "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution". *arXiv preprint arXiv:1712.01767*, 2017.

[19] P. C. Bartolomeu, E. Vieira, S. M. Hosseini and J. Ferreira "Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT" in 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1173-1180

[20] C. Shepherd, G. Arfaoui, I. Gurulian, R. P. Lee, K. Markantonakis, R. N. Akram and E. Conchon "Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems" in 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 168-177

[21] G. Wood "Ethereum: A secure decentralised generalised transaction ledger". *Ethereum project yellow paper*, 151, 2014, 1-32.

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

TW took the lead in conception and writing of this article. OC provided industry inputs, revising and approval for the publication of the content.

Funding:

Publication of this article in an open access journal was funded by the Portland State University Library's Open Access Fund.

Acknowledgements:

The research was funded by Siemens Schweiz AG. The funding was in no respect linked to the use of any kind of technology or methodology. Therefore, the authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

¹ <https://www.merriam-webster.com/dictionary/identity>

² <https://www.uport.me/>

³ <https://sovrin.org/>

⁴ <https://www.hyperledger.org/projects/hyperledger-indy>

⁵ <https://w3c-ccg.github.io/did-method-registry/>

⁶ <https://jwt.io/>

⁷ <https://www.legic.com/>

⁸ <https://www.riddleandcode.com/>

⁹ Using an average Gas price of 55Gwei (23.12.2020)

¹⁰ Ether price of 648 CHF (30.12.2020)

¹¹ E.g Hyperledger Besu or Quorum

Piece of Cake: Assuring Specific Qualities of Product in Farm Lifecycles with DLT – Can Evidenced-Based Practice be supported by Participatory Action Research Methods?

Hannah Rudman
SRUC, Scotland's Rural College, UK

Correspondence: hannah.rudman@sruc.ac.uk

Received: 24 September 2020 **Accepted:** 16 October 2020 **Published:** 27 October 2020

Abstract

A strong need for evidence-based practice in the blockchain and distributed ledger technology (DLT) research, development and action domains is currently clarifying. Literature highlights a lack of transparency around the outputs, outcomes and impacts of blockchain projects. As previously cited in an article of this journal, for example, the US Agency for International Development studied 43 projects and found that nearly all 43 did not want to share their results [1]. The Centre for Evidence-Based Blockchain recently completed a study of 517 companies to see if their blockchain projects could be defined as evidence-based practice. Over four years they measured companies using the PCIO framework (what evidence is there of Problem – Comparison – Intervention and Outcomes) of evidence-based practice. The studies concluded that almost half of the blockchain companies showed 'no explicit evidence of the problem to be solved. Approximately one-third fail[ed] to cite a comparison and intervention analysis, and less than 2% demonstrate[d] evidence of outcomes backed by filtered (critically appraised, peer reviewed) information' (Naqvi & Hussein, p. 8 [2].)

This article presents how qualitative research design and methodologies can help companies and academics achieve evidence-based practice. It presents a case study, in the PCIO framework, of a small-scale agriculture sector project to assure a specific quality. The case study is a conclusion of a project that was run as participatory action research (PAR), involving a consortium including academics, farmer practitioners and a technical DLT platform developer, between 2018 and 2020. The findings show that PAR is an appropriate research method for any democratic collaborative consortia to achieve evidence-based practice through dialogue, discussion, co-development and trusting relationships.

Keywords: *distributed ledger technologies (DLT), participatory action research (PAR), case studies, agri-food supply chains, research and development design, qualitative research methodologies, evidence-based practice.*

JEL Classifications: *O3, L6, and Q1.*

1. Introduction

There are high-profile agri-food sector blockchain case studies from the biggest sector companies working with tech giants such as IBM's Food Trust (its website features seven case studies, with IBM's blockchain solution improving supply chain efficiency, food safety, waste and fraud, brand trust, etc.) [3]. Their purpose is to mainly serve as marketing tools, but the case studies do report evidence of problems solved by the IBM solution. Both regulatory direction and consumer demand are pushing blockchain technology into agri-food supply chains. The U.S. Food and Drug Administration (FDA)'s 2019 initiative The New Era of Smarter Food Safety [4] was built on the 2011 Food Safety Modernization Act (FSMA) by suggesting a modern approach to food traceability. This accelerated a number of blockchain proof-of-concept projects. FoodLogiQ, IBM Food Trust, ripe.io and SAP simulated seafood supply chain data sharing by leveraging GS1 standards, the most widely used supply chain standards in the world. Blockchain technologies in the project facilitated more accountability in the supply chain, through multiple parties across a supply chain supplying data forming an immutable ledger or audit trail of product events and transactions [5]. In August 2020, the U.S. Department of Agriculture said it envisioned distributed ledger technology (DLT) becoming integral to the functioning of complex agricultural supply chains in the future [6].

Chinese consumers became even more interested in transparency during the COVID-19 crisis. In response, the APAC Provenance Council was formed in 2020, including VeChain and Blockchain Australia, again leveraging GS1 standards. By combining resources from all members, the Council aims to provide a comprehensive blockchain-enabled food supply chain finance ecosystem, bridging traceable, safe and trusted trades with shorter billing terms between Australian suppliers and Chinese importers, as well as proving traceability of product [7]. Global-scale hi-tech food supply chain companies are progressing the development of national and international traceability pilot projects with solutions that include blockchain technologies to provide transparency and traceability, as well as improve the speed of tradability [8], [9]. This all builds on Opara's vision from 2002, discussing the future prospects for traceability in the food supply chain, and correctly predicting that access to better hardware and software would eventually enable 'the development of electronic identification (EID) systems, which include electronic tags with chips and handheld scanners for reading, storing and transmitting the data to PCs for analysis and long-term storage' [10].

Food supply chains, whether agri- or aqua- focussed, are conceptually similar, and work as a linear chain of custody of different actors. All food supply chains start with a grower/producer – the producer might be nature itself, or a farmer working with natural resources. Distributors

(hauliers) then take over the chain of custody of the farmed and harvested product when they transport it to food processors, where natural products are then either blended or divided into packaging or combined with other ingredients. The processor sells the end product to retailers who in turn sell to consumers.

Drawing on agriculture and food supply chain literature (e.g. [11], [12]), Parmar and Shah review a number of past and current blockchain projects and suggest a series of issues suffered by each of those actors along the chain that could be improved by the application of blockchain and other technologies (pg. 5926, [13]). Before them in 2015, the Provenance Project recognised the value of consumers and the chain of custody actors in food supply chains by providing them with documentation about a product's origin and journey through the supply chain via a trustable data format in their whitepaper [14].

The paper initially suggested a decentralised application (Dapp) based on the Ethereum blockchain to be the trustable data source. Provenance has since developed a transparency platform and consultancy business, and has worked with the global food brand Princes Group, to provide blockchain tracking and verification for fish and fruit supply chains; with the International Pole and Line Foundation for fish; with Marleybones for pet food; and Bridgehead for coffee (all case studies can be read at provenance.org). Systematic literature reviews of blockchain technology in agriculture mainly discuss the countries where the most activity in the sector is happening – China is the leader with most academic publications about agriculture sector blockchain projects, followed by USA, Italy, India and Spain [15]. The academic literature reveals trends, with research focussed on traceability, security design and blockchain networks as information systems [16]. However, there are far fewer small-scale projects discussed in the literature that focus on the collection of data about what happens to produce on farms, when it is in the chain of custody with the grower/producer. This is just as important as some consumers need to be assured of specific qualities being constantly present in products throughout the entire lifecycle due to health challenges.

This article focusses on a small-scale DLT in agriculture project, showing what evidence there is of Problem – Comparison – Intervention and Outcomes, a framework recognised by Naqvi & Hussein [2] for proving evidence-based practice. The project was a social research involving interdisciplinary collaboration, across a range of disciplinary and organisational boundaries. But what does this mean for research practice? How important is participatory action, connectivity and collaboration in research design? Participatory action research (PAR) is a broad term covering a range of participatory approaches to action-orientated research. It has great practical value in interdisciplinary research practice, common when working with external partners for collaborative project outcomes. PAR involves researchers and participants working together to actively investigate a problematic situation or action in order to change or improve it for good [17]. This article shows that PAR is an approach for academic researchers and external organisations to work together, to co-produce meaningful research designs and practical collaborative project outcomes, as well as prove evidence-based practice.

2. Principles of PAR

The principles of PAR originated over 70 years ago with Lewin and the Tavistock Institute [18]. It is practice-led, rather than practice-based, and contrasts with traditional scientific research where participants are objects of the study. The PAR methodology is structured as a 'cyclical process of fact finding, action, reflection, leading to further inquiry and action for change' (Minkler, p. 191 [19]). The approach includes collective fact-finding, analysis and decision-making involving egalitarian participation by a team, community or organisation to transform some aspects of its situation or structures through action, research and experience (p.1 Reason & Bradbury [20], [21]). As such PAR practitioners attempt to

integrate three aspects: participation (life in society and democracy), action (engagement with experience and history) and research (soundness in thought and the growth of knowledge – Chevalier and Buckles, pp.6–8 [22]) with practical actions seamlessly uniting with research (Chambers, p. 315 [23]) and typically being performed 'with' people and not 'on' or 'for' people (Chevalier and Buckles, p. 5, [24]). PAR provides a genuine co-learning process through which different ways of knowing are valued and integrated and importantly the research process is considered to be as significant as the outcome (Pain and Francis [25]).

The PAR approach typically helps to create actionable knowledge, or interventions, for organisations facing difficulty and change by reflecting on and learning from the organisation's reflections and learning, respectively. It is this idea of meta-learning through the inclusion of academic and practitioner reflection that elevates action research above everyday problem solving [26], [27]. PAR can be particularly effective for multidisciplinary research. PAR approaches focus on enabling full participation of all those involved in the research process [28], and forging partnerships so participants can explore possibilities for transformation together [29]. Although collaboration has become common within the social sciences, there is evidence that multidisciplinary is only now becoming more accepted and understood in the wider academy [30].

PAR is an approach based on a set of core values that follow a broad process, rather than specific methods mapped out in advance. Together, project teams work iteratively to develop the focus of interest, methods and findings, sometimes dividing up tasks according to experience, and always reflecting at each stage. Both the enquiry and decision-making are therefore open and jointly negotiated (see Pain, Kesby and Askins, [31]). This involves the creation of a culture of systematic reflection within the project team. In order to create this culture of reflection it is important to be as open and transparent as possible and to actively include all stakeholders, and the project team, in the research design process. While this might at first appear to be at odds with the usual systematic research process, it has been suggested that it does not fundamentally alter the research method: rather, it places it within a process where it is developed and discussed by a group that has a range of perspectives, knowledge and expertise [32]. This participatory action research consortium involved SRUC – Scotland's Rural College, a collective of farms, and DLT platform software developers working collaboratively to co-create research and action in the form of a proof of concept technology demonstrator.

3. PCIO case study

PROBLEM: This project originated from an enquiry to SRUC – Scotland's Rural College – from a group of farms in the north east of Scotland in 2018. They sought a reliable method of providing traceability, provenance and assurance of the gluten-free oat crop that they grow. Although oats are naturally gluten free, some manufacturers require assurance that they are not contaminated with other grains that may contain gluten. Some consumers need to be assured of specific qualities in food due to health challenges. For example, auto-immune response in people with Coeliac disease or severe gluten allergies (1–2% of most populations) is triggered when consuming more than 10–50 mg. Most health authorities define gluten-free products as containing less than 20 parts per million gluten [33]. Oats are naturally gluten free, but can become contaminated (e.g. by wheat, barley or rye) as they grow and are harvested and stored on the farm, or are processed or transported by food manufacturers. This contamination risk makes them an unreliable food source for Coeliac disease sufferers. Although there is no official gluten-free assurance scheme, the farms have developed their own protocols to ensure that no contamination takes place on the farms, and required a mechanism to provide details and proof of this to the rest of the supply chain. Understanding the capabilities of blockchain technology for agriculture, SRUC held initial meetings with a DLT platform technical development company, to see if the farms' requirements could be met by the DLT platform. As a consortium, we developed a participatory action

research and technical development approach.

INTERVENTION: Funding was secured for a project from The Scottish Government's Rural Payments and Services Department's Knowledge Transfer and Innovation Fund (2019). A DLT platform was used to establish a decentralised private network between the farmers, SRUC (acting as verifiers) and third-party validators to enable them to co-create a persistent digital record through time of data transactions about the oats. All parties in the network stored the decentralised record for resilient information security. The DLT platform also enabled the collaborative building of a shared but permissioned and encrypted digital register, which collected and secured data about the oats' GF status, throughout their growth lifecycle from the different participants. We brainstormed and mapped this process using Visio as a tool to construct a diagram, defining what actor undertook which step, and what digital data were required to prove its validity. Some process steps required sub-steps, where a number of processes would be repeated in the parent step through time (Figure 1).

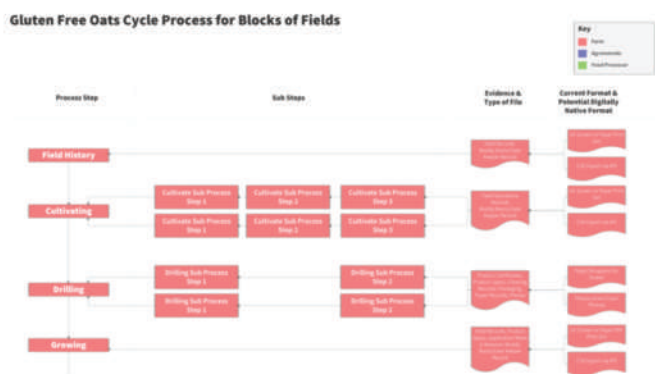


Figure 1: The process mapping of steps and data required as proof in the gluten-free oats cycle.

We then constructed it as a process of steps by actors in the DLT platform's process designer user interface (Figure 2).



Figure 2: The SICCAR DLT platform's process design user interface (see <http://wallet.services>).

The farmers and verifiers in the private network could both read from and write on the register via a controlled process in a programmatically governed way. Each party only had access to write or read the data for which they had explicit permissions. Permissioning was agreed by all the parties via a function in the process designer user interface, and was written as cryptographic rules to the shared register as part of publishing a multi-

party process (Figure 3).

Step name	Field Label	farmer	thirdpartyassurer	verifiers
Field History	Field Record Upload	✓	✓	✓
Field History	Block ID	✓	✓	✓
Field History	Grower Identity	✓	✓	✓

Figure 3: Granular permissioning of each piece of data in SICCAR (see <http://wallet.services>).

Data was only decrypted if a participant is a member of the wallet that the data transaction was sent to (proof of authority is the consensus mechanism the DLT platform uses). Figure 3 shows that the Field Record Upload, the Block ID and the Grower Identity data, all part of the Filed History step in the process, should be decrypted by the Farmer, Third-Party Assurer and the Verifier actors. Access to the actors' wallets is controlled by adding and removing delegates from wallets, and this was managed using each organisation's pre-existing enterprise user authentication and ID management system or directory, and the user management application in the DLT platform. Webforms gave access to all actors in the network through a simple web address, where they could only see actions and data relevant to them, minimising compliance and regulatory obligations. (Figure 4 shows the Farmer's first actions in the shared process, requiring data upload via a webform.)

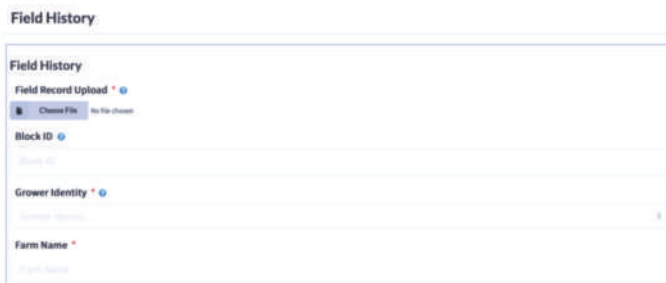


Figure 4: Webform viewable by the Farmer actor, requiring data upload into the DLT platform (see <http://wallet.services>).

Farmers' data had to be validated as being true by the verifiers. Third-party assurers were given access to certain data to audit for certification. Once written on to the register, the data was encrypted so it could not be tampered with. The DLT platform's directed acyclic graph (DAG) architecture model enabled the representation of complex split and combined chains, and for agricultural processes that at points had multiple repetitive steps – Figure 1 shows the requirement for the cultivating step to have a number of sub-steps.

API access to the public data, provided for transparency on the register in unencrypted format, powered a mobile-friendly web app that consumers could access via their phone's camera capturing a QR code to trace and track the gluten-free status of the oats using the data defined as public (Figure 5).

This app was launched by consumers taking pictures of a QR code on the packaging of the oats (Figure 6).

The output of the project was the construction of the secure, private, permissioned DLT network and the publishing of a shared rules-based process on an encrypted distributed register, which was accessible to the

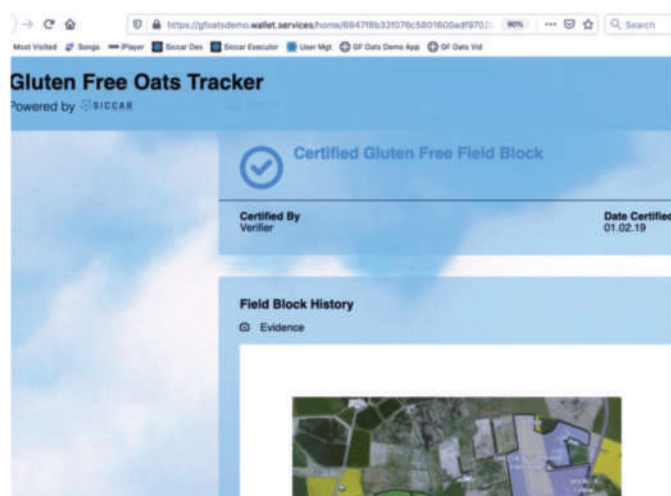


Figure 5: Unencrypted data defined as public, and so viewable to the API, and powering a mobile-friendly web app for consumers to view.



Figure 6: The QR code on the packaging of the oats, which opens the app showing public data, to prove their verified and assured gluten-free status.

consortium members through a user interface of easy-to-access mobile-friendly webforms governed by wallet services. This live and tangible output – a proof of concept (POC) – had a number of outcomes.

OUTCOMES: The project's outcomes, a live, published POC that could be interacted with and demonstrated, proved that the DLT solution enabled and facilitated the provision of transparency to consumers (see Figures 5 and 6, above). Consumers could track provenance, and trace and monitor gluten-free levels of the oats throughout their lifecycle from seed to shop. It also tilted some power in the supply chain back to the farmers, as they were able to evidence the quality of their processes to buyers and food producers for a better price. This builds on the hypothesis that value

distribution becomes fairer with increasing transparency as proposed by Gardner et al [34]. In our case, the DLT solution was an economically fairer sociotechnical development for farmers. The DLT platform developers received a license fee, and SRUC had a live POC, which could be demonstrated to achieve impact in the sector: 100 professionals in the sector experienced demonstrations at the Future Farming workshop in Aberdeenshire on 19 February 2020. There have been another 100 views of the YouTube video demo of the POC [35]. The live and video proof of concept demonstrations, and short online qualitative case study report further attracted the interest of the press and generated stories. In September 2020, there had been one international BBC programme produced that featured the project and its case study [36], one national press story ([37]), two regional press stories ([38], [39]), and four sector press stories ([40], [41], [42], [43]) – significant external coverage, although actual reader numbers cannot be measured from these external sources.

4. Discussion

Knowledge transfer to the agricultural sector was a key impact enabled from publishing the participatory action research project as a PCIO case study, which the press picked up on. Another impact of utilising PAR during the lifecycle of the project meant we were focussed on generating outcomes for all parties' benefits. PAR also demands reflection and evaluation, at the end of cycles, and a summary of learnings within them. For the DLT platform developers, there were learnings that became part of their platform through their agile software development processes: the idea of steps and child steps. This was needed for agricultural processes that had multiple repetitive steps (see Figure 1) and for processes that needed to eventually combine. Halfway through a harvest cycle, adding data to a register, the consortium recognised the need to consider what would happen if a field or harvest failed to be gluten-free due to contamination, therefore requiring the ending of a register (the oats continue into the supply chain for food production, but without the special quality being guaranteed). The design of the register therefore changed at mid-point, and at the end of the harvest, when it was recognised that registers tracking field blocks needed to combine to become the single record for the store.

The learning for SRUC as validators of evidence was that sometimes the best digital evidence would be pictorial and direct from a users' smart device in their pocket on the farm. The metadata of the picture provided the triangulation data proving date and time of pictorial evidence and location of device. The learning for the farmers was that any data they input into the new DLT system ended up being an irritating time-wasting duplication of effort, and that for the system to be an acceptable IT addition, data input would need to be automated from edge devices such as sensors, and that Bring your own Device would need to be strongly authenticated securely into the DLT network.

5. Conclusions and further research

Participatory action, connectivity and collaboration were important in our applied research and development project. The consortium agreed that the PAR project resulted in a proof of concept which proved the technical viability of DLT, and as a case study in the PCIO format, this gained sector and press interest. The need to automate evidence directly from machines – hardwares such as IoT devices and softwares such as sector-specific management systems – as well as from user devices not necessarily in wallets is a technical challenge to overcome next. All hardwares and softwares would need to be strongly authenticated and validated to be acceptable into a secure, private and permissioned DLT network as an actor. The business model was not proven by the project or the PoC, and this would also need to be worked out as part of a more extensive pilot and roll-out.

PAR as an action-focussed cyclical process enabled the consortium's project and fitted with natural cycles of growth and harvest, as well as agile

software development cycles – it presented a very democratic mode of approaching research, learning and the action of technical development.

Multidisciplinary collaboration with external partners enables a type of radical knowledge co-production that can enhance the learning, knowledge and expertise of all those involved, leading to positive research outcomes. Despite the potential benefits of the PAR approach when working with external partners on multidisciplinary collaborative projects, there are a number of organisational barriers to be considered. However, PAR provided the framework to establish research questions, develop methods, conduct collaborative data collection and analysis and produce outputs, but the details of the process must be context-specific. This has meant that to date, PAR and co-production projects occur at a relatively small scale [44]. As agri-food-focussed DLT proof of concept projects and pilots continue and mature, processes will be longer and more complex as different parts of the supply chain join in. The democratic and collaborative nature of bigger, longer-standing DLT networks will find that PAR is an appropriate research method to achieve evidence-based practice and provable outcomes and impact through its focus on dialogue, discussion, co-development and trusting relationships.

References:

- [1] J. Burg, C. Murphy, and J. P. Pétraud, "Blockchain for International Development: Using a Learning Agenda to Address Knowledge Gaps," 29th Nov 2018,
- [2] N. Naqri and M. Hussain, "Evidence-Based Blockchain: Findings from a Global Study of Blockchain Projects and Start-up Companies," *The Journal of the British Blockchain Association*, vol. 3, no. 2, 2020, doi: [https://doi.org/10.31585/jbba-3-2-\(8\)2020](https://doi.org/10.31585/jbba-3-2-(8)2020).
- [3] IBM. "IBM Food Trust case studies." <https://www.ibm.com/uk-en/blockchain/solutions/food-trust> (accessed 14th September 2020).
- [4] (2020). 7 CFR Part 205, National Organic Program; Strengthening Organic Enforcement. [Online] Available: <https://www.govinfo.gov/content/pkg/FR-2020-08-05/pdf/2020-14581.pdf>
- [5] E. Cosgrove. (2020) S-AP, IBM Food Trust, GS1 move toward food supply chain traceability with interoperability test. *Supply Chain Dive*. Available: <https://www.supplychaindive.com/news/gsl-ibm-food-trust-sap-and-more-pass-key-interoperability-milestone-for-579631/> (accessed 13th October 2020).
- [6] A. Hajirnis. (2020) The U.S. Department of Agriculture plans to use blockchain to streamline the EKO food supply chain. *Blocksats*. Available: <https://blocksats.com/the-us-department-of-agriculture-plans-to-use-blockchain-to-streamline-the-eko-food-supply-chain/> (accessed 13th October 2020).
- [7] Blockchain traceability supports brand Australia. [Online] Available: <https://minister.ave.gov.au/littleproud/media-releases/blockchain-traceability> (accessed 13th October 2020).
- [8] Reshma Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," *The Journal of the British Blockchain Association*, vol. 1, no. 1, pp. 1-12, 2018-07-04 2018, doi: [10.31585/jbba-1-1-\(10\)2018](https://doi.org/10.31585/jbba-1-1-(10)2018).
- [9] PTI, "Agriota' e-market platform launched to bridge gap between Indian farmers, UAE food industry," in *The New Indian Express*, 29th August ed, 2020.
- [10] L. Opara, "Traceability in agriculture and food supply chain: A review of basic concepts, technological implications, and future prospects," 2002.
- [11] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giuffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," presented at the *IoT Vertical and Topical Summit on Agriculture*, Tuscany, Italy., 2018.
- [12] A. F. Kamilaris, A. Prenafeta-Boldó, F.X., "The rise of blockchain technology in agriculture and food supply chains," *Trends in Food Science & Technology*, vol. 91, pp. 640-652, 2019, doi: <https://doi.org/10.1016/j.tifs.2019.07.034>.
- [13] M. S. Parmar, P., "Uplifting Blockchain Technology for Data Provenance in Supply Chain," *International Journal of Advanced Science and Technology*, vol. 29, pp. 5922-5938, 2020.
- [14] Project Provenance Ltd. "Whitepaper." <https://www.provenance.org/whitepaper> (accessed 13th October 2020).
- [15] V. S. Yadav and A. R. Singh, "A Systematic Literature Review of Blockchain Technology in Agriculture," 2019.
- [16] O. Bermeo-Almeida, M. Cardenas-Rodríguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas, and W. Bazán-Vera, "Blockchain in Agriculture: A Systematic Literature Review," in *CITIT*, 2018.
- [17] Y. Wadsworth, "What is Participatory Action Research?," *Action Research International*, 1998.
- [18] K. Lewin, "Action Research and Minority Problems," *Journal of Social Issues*, no. November, 1946, doi: <https://doi.org/10.1111/j.1540-4560.1946.tb02295.x>.
- [19] (2000). *Using Participatory Action Research to build Healthy Communities*.
- [20] P. Reason and H. Bradbury, *Handbook of action research*, 2nd ed. London: Sage, 2008.
- [21] D. Coghlan and T. Brannick, *Doing action research in your own organisation*, 3rd ed. London: Sage, 2010.
- [22] J. M. Chevalier and D. J. Buckles, *Participatory action research: Theory and methods for engaged inquiry*. Abingdon: Routledge, 2013.
- [23] R. Chambers, "Chambers, R. (2008) 'PRA, PLA and Pluralism: Practice and Theory.' In *The Sage handbook of action research: Participative inquiry and practice*. Edited by P. H. Bradbury/Reason. Sage.," in *PRA, PLA and Pluralism: Practice and Theory*. ' In *The Sage handbook of action research: Participative inquiry and practice*, H. Bradbury and P. Reason Eds.: Sage, 2008.
- [24] J. M. Chevalier and D. J. Buckles, *A Guide to Collaborative Inquiry and Social Engagement* . 2nd ed. New Delhi: Sage.
- [25] R. Pain and P. Francis, "Reflections on Participatory Research," *Area*, vol. 35, no. 1, pp. 46-54, 2003.
- [26] D. Schon, *The reflective practitioner: How professionals think in action*. New York: Basic Books, 1983.
- [27] C. Argyris, "Actionable Knowledge," in *The Oxford handbook of organization theory*, T. C. Knudsen Tsoukas Ed. Oxford: OUP 2003, pp. 423–52.
- [28] R. Shura, R. A. Siders, and D. Dannefer, "Culture change in long-term care: Participatory action research and the role of the resident," *The Gerontologist*, vol. 51, no. 2, pp. 212-25., 2011, doi: [10.1093/geront/gnq099](https://doi.org/10.1093/geront/gnq099)
- [29] W. Frisby, C. J. Reid, and S. Millar, "Putting "Participatory" Into Participatory Forms of Action Research," *Journal of Sport Management*, vol. 19, p. *Journal of Sport Management*, 2005.
- [30] H. Lee, "Uncovering The Multidisciplinary Nature Of Technology Management: Journal Citation Network Analysis," *Scientometrics*, vol. 102, no. 1, pp. 51-75, 2015.
- [31] R. Pain, M. Kesby, and K. Askens, "Geographies of impact: Power, participation and potential," *Area*, vol. 43, no. 2, pp. 183-188, 2011.
- [32] S. N. Lane, N. Odoni, C. Landström, S. J. Whatmore, N. Ward, and S. Bradley, "Doing flood risk science differently: An experiment in radical scientific method," *Transactions of the Institute of British Geographers*, vol. 36, no. 1, pp. 15-36, 2011.
- [33] I. S. Cohen, A. S. Day, and R. Shaoul, "Gluten in Celiac Disease—More or Less?," (in eng), *Rambam Maimonides Med J*, vol. 10, no. 1, 2019, doi: [10.5041/rmmj.10360](https://doi.org/10.5041/rmmj.10360).
- [34] T. A. Gardner and E. al., "Transparency and sustainability in global commodity supply chains," *World Development*, vol. 121, 2019, doi: <https://doi.org/10.1016/j.worlddev.2018.05.025>.
- [35] *Wallet.Services, Demo: Gluten Free Oats assured by SICCAR Smart Registers*. Available: <https://youtu.be/LpPdD0yxFa0> (accessed 13th October 2020).
- [36] BBC Radio 4, "Oats and Blockchain," in *Farming Today*, 18th August ed: BBC (International), 2020.
- [37] G. Davidson, "Scots farmers pioneer digital 'gluten-free' assurance chain," 11th September ed: *The Herald*, 2019.
- [38] G. Mackenzie, "Simple scan on way to ensure oat provenance," in *The Press and Journal*, September 4th ed, 2019.
- [39] G. Mackenzie, "Technology to trace oats provenance a step closer," in *The Courier*, 4th September ed, 2020.
- [40] V. Bamford. (2020) Gluten-free oat supply chain developed using blockchain technology. *British Baker*. Available: <https://bakeryinfo.co.uk/ingredients/scottish-farms-develop-gluten-free-oat-supply-chain/647481.article> (accessed 13th October 2020).
- [41] G. Davidson, "Scottish growers aim to guarantee gluten-free oats," *The Scottish Farmer*, 19th August 2020.
- [42] F. U. Team. (2020) Six farmers develop Scotland's first gluten free oat supply chain. *Farming UK*. Available: https://www.farminguk.com/news/six-farmers-develop-scotland-s-first-gluten-free-oat-supply-chain_56323.html (accessed 13th October 2020).

[43] G. Selby, "Blockchain boosts food safety and provenance in UK gluten-free oats," *Food Ingredients First (International)*, 24th August 2020,

[44] C. M. Maynard, "How public participation in river management improvements is affected by scale," *Area*, vol. 45, no. 2, pp. 230-238, 2013.

Competing Interests:

HR worked as an employee of the DLT platform provider used during the lifetime of the PAR project, and was a member of the democratic team, collaborating in the PAR process. The PCIO case study was written up, as was this article, once she joined SRUC as an employee in August 2020. SRUC has no special interest in the DLT platform: applied research and development projects across the organisation use a number of different DLT platforms.

Ethical approval:

All actors in the PAR research granted their permission to be mentioned as actors in any public case study.

Author's contribution:

HR designed and coordinated this PAR project, developed the PCIO case study and prepared the manuscript in entirety, with the exception in the acknowledgement below.

Funding:

The PAR project was funded by Scottish Government's Rural Payments and Services Department's Knowledge Transfer and Innovation Fund 2019.

Acknowledgements:

HR would like to thank Dr Claire Bailey-Ross from the University of Portsmouth UK, Dr Jeremy Kendal, Dr Zarja Mursic and Dr Rachel Kendal all from the Durham University UK; Andy Lloyd of the Centre for Life, Newcastle-upon-Tyne; and Bethan Ross of the Science Museum, London for the work on various PAR focussed papers which contributed to the Principles of the PAR section of this article. HR would also like to thank Wallet Services for agreeing to share the DLT platform's images in the figures.

ITO: The Sponsored Token Technology

¹Tianqi Cai, ^{1,2,3}H. J. Cai, ^{4,5,6}David Kuo Chuen Lee, ⁷Dong Yang, ²Kai Wang

¹Zall Research Institute of Smart Commerce, Wuhan, China

²School of Computer Science, Wuhan University, China

³Zallchain Technology Pte. Ltd., Singapore

⁴Singapore University of Social Sciences, Singapore

⁵Shanghai University of Finance and Economics

⁶National University of Singapore

⁷Renmin University of China, Beijing, China

Correspondence: davidkuochuenlee@gmail.com

Received: 06 September 2020 **Accepted:** 13 November 2020 **Published:** 24 November 2020

Abstract

Blockchain technology can be made more efficient with an incentive mechanism using tokens. This article proposes an innovative method of initial token offerings (ITO), allowing issuers such as the government to sponsor and implement policy targeted at specific products, projects or technology. Sponsor's qualifications can gradually be relaxed and guided by a pre-determined process. With a combination of call auctioning and commanding price (CP) determination, the initial issue price is fixed by the sponsor and ultimately by the consensus of all stakeholders. This approach ensures that the initial token price is non-zero at launch and leaves room for revaluation in line with subsequent development of the project or technology. ITO can attract more enterprises, teams and individuals to participate in the innovation activities of critical projects or technological breakthroughs by reducing their economic costs and risks, thus accelerating project collaboration. It also combines a conducive regulatory environment and market forces to achieve flexibility and effective management of technological innovations.

Keywords: *token; commanding; issue price; circulation*

JEL Classifications: *G18, G28, G38, K22, K23, O16, O38*

1. Introduction

Over the past few decades, financial innovations such as stocks, bonds, real estates and complex instruments have generated good market returns for investors. But the continual artificial economic growth via the issuing of debts through quantitative easing will not last forever [1]. Digital currencies have the potential to become a new form of value carrier or even the new type of default currency, going beyond the current definition of money and extending the concept of value through tokenisation [2–4]. Today, initial public offerings are an essential way to raise funds for traditional companies. But with digital currencies, more innovative ideas have been adopted. Whether these recent innovations will sufficiently meet the needs of the future monetary system is still debatable [5–11].

An Initial Public Offering (IPO) is an act of offering the stock of a company on a public stock exchange for the first time, a method regulated by most state securities and exchange administrations. With the advent of Bitcoin (BTC) and the beginning of the token economy, four notable financing methods have emerged in the blockchain world. Initial Coin or Crypto-Token Offerings (ICO) [12] refers to the initial issuance of tokens by blockchain projects to the public in exchange for cryptocurrencies such as BTC, Ethereum (ETH) or others with liquidity for the project operations. Initial Fork Offerings (IFO) refers to the issue of new tokens generated by forking mainstream cryptocurrencies such as Bitcoin. Initial Miner Offerings (IMO) refers to the issuing of tokens in exchange for mining machines or related hardware equipment. Initial Exchange Offerings (IEO) refers to issuing tokens that will be listed directly on the cryptocurrency exchange [13–16].

The sole purpose of these four fundraising methods is to raise capital from investors. There is no circuit breaker in the round-the-clock trading of digital currency on crypto exchanges. The lack of regulation has little consumer protection, and investors may risk losing the entire amount of investments¹ [17, 18].

There are also enormous compliance and capital risks in ICOs and IEOs. While Security Token Offering (STO) meets regulatory conditions in some jurisdictions, there is a long time lag in actual offering and listing as there are many regulatory hurdles. A time period of up to six months' lag to settle simple legal issues is not unusual. Long audit period is also a pain point for these time-sensitive blockchain projects. Unable to meet the urgent need of capital, STO has little advantage over IPO [19–27].

The core value of blockchain technology comprises the proof of existence and a token [28]. The former refers to maintaining immutable records and is an essential feature for blockchain. The latter is subject to increasing scrutiny by most regulators. A token mechanism is especially vital to incentivise connection and collaboration. A blockchain without token commands a lower valuation [29–31].

The choice of a valuation model is an issue, as is the risk. In an IPO, one or a combination of valuation methods such as time-adjusted returns and market comparison can be used for price-fixing. In book-building before IPO², the price may be based on cumulative bidding, fixed price, auctioning or other established methods. After listing, market makers³ are allowed to provide bid-ask within the maximum spread to provide liquidity and price stability. However, in an ICO, the issue price is mostly decided unilaterally

and predominantly by the issuer. There was also the use of discriminatory and uniform pricing methods for some projects. Meanwhile, some official policies have been released lately⁴, and their effectiveness remains to be seen. Generally, there are insufficient regulations on market-making that provide market stability and liquidity [32-35].

2. Tokens as a Core Value of Blockchain Technology

Cognition is fundamental to Commanding Price (CP) mechanism. The mental action or process of acquiring knowledge and understanding through thought, experience and the senses is key to commanding price formation (CPF). CPF is observed in the pricing of new inventions, valuation of start-ups and emerging museum art pieces, and intention may be at the core of commanding pricing. The initial pricing decision is linked to the intent, and in the case of the low price of a ticket to a museum, the government's intention is to promote high visitations. The core of CPF is its linkage to a purpose and may create other consequences such as an arbitrage opportunity. The risk and responsibility of balancing the conflicting interests, in this case, arbitrage opportunities and promotion of education welfare for the visitors, need to be balanced by the central planning authority. Very often, the inability to balance these competing interests of commanding pricing may lead to public resistance as there is an inherent risk of distortion of free-market structure that eventually breeds monopolies.

Hayek believed that the principle of self-organisation of the market economy was a significant contribution of classical economics and opposed any form of economic planning. Hayek argued that even the right to issue money should be returned to private banks without a monopoly from the administration. The theory of liberalism and non-government interference in economic activities and the idea of fiscal revenue based on the principle of fiscal balance have dominated the capitalist world for more than a century. From Hayek's point of view, the primary role of the state should be to maintain the rule of law and to avoid involvement in other areas as far as possible [36, 37].

After entering the period of monopoly capitalism, the contradiction between the social nature of production and the private possession of the means of production became increasingly prominent, and the period of early 1930s saw the break out of the world economic crisis. Keynes believed that the doctrine of achieving balanced employment through the automatic market regulation mechanism had been falsified. He actively advocated state intervention in economic activities, making fiscal revenue an essential tool for stimulating effective demand, that is, consumption demand and investment demand, and strengthening macroeconomic management. The main conclusion of Keynesian economic theory is that there lacks an automatic mechanism that is powerful enough for production and employment to move towards full employment in the economy [38]. Keynes proposed the Bancor plan in 1944 at the United Nations Monetary and Financial Conference in Bretton Woods, New Hampshire, which eventually became aborted following with the White Plan proposed by the United States. In Keynes's monetary scheme, there should be a unified world currency, i.e. Bancor Coin, by the International Clearing Union. The allocation of money would be calculated based on the average value of import and export trade in the three years before World War II. The Bancor agreement can be considered as a form of the commanding pricing method. [39]

Hayek argued that free-price mechanisms were not designed deliberately in advance. But these mechanisms were led by spontaneous social order or by human behaviours rather than human designs. Effective exchange and use of resources could only be maintained through price mechanisms in the free market. [40]

The applications of commanding price mechanism are seen often in the practice of finance. There are notable examples such as the linked exchange rate⁵ and the Secured Overnight Financing Rate (SOFR)⁶, perceived as the

issuance with official endorsement and sponsorship. According to the value theory of consensus⁷, value is derived from consensus. In a future-oriented monetary system, no matter how a specific pricing method is implemented, the only way to generate value is to reach a consensus on price within a specific range. Government-commanded token prices are similar to the national price-stabilised commodity prices. The idea of price stability in China has had a long history [41].⁸

Digital currency is a possible new form of wealth in the future. If there is an absence of a commanding or sponsoring party, there will possibly be a repetition of history, which saw many digital currencies having a breakout in price and subsequently going to zero. Moreover, if the government-sponsored issuance does not provide enough resources to attract users to reach a consensus, the digital currency system is unsustainable. For instance, some Latin American countries continuously printed money without a broad consensus among the public, which saw the sovereign money depreciating sharply.

Therefore, the pricing method for the future business systems should be a balancing mechanism between the commanding and multi-party participation, with both the guidance of the nation's will at the macro level and the flexibility of market forces, in order to find an entry point of the combination of the planned economy and the free market. In the early stage of project development, the commander (price fixer) or sponsor takes on the responsibility of endorsement and backstop to attract participants. With the organic growth and increase in participation, the commander can gradually exit, and the pricing will be determined by the consensus reached by the growing number of participants. The corresponding token price fluctuation will be volatile and should be issued in a limited price range to reach consensus gradually. A commanding mechanism with multiple participants is more likely to use blockchain to accelerate the process of reaching consensus among stakeholders. The future economic activities will include more pricings on these specific contents in different price ranges to make the valuations of innovations quicker and more reflective of the market forces.

3. ITO 1.0: A Token Technology Sponsored by the Government

Although many governments have yet to allow ICOs, the government itself is suited to use the token technology to effect macroscopic control in a consortium blockchain scenario. We refer to the initial token offerings sponsored by governments as ITO 1.0, which can be regarded as an extension of the contemporary tangible standardised futures market, such as that in grain or steel, to a more abstract and intangible non-standardised product market. By adopting the token technology, the government can provide precise and rapid resource subsidies for key products, technologies and services intended to support and guide technological innovations in a directional way.

From the perspective of macro-control, especially in dealing with time-sensitive emergencies, the government should use token technology to provide accurate, fast and effective resource-allocation channels for key issues that require various types of support. The most direct application scenario is the distribution of government subsidies. The government can participate in a consortium chain and allow the positive effects of tokens to be fully realised. In a contemporary public chain, the token price corresponds to the future value instead of the present value. The former is more difficult to determine. Public chain's token prices evolve similarly to a rollercoaster ride – when good news emerges, prices may seemingly irrationally rise ten-fold or even one hundred-fold [42], and they may subsequently drop drastically by more than 90% [43]. These fluctuations leave many without the confidence to invest, exerting unnecessary pressures on the project team and thus the morale. However, with the government's involvement, this shortcoming can be corrected to a certain extent. For example, government subsidies or industry guidance funds can be used to establish the fundamental token value, and resources can be

distributed within companies by giving tokens. The support fund is linked to the future earnings of the target industry. One of the possible ways of linking is that the government making equity investment with the tokens in the enterprise or team according to the information of the industry, enterprise or team size and support intensity and so on, so as to integrate the support fund into the industry in the form of tokens. The government investment should not focus on the capital but should instead be made in hopes of supporting the industry and the environment needed for its success. As a result, the project's value would not decrease to zero at the initial stages and instead would have substantial upside potential.

Government subsidies and industry guidance funds already exist and have come under much criticism. From the perspective of liberal economics, they are considered the method of a planned economy, which is inefficient and has the possibility of policy arbitration, etc. Despite how these criticisms make sense, there seem to be no better solution, until now. With the advancements of blockchain technology, it serves to be the better solution. For example, China now wants to encourage the development of a new energy-based vehicle industry. While clean energy is the future goal, market guidance alone is not sufficient as the domestic technology does not have a clear competitive advantage.

Furthermore, a large amount of funding would be required for the manufacturers' initial capital. Reaching profitability will likely take years, and government investments can serve to be very helpful when emerging enterprises experience such difficulties. The current practice is that the government will provide subsidies for all new domestic energy-based vehicles so that the subsidy amount will directly reduce the price and hence, consumers will be able to buy vehicles at low prices. Consequently, numerous previously unknown electric car brands have suddenly emerged while prices have risen to unjustifiably high levels without a match in quality, demonstrating a deceptive effect of subsidies on the car market. From the government's point of view, this problem is challenging to solve. Having to decide both on the item and amount of subsidy means that many background operating aspects remain subject to manipulation. Even if the government stipulates numerous rules to apply to indicators, there will still be artificially manipulated results of the corresponding indicators that lead to cheating and underhanded actions.

If the government wants to provide targeted support, instead of cars, perhaps it should subsidise critical technologies that can be implemented with the token technology. In the electric car industry, battery technology and electric-kinetic conversion are two key technologies. The government can issue two kinds of tokens, such as Token A for the battery field, which can be used for battery trading, and Token B for electricity-related uses, which can be used to buy and sell electric engines. Token A will be given to businesses that can only purchase battery equipment so that the respective tokens will always remain inside the ecosystem. Besides, the company can continue to hold Token A, with the expectation that the token price would rise in the future. As the industry develops and battery technology becomes more advanced, and as the total quantity of Token A is limited (e.g. 10 million), then one unit of Token A will become more valuable in the future than at present. This means that if the battery industry develops, Token A will continue to appreciate. This is likewise for the mechanism of Token B to the engine field. The interesting feature of the two tokens is that they provide more targeted rewards to different businesses and technologies, and allow a flexible approach with a higher tolerance to the varying development speeds.

By introducing the blockchain technology, the industry-led fund model can achieve specifically targeted subsidies.

The first aspect is the use of tokens under the guidance of authoritative institutions. Subsidising key technologies to be innovated or optimised for upgrading rather than subsidising products will focus more precisely on industry support. Government subsidies and industry guidance funds can

be used as a basis value; subsequently, tokens, instead of currency would be issued to keep the funds circulating in the ecosystem, which will help achieve the vision of supporting the industry and establishing a healthy ecosystem. This approach is relatively fair towards companies. With government start-up funds, small-scale companies can also participate in the industry, and as long as they can solve the fundamental problems, they will gain profits by selling qualified technology and products. If the government holds a portion of the tokens, and as the market develops, the tokens will rise further, and their future value is likely to exceed the initial value.

The second aspect is the targeted industry incentives by issuing tokens with basic prices. Tokens can be used to implement more detailed and precise incentives, channel funds into the cutting-edge fields, thereby spurring innovation. More specifically, it is possible that developing a certain process can affect the entire ecosystem and industry both upstream and downstream, and smaller-scale companies can focus their resources on solving key problems to increase their competitiveness in the market.

The third aspect is that tokens can produce more value when combined with the market. The tokens in the ecosystem are traceable, and an increase in circulation of tokens produces more value than a one-time trade of the traditional fund subsidy. Circulation also involves the market forces and the government only needs to ensure that a macro regulatory system is in place. It can be said that the government can both lead and let go. The system can have central regulation, distributed liquidity advantages together with the perfect combination of a planned economy and a free market. Therefore, we believe that the adoption of token-based blockchain technology is an appropriate solution.

In addition to the guidance and management of internal innovation, ITO can also be applied to the overseas expansion of Digital Currency Electronic Payment (DC/EP). According to the publications and speeches by YAO Qian, MU Changchun and other researchers from the central bank, China's DC/EP have basically completed the top-level design, standard formulation, functional development and joint adjustment test. Under the principles of stability, security and controllability, China's DC/EP has been started in four pilot cities, namely Shenzhen, Xiongan, Chengdu and Suzhou, for the internal test. The first batch of pilot institutions includes four state-owned banks and three major operators. The pilot scenarios include transportation, education, medical treatment and consumption, and more optimised DC/EP functions will come out to proceed with a legal tender in the digital form for application prudently. The domestic Ren Min Bi (RMB) digital currency should emphasise the stability, and the internationalisation of RMB needs to consider the growth aspect. By adopting ITO, at the initial phase of the issuance, overseas digital currencies can be related to the domestic RMB by providing a base price. Hence after, foreign-based digital currencies will depend on participants and market forces to achieve its circulation value. As China's international status ascends, RMB will appreciate, matching its offshore development and its organic growth process.

4. Possible Risks and Coping Strategies of ITO 1.0

Many countries still forbid token issuance because of the potential risks and unclear countermeasures. [44]

One concern is moral hazard. At present, the objective of government-led funding in the non-public investment field is to foster companies. At the same time, funding in the public investment field also means the government is endorsing the project's background and authenticity, which would attract more investors. Without additional implications, the worst-case scenario is government being held responsible for mistakes in investment decision-making. However, the existence of additional implications could change the role of the government from that of a referee to that of a participant, and even potentially make them jointly liable for

being the party that is providing false statements to project participants and deceiving public investors. There is no doubt that the relevant individuals who make decisions and provide information will face a significant moral hazard. In the stock market, there are many cases of local governments being involved in public companies' fraud, and these serve as cautionary tales. Specific measures that include setting up regulatory authorities and giving exchanges significant administrative powers are also implemented to balance the market.

The second concern is the dilemma caused by information asymmetry. The asset-side or project teams has a natural advantage of information asymmetry. Should there be no legal provisions for information disclosure, the advantage will certainly be significantly tilted towards the asset-side. From the point of view of objective information disclosure, blockchain and the Internet of Things are suitable for objective information disclosure of production indicators. However, detailed granular information disclosure is difficult to implement for financial and business operating indicators, as it can lead to a complete loss of an enterprise's privacy. However, if financial and business operating indicators are not disclosed, the information asymmetry problem faced by capital providers cannot be solved. The crowdfunding mechanism established by the United States JOBS Act may provide a way out by advocating a cap on funds, a cap on financing on the asset side, and an exemption from certain disclosure obligations. However, in the context of blockchain and tokens, significant innovations are still required to apply the blockchain technology.

It can be expected that ITO 1.0 will encounter those two challenges during implementation. In this regard, the government only endorses and leads in the early stage of the cold start of a project, and then transitions to using the market mechanisms to distance itself appropriately. The private information of companies is stored in the blockchain over time but is not disclosed synchronously. Instead, disclosure is performed step-by-step according to time period or milestones achieved so that the demands of both privacy and regulation can be satisfied.

The government does have an endorsement role in the cold start of ITO 1.0, using fiat currency funds and their credibility to stimulate the technical direction or fields they intend to support to attract teams with qualified technical expertise. However, this endorsement is not long term and is limited to solving the cold-start problem only. Instead of a long project cycle in the stock market, the project cycle in ITO 1.0 is much shorter, which can reduce the fund risk to some extent. Of course, a project may evolve in two ways. If the project is unsustainable, participants will not be optimistic about the future and will sell the tokens to withdraw from the project. Hence, the token price will fall and the government will ultimately be able to buy the tokens at a low price, and all participants will quickly exit. Alternatively, if participants are optimistic about the project and are willing to obtain more tokens at high prices with the expectations of higher revenue in the future, the government only needs to develop macro-regulatory principles on the premise of allowing participants to liberalise the market instead of continually endorsing the entire project. The government's endorsement is not a one-time event, i.e., tokens can be issued and released gradually to balance the market's supply and demand, and can also stop losses in time for the case of unsustainable projects.

ITO 1.0 reduces the likelihood of corporate policy arbitrage. For listed enterprises, there is a possibility of collusion, but in the ITO mechanism, participants are not a single subject but rather multiple subjects with a horizontally competitive relationship. The supporting rules are no longer aimed at enterprises but instead target key technologies or key links. In the interaction of government and participants, the cost of arbitrage increases and supervision from competitors increases as well.

Alternatively, consider the battery technology of new energy vehicles as an example. Since the government will regard battery technology as the key point, the subsidy will target only the participants that are closely related

to the link. If a company colludes upstream and downstream and forges battery data on the chain to try to obtain more tokens, other companies in the battery sector will be able to expose such a fraud, and the government can monitor the audit checks.

To deal with the difficulty of information asymmetry, a possible solution based on the blockchain technology entails one-time storage and multiple disclosures. Sensitive financial data will still be stored in a timely manner. But in order to maintain the basic standards of privacy, only non-sensitive data will be disclosed at that time. Depending on the sensitivity of the data, disclosure of detailed granular data can be further delayed for a period, such as a week, a month, a quarter or a year gradually, or the data can be disclosed as required by a project milestone. In other words, data cannot be tampered with from the beginning as it has been recorded as a trusted block, and yet disclosure can be deferred to provide a basis for subsequent audits while protecting privacy. The verifiable random functions (VRFs) can also be used to validate some data that is not fully disclosed.

As a new financing method, ITO will be confronted with many challenges. The design and implementation need improvements. If its dynamic mechanism together with flexibility is properly applied, it will play a significant part in future investments.

5. ITO 2.0 and ITO 3.0

ITO 2.0 refers to a version of ITO that allows companies or organisations to sponsor token issuance, and ITO 3.0 further allows qualified individuals to sponsor and issue tokens. The evolution from ITO sponsored by the government to ITO sponsored by enterprises, organisations or teams and finally, to ITO sponsored by individuals, is a gradual process from ITO 1.0 to ITO 3.0. Sponsors can encourage products or technologies they want to support, and participants form a healthy ecosystem within different limited domains. The pricing method of tokens is related to the cognitive level within those domains; in other words, the value is derived from a consensus.

There are two main pricing mechanisms for ITO 2.0. The first, bargaining, is the pricing method involving the two sides of the peer-to-peer pricing. It is not only because of the relative reciprocity that both sides have expectations of the final completion of this pricing, but also because of the recognition of the other's expectations and hence the greater expectations of profit. The whole process of bargaining is the process of constantly testing each other's cognition, which only involves a few participants because the subject matter is clear, as is the goal. The second mechanism, negotiation, is multilevel and more common. Because of the existence of a cognitive asymmetry, negotiation is possible. A so-called mismatched price is normal. A transaction can be concluded because the value reference systems used by both parties for the current price may be different in terms of the value generated by the transaction, such as subjectively believing that other aspects of the transaction can compensate for a disadvantageous price, or because of different expectations arising from the negotiation as to the future value.

Auctioning is a pricing method in ITO 3.0 that is followed by greater acceptance, and the consensus can be reached in a slightly larger domain. The essence of auctioning is holding the opinion that the current price does not reflect the real value. Participants are willing to buy at a higher or lower price, and a stock transaction essentially entails auctioning. In the token market, auctioning is also the main way for traders to reach a consensus. The value arises from a consensus, which is based on the trader's cognitive level. A person's measure of value is subjective, and the fair value of an item within an organisation can be regarded as an extension of the organisation's consciousness and cognition. This also means that different people have different reference criterion that may even be entirely subjective. The price movements arise from the evolution of cognition. In the early stages of cognition, or the early stage of formation of a commanding price, the

room for negotiation is plentiful, but time is relatively limited. It is only if all conditions and game information are transparent and sufficient that price formation can gradually continue, approaching the necessary labour time. As the degree of consensus deepens, the convergence trend towards the value and price of the token remains valid.

Through ITO 2.0, organisations can attract talent to participate in the research and development of key products or technologies and attract investors to support the project. This would help the organisation enhance innovation capabilities and provide new financing channels. Companies can invest in key technologies for other organisations to quickly achieve a multidimensional strategic layout as well. IEO can be regarded as a form of ITO 2.0 with issuers that are qualified exchanges that provide real resources as an initial price to sponsor the project or technical innovation.

Through ITO 3.0, individuals can invest personally in the direction of interest to them. ITO 3.0 can also attract external investment, helping to gather resources to solve key technological problems or develop target products. Accordingly, those with a more robust learning ability and a higher cognitive level will be more likely to access resources and make breakthroughs in their field of expertise, which is also a way of developing a knowledge-based economy. ICO can be considered as a form of ITO 3.0 with qualified individuals providing resources to sponsor the project or technology.

The transition from ITO 1.0 to 3.0 must be organised; otherwise, there will be adverse phenomena, disrupting the financial market. The technology innovation must first be sponsored at the government level with the practical implementation of the mechanism being validated and optimised. Afterwards, an appropriate policy will allow organisations to issue tokens, and finally enable individuals to participate as sponsors. Starting with the government-sponsored ITO 1.0, the actual participants comprise businesses, organisations and capable individuals who are willing to believe in and contribute to the project through the government's endorsement. Regardless of the version of ITO, the underlying consensus value theory still applies, i.e., the value arises from the relevant participants reaching consensus as to the same entity. Afterwards, the tokens as a carrier of such consensus can circulate in communities and represent economic value.

6. Combining Call Auctioning and the Commanding Pricing Method

Compared to blockchain systems with token mechanisms, systems without tokens are limited in data storage and sharing, which will restrict their potential. ITO can be applied in the consortium blockchain first, which requires an incentive mechanism as well. In a consortium chain that integrates human and computer intelligence, nodes cannot fully foresee the future and prepare thoroughly. Hence a dynamic evolution that is supported by the incentive mechanism is needed. The corresponding participants must continuously adapt and improve their cognitive level, allowing tokens to be circulated continuously to create value.

The pricing method of ITO is a composite method that combines call auctioning with the commanding price, which is depicted in Figures 1 and 2, and users are only allowed to participate in ITO with an agreement on the pricing method. Pricing can be implemented and performed in the form of smart contracts in which the rules are specified clearly, and the nodes involved in an ITO are required to authenticate themselves to take further actions. The pricing process can be divided into the four steps described below.

Step One. In this step, the sponsor plays a significant role during the transactions. The sponsor holds the collateral assets as a reserve according to the number and price of issued tokens to determine the token's initial reserve rate. The sponsor is also responsible for fulfilling users' transaction needs. If any user's purchase or sale orders are more than the size that can be fully matched with other users' orders, the sponsor is required to trade

with users. The sponsor's role is distinct from the operation of traditional exchanges.

Step Two. The latest token price is determined by call auctioning among all nodes involved in circulation, which further sets the closing price of each transaction within the call auctioning period.

Step Three. Under certain conditions, such as when token prices calculated by call auctioning is very different from the recommended market price calculated according to liquidity, the sponsor is authorised to establish a commanding price. It can be realised by adjusting the reserve rate, and the commanding price will serve as the starting price in the next round of call auctioning. The range or rule of the commanding price can be specified in the smart contract in advance.

Step Four. In this step, each transaction is confirmed accordingly to a tamper-proof valid order record. The confirmation is a 4-step process as follows.

In step one, the initial reserve ratio *W* is determined by the formula (1), where Balance is the total amount of funds committed by the sponsor, and Token Total Value is the product of the total token issuance and the price at issue. The value of *W* ranges between 0 and 1; the total amount of adjustable collateral funds usually does not exceed double the collateral funds of issuance, and those amounts can be regulated in the smart contract in accordance with the actual circumstances of the project.

$$W = \frac{Balance}{Token\ Total\ Value}$$

Formula 1: Initial Reserve Ratio W

In step two, auctions in ITO are significantly longer than the general stock market short-term call auctions and may last up to 30 days. During a round, users can allocate orders before the deadline is reached. The system will then confirm the latest token price based on the data with the largest number of valid matching orders.

In step three, based on the orders placed during the period, a proposed market price is obtained using formula (2). If the price is significantly different from the latest deal price obtained in step two, or if the sponsor considers the difference from the expected price to be large, the commanding price may replace the price generated by step two and become the new token price and the starting price for the next round of the call auctioning cycle.

$$TokenPrice = \frac{Balance}{TokenSupply * W}$$

Formula 2: Token Price

In step four, the issue price is used as the starting point in the first round, while the token price generated in step two or step three is used as the ending price. Applying the linear or exponential interpolation rules, the transaction price is calculated for each day during the period. Lastly, backtracking is performed, and the valid orders are confirmed based on their dates.

Table 1 simulates the intervention of the commanding price and its effect. If the price becomes unacceptably low, the sponsor will reduce the reserve rate. If it is overpriced, the reserve rate will be raised. The specific mode of regulation is determined by the smart contract. In Table 1, based on the commanding reserve rate, the amount of reserves is adjusted, and the relevant token price can be calculated. A commanding price can also be set based on the issue price and price movements of the previous period, and changes in reserve rates and adjustments in funds are obtained. Smart

contracts can regulate the ranges of commanding price.

The difference between ITO and other pricing methods is that due to the combination of the two pricing mechanisms, the price clearly reflects the respective attitudes of participants and sponsors towards the project. This provides sponsors with a way to contain bubbles or exit projects.

If participants are not optimistic about the project, they will choose to sell the tokens to cash out and exit the market as soon as possible, resulting in a decrease in the token price. At this time, if the sponsor chooses to intervene and make adjustments to raise the price, it signifies that the sponsor is willing to continue to support the project. However, if the sponsor intervenes and lowers the price further, it signifies that the project has failed, and the sponsor is willing to suspend or terminate the project. In another case, if the participants are optimistic about the project, there will be more purchase orders, and the token price will continue to rise. In this scenario, if the sponsor raises the price, it indicates that the sponsor has a positive attitude towards the project and will increase support. The sponsor can also choose not to intervene in price formation and exit the market smoothly; however, if the price is reduced by an adjustment, it shows that the sponsor holds the opinion that the price is inflated and the bubble needs to be contained.

Algorithm: The Combination of Call auctioning and Commanding Pricing Method in ITO

```

Input token, token_issuePrice, token_presentPrice, section_days,
all_transactions, W, balance, tokenSupply

// Calculate the call auctioning price.
find auctionPrice in all_transactions which with most matchmaking
tokens
if auctionPrice.length > 1 then // More than one price with same most
token amounts
    auctionPrice = average value of price //calculate the average of those
    prices
end if

// Decide to use commanding price or not. Confirm token's present
price.
new suggestPrice = balance / (tokenSupply * W)
// the judgment condition can be modified as appropriate
new delta = (auctionPrice + suggestPrice)/2*token_presentPrice * 100%
- 100%
if delta > 30% || delta < -30% then
    input commandingPrice // or input new W to calculate the
    commandingPrice
    token_presentPrice = commandingPrice
else token_presentPrice = auctionPrice

// Calculate specific price of each transaction.
new deltaAll = (token_presentPrice - token_issuePrice)/section_days
new dayPrice[].length = section_days
for(i=1; i<= section_days; i++)
    dayPrice[i]=token_issuePrice + i* deltaAll
end for
new unconfirmedTXs is null
for(day=1; day<=section_days; day++)
    find day_transactions in all_transactions which is valid and date is day
    day_transactions = day_transactions + unconfirmedTXs
    unconfirmedTXs = null
    for each tx in day_transactions do
        if tx is buying and tx.price > dayPrice[day] then
            tx is confirmed at tx.price
        end if
        else if tx is selling and tx.price < dayPrice[day] then
            tx is confirmed at tx.price
        end if
        else if tx.price equals dayPrice[day] then
            tx is confirmed according to buying or selling
        end if
        if tx is not confirmed then
            add tx into unconfirmedTXs
        end if
    end for
end for
    
```

Figure 1: Pseudo Code of Combination of Call Auctioning and Commanding Pricing Method in ITO

In a blockchain system, each node is responsible for its credit by acting honestly, and therefore they would tend to upload authentic data. If other nodes intend to gain and use those data, they will be required to pay relevant tokens. In such a system, the legal tender is not suitable for replacing tokens. The reason is that the value of the former is stable, while projects experience dynamic developments, making it unstable. There is a likelihood of success and failure of projects. The value of a project is usually not reflected in the present value but reflected by its future development. Positive developments made by the project will result in a healthier ecosystem, increasing the value of the project. Similarly, the value of a project could reduce to zero or even negative if development fails to yield results.

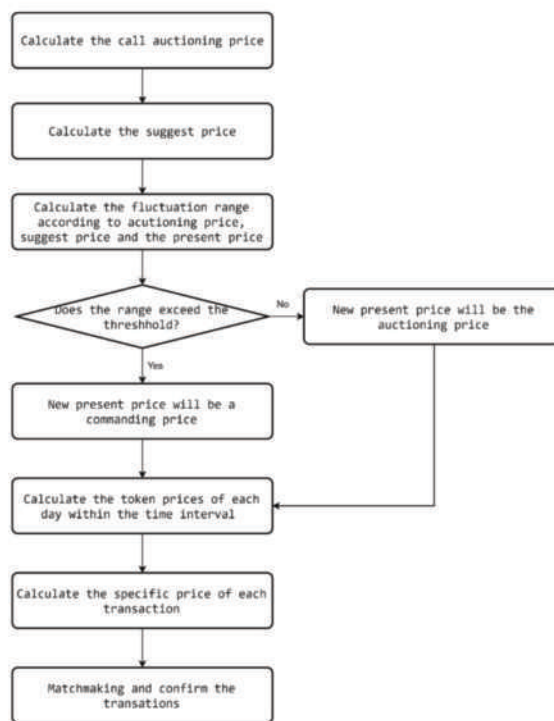


Figure 2: Flow Chart of Combination of Call Auctioning and Commanding Pricing Method in ITO

Apart from its function as a digital currency in the block chain, tokens can also act as an incentive mechanism to accelerate consensus reaching processes. Using ITO 1.0 can be an advantage when solving some of the public benefit problems that are not easy to address at the macro level. When the government supports a project, it may be difficult for the initial participants to receive the benefits directly in a traditional way. Hence, utilising ITO provides participants with a way to receive visible benefits while contributing to government-supported projects.

For example, promoting foreign trade platforms is difficult because it is hard to formulate uniform rules and standards. There may be many parties who enter with the mindset of wishing to invest little but wanting to gain massive profits. Without consistent rules and standards, if provisions can be set by anyone, many interested parties will come into disputes as they wish to be the ones gaining more profits. If the ITO mechanism is adopted for government sponsorship, once the platform has become well-established, the government will be willing to support it contributing to the entire economic system. However, the government cannot be deeply involved, as rent-seeking problems may arise otherwise, evident from cases in recent years, suggesting that a fully government-led platform is not necessarily suitable for the business market. Once the government has provided supporting resources, it will encourage individuals, companies, associations and other subjects to participate in platform construction.

The government can then evaluate the capabilities of each participant and allocate them resources in the form of tokens. The base price of a token is determined by the funds the government has provided. As the project progresses, the government can proceed to gradually exit the project, allowing the token price to evolve with the value of the platform. In other words, if the platform is successful, the token price will rise; otherwise, it will fall.

Table 1: A simulation of fluctuations and commanding prices: the negative value stands for sponsor buying-back, and positive value represents users buying-in.

W	Reserve	Liquidity	Market Price	Change of Liquidity	
0.5	5,000,000	10,000,000	1	0	issue price
0.5	4,000,000	9,000,000	0.888888889	-1,000,000	
0.5	2,666,667	7,500,000	0.711111111	-1,500,000	
0.5	1,244,444	5,500,000	0.452525253	-2,000,000	
0.35	1,244,444	5,500,000	0.646464646	0	Reduce the reverse rate to 0.35.
0.35	1,179,798	5,400,000	0.624231735	-100,000	
0.3	1,179,798	5,400,000	0.728270358	0	Reduce the reverse rate to 0.3.
0.3	1,398,279	5,700,000	0.817707069	300,000	
0.3	2,379,528	6,900,000	1.149530227	1,200,000	
0.3	4,678,588	8,900,000	1.752280158	2,000,000	
0.4	4,678,588	8,900,000	1.314210119	0	Raise the reverse rate to 0.4.
0.4	5,992,798	9,900,000	1.513332864	1,000,000	

Should a platform’s development be unsustainable, participants in the project that are unoptimistic will sell their tokens, resulting in the token prices to fall. The government can buy back these tokens at a lower price, allowing participants to exit the platform, shutting down the project as a result. If the platform development can continue, participants feel optimistic about the future trend and may pay high prices to obtain more tokens, and the token price will rise; ultimately, those holding more tokens will reap greater benefits in the future. The government can gradually release tokens to regulate the market’s supply-and-demand balance despite not being operationally involved. They can transfer the commanding right to the market itself while potentially benefiting from the process, and participants holding a significant number of shares are able to obtain the platform management rights eventually.

Foreign trade platforms with token-based technology have the advantage of being potentially more flexible and efficient. For example, in January 2020, enormous amounts of medical supplies were needed in Wuhan. Medical supplies were provided through a variety of organisations and channels, which involved a large number of logistical networks, resulting in low efficiency as a result due to confusion and miscommunication between different parties. A token-based foreign trade platform will allow information on the platform to be secure and accessible by all parties without the ability to alter the information. It will enable collaboration between the parties to be a smoother and more transparent process, reducing the likelihood of miscommunication. Presently, the coronavirus

is still spreading all around the world, and the overseas demand for supplies is rising. In this context, a new foreign trade platform to facilitate international trade information sharing and distribution of supplies would be greatly beneficial.

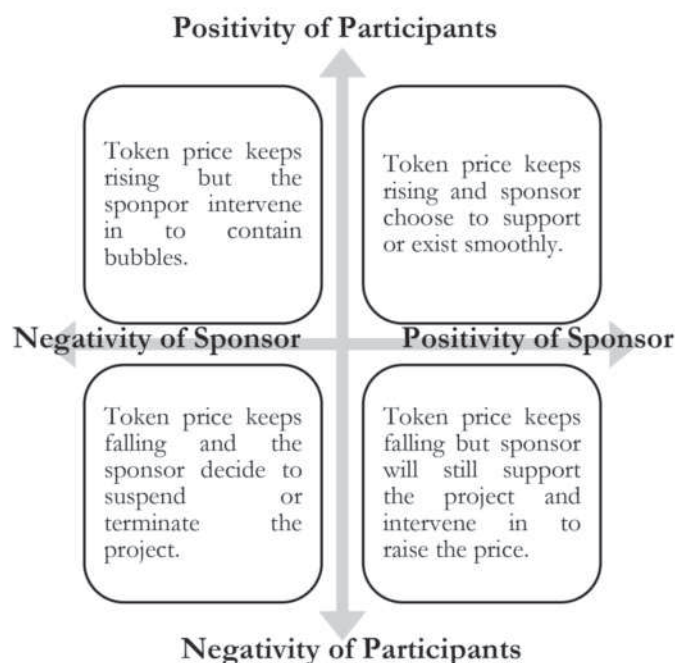


Figure 3: The attitudes of sponsors and participants will be reflected in token price.

7. ITO is a New Direction for Future Scenarios

Fundraising and value management are always worthy of in-depth study. The traditional financial markets, such as stocks, futures and options, can be regulated by some effective and centralised framework⁹. This kind of policies can confine the fluctuation of value within a limited domain. Still, they are not sufficient for pricing the potential value of innovative technology in scientific research or the pricing of the projects in the pre-private-equity stage, without enough flexibility and efficiency. In the way of blockchain fund raising, although ICO has high flexibility, the issuance price of the token is almost dominated by the issuer, and there is no effective regulations and rules to ensure the stability of the token value and the liquidity of the market.

ITO proposes a solution to the problems above. It is a fund-raising method between the government-supported funds for companies or research teams, and the private placement and IPO. Combining the advantages of planned economy and market economy, it is able to carry out in-depth and accurate support and investment, and guarantee the stability of the token value through the implementation of blockchain technology such as a smart contract to avoid the token speculations¹⁰.

Once the mechanism of ITO 1.0 has been validated, the ITO policy can be gradually liberalised and move on to ITO 2.0 and ITO 3.0. ITO 2.0 may allow funds, companies and even capable teams of individuals to participate in the issuance of tokens. In ITO 3.0, eligible individuals can also be allowed to raise resources to gain support. A healthy ecosystem will form within different scopes, and a merger will occur gradually into a system with a robust and diverse ecosystem, which will be a new direction for future investment.

There are more scenarios where ITO can be greatly beneficial. Education-oriented tokens that can only be used to exchange learning resources can be issued to students, and those who learn well or improve significantly

will receive more bonus tokens that can be exchanged into gifts or even cashed out. This provides a competitive and intense learning environment to solve the inefficiency problem of contemporary online education. In the fields of patents or intellectual property, some local governments provide extensive subsidies, but the latter are usually largely focused on quantity. In fact, different locations have their own local advantages that should be particularly prioritised to form a representative and competitive field. The local governments should plan and position first; for example, if they wish to encourage solar energy technology, the corresponding patents will be rewarded with subsidy tokens. Such tokens can be circulated and transferred within the relevant locality and facilitate patent-driven productivity gains, increases in social capital, etc., and ultimately may gradually form a unique competitive advantage. Such focused investment or support can be implemented through utilising the token-based blockchain technology.

ITO can be applied not only to the economy but also to public affairs. For instance, it can be applied to coronavirus-related topics, including developing cures, analysing public opinion, optimising logistics, etc., where different organisations or individuals can be assigned related tokens and social capital. Individuals can support different nodes by voting with their tokens. However, if participants do not make correct choices, voted tokens will become a cost to uninformed voters, and only informed voters with sufficient knowledge will gain more tokens. Therefore, individuals will be encouraged to do proper research and invest in nodes that solve problems.

There are many ITO scenarios that governments can get involved with. For example, sewage treatment is an area the government is willing to invest in, but local governments and enterprises may have the impulse to use policies to arbitrage. On-the-spot inspections cannot fundamentally prevent this phenomenon. If the blockchain technology is introduced, tamper-proof water quality monitoring data will be continually uploaded, and upstream and downstream water quality indicators can also be connected for comparison. This prevents and limits the ability of local players to distort data. The rewards of successful treatment can be regulated through smart contracts; i.e., relevant enterprises, organisations and scientific institutions can be assigned some tokens initially, but rewards will eventually be given according to actual contributions and achieving established targets. The issued tokens can circulate immediately, and their value will derive from the industry undergoing a healthy development; otherwise, the tokens will become worthless. Compared to giving money directly, tokens can provide a greater incentive with the potential of rising to ten times or even a hundred times their initial value very quickly, which will require each participant to contribute and engage in mutual supervision through fair competition in the market rather than depending on government intervention.

In addition to the applications of smart contracts for value management, ITO can also be used to solve the problem of in-depth and accurate financial investment that is difficult to achieve through centralised policies. For example, for the scientific research projects of universities or research institutions, ITO can be used to issue specific tokens of different technical steps in the research achievements, and invest in one or several vital fields. On the one hand, it provides financial support for scientific research achievements; on the other hand, with the transformation of scientific research achievements, corresponding tokens can deliver their growth potentials at their ascending prices. For enterprises or industries, differentiated supports can be carried out according to their scales. That is, the small-scale companies can be given token with relatively loose conditions, and the token circulation can be tracked for its value evaluation; for the large-scale ones, enterprises can be required to carry out fund matching according to the proportion of support amount, and relevant expenses can be reduced by issuing different kinds of tokens to ensure support funds are used in the target fields.

ITO has significant advantages over traditional financing. First, with the government acting as the sponsor, in the initial stages, the project will be valued appropriately with room for appreciation. Second, it makes

it possible to address project details and provide specifically targeted investment or support, which can reduce the costs to enterprises while making it conducive to the development of smaller businesses. Third, the circulation rules of tokens enable enterprises to access resources quickly, encourage the formation of a healthy ecosystem in the industry and will lead to sharing of value-added dividends.

The traditional financing methods of a blockchain such as ICO and IEO are often regarded as tools for money laundering that disrupt the order of financial markets to some extent. However, blockchain technology such as ITO can help the government strengthen its guidance and facilitate innovation instead of causing negative effects. The key is to start from a government sponsor, liberalise the policy gradually according to the status of system development and use the right to sponsor token issuance to release tokens gradually to qualified institutions, organisations and finally individuals following a smooth transition from ITO 1.0 to ITO 3.0 to reach the full potential of the blockchain technology.

References:

- [1] Y. N. Harari, "Sapiens: a brief history of humankind," Beijing: Citic Press, 2017.
- [2] H. J. Cai, "On digital currency and the transfer of world wealth and technology centers," *Frontiers*, vol. 196, no. 6, pp. 62-74, 2020.
- [3] D. K. C. Lee, G. Li and Y. Wang, "Practical applications of cryptocurrency: a new investment opportunity?" *Practical Applications*, vol. 6, issue 4, 2019. Accessed on: Sep. 07, 2020. [Online]. Available: <https://doi.org/10.3905/pa.6.4.324>
- [4] J. M. Zhu, "Money is losing its neutral character," *China Business News*, A11, Nov. 20, 2018.
- [5] D. He, R. Leckom, V. Haksar, et al., "Fintech and financial services: initial considerations," USA: International Monetary Fund, Staff Discussion Notes, 2017. Accessed on: Sep. 07, 2020. [Online]. Available: <https://doi.org/10.5089/9781484303771.006>
- [6] D. K. C. Lee and E. G. S. Teo, "The new money: the utility of cryptocurrencies and the need for a new monetary policy," May 23, 2020. Accessed on: Sep. 07, 2020. [Online]. Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3608752>
- [7] D. K. C. Lee and E. G. S. Teo, "Cryptocurrencies, stable coins and the growing pressure for new monetary policies," *Centre for Financial Regulation and Economic Development of CUHK*, Jul. 3, 2020.
- [8] F. Bi, "The prospect of financial reform of global blockchain," *Economic Relations and Trade*, no. 9, pp. 93-96, 2018.
- [9] L. H. Li, "Accelerate establishing digital finance and inclusive finance," *China Finance*, 2020.
- [10] D. K. C. Lee and C. Lim, "Blockchain use cases for inclusive fintech: scalability, privacy, and trust distribution," Sep. 9, 2019. Accessed on: Sep. 07, 2020. [Online]. Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3629135>.
- [11] D. K. C. Lee, "Digital economy and blockchain. TEAGEEKS," May 31, 2020. Accessed on: Sep. 07, 2020. [Online]. Available: <http://tjageeks.com/2020/05/31/digital-economy-and-blockchain-professor-david-lee-kuo-chuen-professor-of-finance-programme-singapore-university-of-social-sciences/>
- [12] D. Liebau and P. Schueffel, "Cryptocurrencies & initial coin offerings: are they scams? - an empirical study," *The JBBA*, vol. 2, issue 1, April 02, 2019 BST. Available: <https://jbba.scholasticahq.com/article/7749-cryptocurrencies-initial-coin-offerings-are-they-scams-an-empirical-study>
- [13] B. Li, B. Zheng, Z. Y. Guo, et al., "The state-of-the-art blockchain applications in finance: progress and trends," *Journal of Applied Sciences*, no. 2, pp. 151-163, 2019.
- [14] H. Li and L. K. Hu, "Rethink the supervision of ICO," *Law and Economy*, no. 2, pp. 3-16, 2019.
- [15] J. Y. Li, X. H. Fan and Y. Wang, "Design of sharing economy privacy protection mechanism based on block chain," *Computer Applications and Software*, no. 1, pp. 296-301, 2019.
- [16] A. J. Ren, "Reform bill market with blockchain," *South China Finance*, vol. 3, no. 475, pp. 41-44, 2016.
- [17] G. F. Sun and S. Chen, "The security essence and legal regulation of ICO," *Management World*, vol. 35, no. 12, pp. 45-52, 2019.
- [18] Y. W. Li, "Blockchain: how to stop a gap in legal supervision," *Newspaper of Posts and Telecom*, Dec. 6, 2019.
- [19] Z. Li and L. F. Huang, "International cooperation of digital currency supervision," *Journal of University of Electronic Science and Technology of China*

(Social Sciences Edition), no. 1, pp. 12-19, 2020.

[20] T. Wu and M. Li, "New dimension of blockchain financial supervision and governance," *Finance & Economics*, no. 11, pp. 1-11, 2019.

[21] D. Yang and Y. Ma, "Talk about digital currency with leading cadres," Party School of the Central Committee of C. P. C. Press, 2020.

[22] D. Yang and B. Y. Xing, "Experience and enlightenment of STO regulation in the United States," *China Finance*, no. 5, pp. 76-77, 2019.

[23] Q. Yao, "The similarities and differences between distributed ledger and traditional ledger and their practical significance," *Tsinghua Financial Review*, no. 6, pp. 64-68, 2018.

[24] X. R. Yi, "Blockchain technology, digital currencies and financial risks: a general analysis of financial theory," *Social Sciences in Nanjing*, no. 11, pp. 9-16, 40, 2018.

[25] L. Zhao, "How to regulate the decentralised blockchain?" *Economic Information Daily*, Jan. 09, 2019.

[26] C. Zang and L. N. Zhou, "Blockchain application of bill scenario," *China Finance*, vol. 872, no. 2, pp. 76-77, 2019.

[27] M. H. Zhang, "Regulation of token issuance from the perspective of foreign market securities law – based on the regulatory practices in the United States, Singapore, Australia and Hong Kong, China," *Law and Economy*, no. 3, pp. 106-120, 2019.

[28] H. J. Cai, S. J. Jiang, T. Q. Cai, J. W. Geng, and X. J. Cheng, "Blockchain: embracing the future of intelligence," Beijing: People's Publishing House, 2020.

[29] H. J. Cai, T. Q. Cai and J. W. Geng, "A blockchain system with integrated human and computer intelligence," Wubian: HUST Press, 2019.

[30] H. J. Cai, "Token: a tool to quickly reach local consensus within a limited domain," *Modern Bankers*, no. 6, pp. 39-41, 2018.

[31] T. Q. Cai, H. J. Cai, H. Wang, et al., "Analysis of blockchain system with token-based bookkeeping method," *IEEE Access*, vol. 7, pp. 50823-50832, 2019.

[32] M. Chanson, M. Risius and F. Wortmann, "Initial Coin Offerings (ICOs): An Introduction to the Novel Funding Mechanism based on Blockchain Technology," *Proceedings of Twenty-fourth Americas Conference on Information Systems*, 2018.

[33] T. M. Griffoli, M. S. M. Peria, I. Agur, et al., "Casting light on central bank digital currency," USA: International Monetary Fund, Staff Discussion Notes no. 18/08, 2018.

[34] R. Randolph, "The new digital wild west: regulating the explosion of initial coin offerings," *Harvard Law School Forum on Corporate Governance and Financial Regulation*, 2018. R. W. Greene and D. K. C. Lee, "Singapore's open digital token offering embrace: context and consequences," *The JBBA*, vol. 2, issue 1, pp. 1-11, 2019.

[35] F. A. Hayek, "Individualism and economic order," Routledge Press, 1948.

[36] F. A. Hayek, "The constitution of liberty," University of Chicago Press, 1999.

[37] J. M. Keynes, "The general theory of employment, interest and money," *Limnology & Oceanography*, vol. 12, no. 1-2, pp. 28-36, 1936.

[38] D. G. Hu, "The development and evolution of Keynesianism," Beijing: Tsinghua University Press, 2004.

[39] F. A. Hayek, "The use of knowledge in society," *Knowledge Management and Organizational Design*, vol. 35, no. 4, pp. 7-15, 1996.

[40] S. J. Zhang, "The theory and measures of state price control in ancient China," *Research on Financial and Economic Issues*, no. 3, pp. 46-50, 1990.

[41] J. Young, "Wrapped Bitcoin market cap up 27834% year-to-date, showing DeFi's strong growth in 2020," *Longhash*, Oct 19, 2020. Accessed on Oct. 20, 2020. [Online]. Available: <https://www.longhash.com/en/news/3388/Wrapped-Bitcoin-Market-Cap-Up-27834-Year-to-Date,-Showing-DeFi%E2%80%99s-Strong-Growth-in-2020>.

[42] A. Hao, "Sixty-seven percent of cryptocurrencies are still down over 90% from their ATHs," *Longhash*, Jul 5, 2019. Accessed on Sep. 07, 2020. [Online]. Available: <https://www.longhash.com/en/news/2540/Sixty-Seven-Percent-of-Cryptocurrencies-are-Still-Down-Over-90-From-Their-ATHs>.

[43] S. Bai, "Blockchain technology and applications," *China Bond*, no. 5, pp. 81-85, 2018.

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

TQC, HJC and DKCL designed and coordinated this research and prepared the manuscript in entirety. DY contributed to the supervision part and KW helped to

analyse the related work from Hayek and Keynes.

Funding:

This work was supported in part by the National Natural Science Foundation of China under Grant 61832014.

Acknowledgements:

We would like to express our appreciation to Professor Bai Shuo, and Section 4 is benefited from the discussion with him.

¹ In June 2018, for example, the FCoin exchange was a hit with investors because of the potential trading revenue from transactions for investors acting as a mining node for an exchange. Binance's founder Changpeng Zhao described the mining node as "not only a disguised ICO, but also an over-priced ICO". The price of FCoin increased by 100 times within two weeks of the launch. However, the price peaked on June 13, 2018, and subsequently crashed to almost zero. On February 10, 2020, the FCoin exchange suspended its system. Founder Jian Zhang admitted that their biggest problem was not the re-launch of the network, but the inability to provide enough reserves to pay off the debts. The amount of non-payment is expected to be between 7,000 and 13,000 BTC. FCoin did not set a maximum reward threshold and exhausted the incentive payouts in a short time. The right to issue new dividend tokens was not within the control of the project team but dictated by the trading volumes. This design fault resulted in scalping and arbitrage, worsened the platform ecosystem and led to its eventual collapse.

² For example, once the issuer obtains the ETL (Eligibility to List) from SGX, the issuer will lodge its prospectus with MAS for registration and commence book-building to gauge market interest in the issue. <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Securities-Futures-and-Fund-Management/Regulations-Guidance-and-Licensing/FAQs-on-Offers-of-Shares-and-Debentures-and-CIS-8-Oct-18-Revised.pdf>

³ For example, https://www.mas.gov.sg/-/media/MAS/resource/legislation_guidelines/Securities_futures/sub_legislation/Guidelines_Regulation_of_Markets.pdf (Page 11) and <http://rulebook.sgx.com/rulebook/66-obligations-designated-market-maker>

⁴ The Monetary Authority of Singapore (MAS) released the Consultation Paper on a New Omnibus Act for the Financial Sector on July 21, 2020, which is a big move for token economy in Singapore.

<https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/2020-July-Consultation-on-FSMA/Consultation-Paper-on-a-New-Omnibus-Act-for-the-Financial-Sector.pdf>

⁵ The linked exchange rate is a fixed exchange rate system, which fixes the exchange rate between local currency and a certain foreign currency, and strictly follows the fixed exchange rate, so that the currency issuance is linked with the foreign exchange reserves.

⁶ The Alternative Reference Rate Committee (ARRC) proposed SOFR, a broad measure of the cost of borrowing cash overnight as collateral for Treasury bonds.

⁷ The price movement comes from the evolution of cognition. In the early stage of cognition, or the formation of a commanding price, the arbitrage space is large, but the time is relatively limited. Only when all the conditions are transparent and the game is sufficient, can the formation of prices be gradually sustained, approaching the necessary labor time. In reality, the factors are often way complicated, even if the production factors and conditions have been almost transparent, the price of steel still fluctuates significantly.

⁸ At the end of the Spring and Autumn Period (approximately 500 B.C.), a series of measures were proposed by FAN Li. Until now, the government taking measures to dampen price pressure is still an important aim of macroeconomic regulation and control (macro-control) in China. For example, during the COVID-19 outbreak, the price of key goods such as masks and disinfectants have been monitored closely by the state. Sellers will be fined or be taken off the online portal if they have been found to sell the products at exorbitant prices.

⁹ For example, the policies of Securities and Futures Act (CAP. 289) <https://sso.agc.gov.sg/Act/SFA2001> issued by MAS in Singapore have been adopted.

¹⁰ For example, in a smart contract that is deployed in advance, the investment cycle is one month and the fluctuation limit is 10%, which means the issuer needs to cash in the token value with the investors every month. If 1000 Token A are issued at the price of 2 BTC, and the price falls below 1.8 BTC within one month, the issuer needs to exchange with investors at the price of 1.8 BTC after maturity. The issuer cannot misappropriate the principal for market making, and the issuing price in the next cycle shall not be higher than 1.8 BTC, and therefore the investors' loss will be limited in each cycle. If the development of the project is not as expected, the price of Token A continues to fall. After several cycles, the amount of funds raised becomes smaller and smaller, and the project will be terminated gradually. On the contrary, if the price of Token A continues to rise and exceeds 2.2 BTC in the cycle, the contract will restrict that investors can only sell out instead of buying in Token A, so as to assure that the token price will not increase too fast in each single cycle.

Industrial Symbiosis Networks in Greece: Utilising the Power of Blockchain-based B2B Marketplaces

Stavros T. Ponis

School of Mechanical Engineering, National Technical University of Athens, Greece

Correspondence: staponis@central.ntua.gr

Received: 21 September 2020 **Accepted:** 20 November 2020 **Published:** 5 December 2020

Abstract

The proliferation of industrialisation and its environmental consequences over the last decades dictates the need for transitioning to a 'Circular Economy' (CE) business model with a view to balancing manufacturers' economic prosperity and environmental sustainability. Business models based on 'Industrial Symbiosis Networks' (ISNs), within which traditionally independent industries continually exchange energy, materials and by-products, with no or minimum waste produced, have the potential to proceed in this direction. However, due to various cultural, organisational and managerial barriers, their state of development in Greece, similar to rest of the world, is very low. That is exactly where this article sets its objectives, aiming to alleviate these barriers and contribute in establishing cross-sectoral synergies by introducing an innovative business model, supported by an exchange platform in the form of a blockchain-based B2B digital marketplace. The proposed business model will detail a plan for creating symbiotic relationships among manufacturing companies in Greece and will be supported by a blockchain-based marketplace, which will enable material, by-product and energy exchanges in a reliable and secure way. Blockchain will act both as an exchange platform and a trust mechanism, since its decentralised nature, which is manifested in all its capabilities i.e. smart contracts or tokenisation will increase the business model's reliability and facilitate its adoption and market penetration. The successful implementation of the proposed business model will bring about a multifaceted positive impact ranging from its contribution to exceeding the current state-of-the-art in the intersection of environmental science and information technology, to benefiting society and economy through fostering sustainable regional development.

Keywords: *Blockchain, B2B Marketplaces, Circular Business Model, Industrial Ecology, Industrial Symbiosis Networks, Industry 4.0*

JEL Classifications: *Q57*

1. Introduction

The proliferation of industrialisation over the last decades has undoubtedly led to environmental degradation, while casting a long shadow over manufacturing companies, failing to efficiently conform to waste prevention policies and capture the financial and social benefits of a more circular and sustainable manufacturing practice [1], [2]. At the same time, the ever-increasing population dictates the continuous evolution of businesses' manufacturing processes, in order for them to accommodate growing customer needs and ultimately flourish in today's constantly shifting competitive landscape [3]. Unfortunately, these business achievements come, all too often, to the detriment of the environment, rendering industrial activity responsible for a plethora of adverse effects, including waste generation, harmful Greenhouse Gas (GHG) emissions and depletion of natural resources [4]. As a matter of fact, in Greece, waste resulting from such activities is predicted to amount to 18.074 tons in 2020, while GHG emissions exceeded 7 megatons (Mt) in 2017 [5]. To add insult to injury, Greece's voracious consumption levels are so unsustainable that it would need to grow four times its current acreage to meet consumers' future needs, which indisputably aggravates resource depletion, land use and global warming. It is beyond the shadow of doubt that industrial systems cannot be sustained for long, when natural materials become scarce and waste to nature exceeds its carrying capacity, i.e. the ability with which nature can decompose waste within a given time and space.

Under these circumstances, the need to ensure manufacturers' environmental compliance without compromising their resource supply

and undisrupted production, and hence their economic benefits, is of paramount importance. In view of the intrinsic mechanics of the conventional linear economy, which rely on a wasteful 'take, make and dispose' flow [6], the need for transition to a sustainable Circular Economy (CE) business and manufacturing model emerges as a viable and imperative solution for achieving a better balance and harmony between economic prosperity and environmental sustainability. Environmental practices such as the 6Rs, i.e. 'reduce, reuse recycle, repair, rethink and refuse', fully encapsulate the essence of CE by promoting closed-loop flows, which optimise material cycles, maximise resource efficiency and reduce environmental impacts [7]. In this direction, Industrial Ecology (IE) has been widely considered for over two decades, as an immensely useful framework for facilitating and guiding this transition towards circular and sustainable manufacturing [8]. This is accomplished by investigating the hypothesis that an industrial system can be viewed as an ecosystem constantly trying to avoid waste, reintroducing waste as a resource and preserving the value of a product as long as possible [9].

The research presented in this article focuses on Industrial Symbiosis (IS), a concept which dates back in 1997 coined from the successful case of the Kalundborg recycling network in the northern part of Sjælland in Denmark [10]. Since then the term has become established within the field of IE and also within the business community and policy makers. IS in essence, aspires to form interorganisational networks, termed Industrial Symbiosis Networks (ISNs), emulating the symbiotic functioning of ecological systems, within which traditionally independent industries continually exchange energy, materials and by-products, with

no or minimum waste produced [11]. These networks traditionally exploit geographical proximity and manage to bring about a twofold advantage over traditional industrial systems. First, they manage to improve resource efficiency by transforming waste streams into new valuable resources, which are thereafter used in other processes. In that way, ISNs prolong the economic useful life of materials, which have exhausted their physical and/or functional service life and would otherwise be disposed of. Second, the production of waste, GHG emissions and subsequently the environmental footprint of collaborating industries is significantly reduced [4].

However, despite its merits, the practical implementation of ISNs is currently lacking the expansion the underlying concept of IS deserves. There are many reasons for this hampered performance. First of all, participating in an ISN is an investment and as such financial barriers and investment-inherent risks have to be overcome in order to proceed in such a decision. Still, these barriers being hard in nature can be easily quantified and in most cases the decision to proceed in the development or participation in an ISN would be favorable, since the benefits of creating a demand-supply network of processed by-products are significant [12]. Alas, as literature proves, there is a variety of cultural, organisational and managerial factors negatively affecting decision making on forming or participating in an ISN, as shown in Figure 1.

Greece is not an exception when it comes to the application of IS concepts in industry and manufacturing systems. The state of ISN development is very low and Industrial Symbiosis, as a concept, is not well acknowledged among stakeholders, policy makers and regional authorities [13]. Therefore, in light of Greece's environmental status quo, peaked consumption profile and resource scarcity, the adaptation of the ISN paradigm by the Greek industries seems like an imperative. That is exactly where this research sets its vision, objectives and aspirations aiming to contribute in alleviating the aforementioned barriers by introducing an innovative Circular Business model for ISNs in Greece supported by open-source blockchain technology, which seems a perfect fit for tackling major obstacles of ISN development and operations, such as trust, information sharing, compatibility, misalignment and limited management awareness and insights.

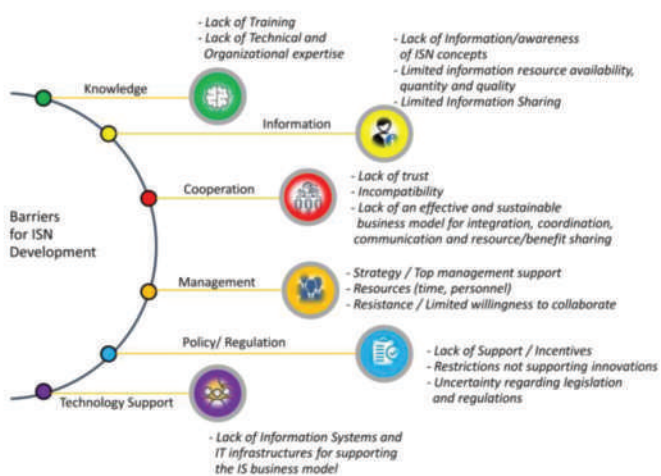


Figure 1: A Taxonomy of barriers for ISN development

2. Challenges

Our initial review of available literature and the current perception of industry and policy makers as expressed in white papers and regulatory documents supports – with little or no dispute – the argument that Circular Economy and specifically Industrial Symbiosis Networks have the potential to support the sustainable, environmentally responsible and ‘clean’ growth and development of industrial manufacturing systems.

Nonetheless, the development of ISNs globally and the number of cases where the ISN model has become prevalent is still lagging, with most of the cases referring to the establishment of eco-industrial parks [14], [15]. The main reasons behind that situation are summarised in the barriers of Figure 1, which are hindering ISN development and therefore, in essence, outline the framework of challenges this article aims to address. Indeed, the proposed business model aims to a) provide the impetus needed to tackle these obstacles of ISN development by raising awareness and providing them with a viable circular business model and a roadmap with guidelines for its implementation, b) support Greek manufacturing companies to examine ways to build a knowledge base of material/by-products and waste exchanges and to further study and rethink their business processes in order to facilitate the establishment of synergies across companies of the same or different industries and c) support the development and operation of closed-loop material/by-products and waste exchanges within and across industrial ecosystems supported by an open source, low-cost and reliable information technology infrastructure.

Lack of management knowledge and awareness of ISN concepts, mechanisms and benefits is a key challenge to overcome when attempting to identify potential synergistic opportunities. Absorptive capacity, i.e. the ability to ‘recognise the value of new, external information, assimilate it, and apply it to commercial ends’ [16], succinctly captures the capabilities needed for knowledge transfers to translate into financial incentives. The proposed business model will be aligned to the need for enhanced absorptive capacity of stakeholders and effectively address it by creating mechanisms to educate potential stakeholders and enhance their understanding of IS concepts, technical and organisational aspects of symbiosis, rules of participation, expected benefits and their sharing mechanisms. As for information sharing between potential participants, it is obvious that lack of it can create conflicts leading to reduced intention and willingness for resource sharing. The proposed research addresses this challenge by establishing a means of coordination of information flows pertaining to resources’ origin, availability, quantity and quality. Emboldening exchanges of such knowledge is capable of increasing the cognitive proximity and understanding of each other’s business, thus leading to improved selection capabilities and utilisation of resources to the furthest extent possible. Another dissuasive factor against ISN development is the lack of compatibility, which can result from different company sizes, management culture or even more operational reasons such as old and long-standing contracts. The proposed research addresses this challenge by establishing direct information exchanges and knowledge base access, in order to enhance visibility even for smaller companies and transparency regarding available resources and production outputs (waste/by-products) for all the companies participating in the ecosystem. This approach will eventually eliminate the unfamiliarity with one another’s business and lead to the creation of synergies between industries and their manufacturing systems.

An additional fundamental challenge ISN development is faced with is the lack of support, i.e. deficiencies in policies, outdated regulations and restrictive definitions of waste, by-products and industries’ potential involvement in their usage. Again, the proposed business model, through its successful operation, will be able to contribute, in the long run, to the identification and specification of required legislation and regulations on all scales, including companies, industries, supply chains and beyond, to support IS applications. Last but not least, although the introduction of the proposed business model might point the way towards legislative changes, its influence on current management practices and decision-making in organisations will probably be ponderous. It is only through its success and expansion over time that the proposed business model will be able to shift companies’ focus towards reshaping actual strategies to examine the lack of training, expertise and resourcing of time and personnel under the lens of organisational ISN-oriented change.

Intentionally we left for last the challenge of trust, which according to

literature is the most prominent between challenges, since most potential participants have no experience of a symbiotic relationship and no cooperative mechanisms of this nature in place, thus they are hesitant to adopt an ISN business model. Indeed, building a trusted IS ecosystem is of paramount importance and overcoming common obstacles, such as competitive attitudes or corporate 'social isolation' is a vital prerequisite for forming viable, long lasting and functional synergies. To deal with this difficult challenge and also provide the necessary technology support (see Figure 1) for the proposed circular business model to work efficiently, we introduce an innovative B2B (Business-to-Business) marketplace based on blockchain technology, which will be described in detail in the next section. Truth is that there are numerous research efforts studying the potential of Blockchain in greening supply chains or applying Circular Economy business models, but to our best knowledge, current literature lacks any research efforts dealing with ISN, supported by Blockchain-based marketplaces. If one had to pinpoint a research fairly resembling the one presented in this article, this would pinpoint the work of Nallapaneni & Chopra [17]. The authors study the energy flows in Networks of Firms resulting in an Industrial Symbiosis-based Multi Energy System (IS-MES). They claim that the actual implementation of such an IS-MES is vulnerable to cascading failures emerging from one firm in the network, which makes them inherently resilient. To counter this resilience challenge, they propose the use of the Blockchain-based Online Information Sharing (BOIS) platform, where a firm-to-firm (F2F) IS relationship establishment mechanism following the IS principles is possible through the blockchain-based smart contracts. In essence, the potential of blockchain to support environmental sustainability, according to [18], comes down to one key feature: its ability to provide a verifiable record of who exchanges what with whom and therefore who has what at a given time. Many of the challenges for how we manage natural resources and maintain ecosystem services arise because of a lack of trust and confidence in the rules governing exchange and possession.

In the proposed business model, blockchain acts both as an exchange platform and as a trust mechanism. Traditionally, a B2B marketplace relies on an intermediary (market owner) who brings together multiple buyers and sellers to facilitate transactions. Because trust is fundamental for valued relationships in B2B markets, this entity acts as a Trusted Third Party (TTP), which safeguards against fraud and the misuse of trust among market participants. Additionally, the TTP keeps the electronic registry of the transactions, ensures its integrity and depends on the banking payment system for settling registered transactions. For these services, the TTP charges transaction fees covering its operating expenditures. However, because the TTP controls the infrastructure, information flow and the processes governing the marketplace, trust issues are raised. Blockchain eliminates this issue by its trustless definition, since there is no central authority dominating the market. Record keeping and data-sharing in the ISN ecosystem will be kept in a digital ledger, visible to all authorised members only, since the blockchain will be permissioned, thus enhancing transparency and traceability, while at the same time protecting sensitive information from unauthorised parties. Naturally the level of shared information, especially as sensitive as sustainability information, could be a point of conflict and tension and it is something that will be researched in the context of the proposed research. Finally, regarding the trust issues raised by the inherent reliability and security capacity of the B2B blockchain marketplace, up to now few are the cases of failures and attacks to such systems. Still, since the technology is yet at its infancy, the research will put specific emphasis on security aspects. Regardless, by definition blockchains share information in highly secure and reliable cryptographic modes, a fact which when coupled with the inherent technology characteristics of immutability, consensus and distributed ledgers, enhances the trustworthiness of information and lessens the probability of its falsification, fraud or corruption.

3. System Architecture

According to [19], there is an immense need for a web of knowledge to facilitate the establishment of physical exchanges of resources among diverse organisations. Furthermore, the definition by [20] further clarifies that the exchanges must be novel and that IS requires the integration of the following features in order to be successful and have a significant impact in science and society, i.e. a) a functional web of knowledge, b) a network of diverse organisations, c) novel sourcing of inputs, d) value-added destinations of non-product outputs (and further end-life products), e) improved business and technical processes, f) a collective approach of a system as a whole and, finally, g) a justified definition of the boundary of the industrial ecosystem (material-based, product-based, geographic-based). Exhaustive scrutiny of the CE and IS's current state-of-the-art testifies, to the best of our knowledge, that such efforts do not exist.

As already mentioned, forging IS partnerships between Greek manufacturing companies, has thus far been inadequate [13] for them to fully reap the benefits of IS – a fact, highlighting our proposal's inherently innovative character. Therefore, the proposed research puts special emphasis on bridging technological advance and market application, while attuned to the triptych of balancing and maximising environmental, economic and societal values. The proposed business model combined with the development of the blockchain B2B marketplace platform will actively serve this purpose by stimulating cross-sectoral connections, enabling material flow compatibilities and leading to the formation of industrial synergies. In the epicentre of the article's innovation lies the notion of third-generation marketplaces, i.e. decentralised B2B exchanges. The term 'exchange' refers to traditional price-setting mechanisms including auctions. In essence, the proposed marketplace will utilise blockchain technology for waste/by-product trade digitisation, enabling multiple participants to collaborate and transact using shared views of the system's knowledge base for selecting suppliers and products (waste or by-product type and quantity) and current transactional information including shipping details and expected delivery dates.

The marketplace will incorporate a private Payment system for Ecosystem Services (PES) and a Smart Execution of Transaction (SET) capability, based on decentralised applications running on the blockchain platform, i.e. Smart Contracts. Specifically, each participant of the ISN ecosystem will be able to browse the knowledge base for identifying available products (waste or by-products) they wish to acquire and then proceed in closing a predetermined available smart contract embedding codified business logic, rules and terms hard-coded using a programming language such as C++, JavaScript or Java. The contracts will be fully transparent, verifiable and permanently written into the marketplace's blockchain. This SET capability is of great importance for the financial viability of the ecosystem, since the design and operation of the contracts can be achieved at minimal cost, several orders of magnitude lower than the costs of operating computer servers and personnel as in traditional marketplaces. Moreover, the marginal cost of developing a new contract or replacing a redundant one with an improved newer version, as in the case of a change in contractual terms, is expected to be equally low. Finally, as mentioned earlier, one has to note the importance of SET for building trust among participants in the ecosystem, since all transaction processes on decentralised B2B exchanges will be self-executed and the transmission of information, product ownership and value will take place in a fully autonomous fashion without a central authority policing, monitoring and potential influencing the integrity of fair transactions.

Each one of the transactions in the marketplace will be validated and recorded in the blockchain registry upon the payment of the supplier of waste/by-product. For that reason, the marketplace will use a private PES functionality materialising the exchange of waste, by-products and materials through a transparent and immutable way, monetised and translated into tokens. The traditional energy-intensive Proof-of-Work (PoW) consensus algorithm will be replaced by a new 'Proof-of-Contract' method (PoC), which will be based on the main principles of the Proof-of-Stake (PoS)

consensus mechanism. Instead of having miners (PoW) or validators/ forgers (PoS), in the proposed consensus mechanism, the ecosystem will use the concept of ‘Closers’, i.e. members of the blockchain with a high credibility score. In the proposed research, credibility is measured as a weighted sum of three factors, the number of ‘closed’ contracts, the number of parties participating in these contracts and the sum of tokens exchanged in these contracts. In that way, the major security concern of PoS consensus mechanisms, i.e. the party owning more than 51% of the ecosystem’s token value can manipulate transactions, is significantly ameliorated. As the authors in [21] argue, while in the PoS one needs to store enough tokens to dominate the ecosystem, in the suggested hybrid consensus-reaching approach using credibility score, one needs to use enough tokens in order to make contracts. Since storing and using tokens are opposite ideas, it is harder to increase both of them, and it is harder to manipulate the ecosystem.

The successful execution of the transaction will release – as a reward – the number of tokens hard-coded in the smart contract. It is reasonable, that the exchanges in the ecosystem are not necessarily reciprocal, meaning that a company might have materials, by-products or waste to offer without needing to receive any in exchange, or vice versa. This will undoubtedly contribute to the accumulation of unutilised tokens within the network. To address this eventuality, the ecosystem will explore the options offered by an Initial Coin Offering and the token’s participation in an established exchange, such as Coinbase.

The high-level architecture of the proposed Blockchain-based marketplace is presented in Figure 2. It has three access points, depending on the user type (project, business stakeholders supply-side and business stakeholders demand-side) attempting to enter the ecosystem and all users have to be registered before using the marketplace functionalities. The architecture is segmented in five integrated functional areas, i.e. Identity and Access Management (IAM), Database and Knowledge Management (DKM), Ledger Management (LM), Smart Execution of Transactions (SET) and Payment for Ecosystem Services (PES). Each functional area includes a set of blocks, each one providing a specific set of ecosystem functionalities, for example the Query Execution Manager (QEM) is a functional block of the Database and Knowledge Management area and is responsible for both scheduling query execution and directing queries to the appropriate tables inside the system’s knowledge base. The QEM enhances response, decreases processing times and delivers data to users in appropriate formats.

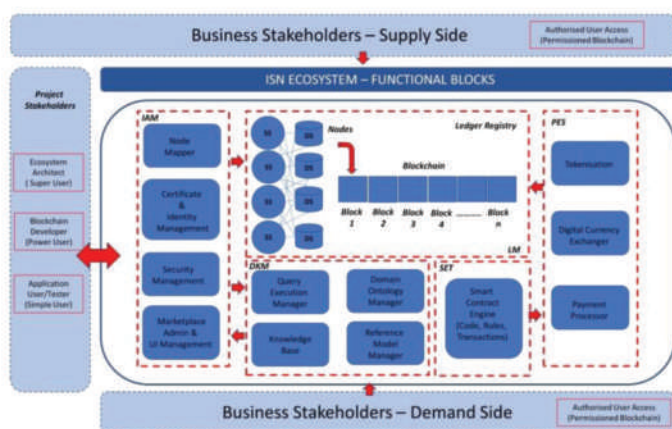


Figure 2: Functional Blocks of the Proposed System

The Blockchain-based marketplace will be the epicenter of the proposed business model, which will take advantage of its functionalities in order to secure its flawless and uninterrupted operation, while creating a trusted collaborative environment for all the participants of the ecosystem.

4. Expected Impact

Industrial Symbiosis (IS) and the formation of interorganisational networks operating on a symbiotic nature can play a significant role in the global efforts for industrial sustainability and manufacturing compliance with Circular Economy principles. And the stakes for such a strategy, management, corporate culture and organisational change are far from insignificant. Actually, according to [22], the application of Circular Economy principles in all sectors and industries will benefit Europe environmentally and socially, while having the potential to generate a net economic benefit of EURO 1,8 trillion by 2030, resulting in over 1 million new jobs across the EU by 2030. The proposed research provides a set of targeted solutions and services for enhancing and supporting all the above success factors for an ISN to flourish and create significant scientific, social and potentially financial impact.

The research presented in this article is expected to have a strong socio-economic impact, since the adoption of its results can potentially lead to the emergence of novel ISNs in the Greek periphery and enhance regional development, by enabling existing and new industries, as well as communities, to access more competitively priced resource inputs and reduce their waste management and emission control costs. More resource inputs will be transformed into marketable products, which further enhances resource productivity and provides economic benefits. Moreover, in some cases the adoption of the proposed business model will bring new processing or transfer needs, which will in turn stimulate new business development and employment. Finally, the success of the proposed research can ignite a series of improvements to regional eco-innovation capabilities, with profound implications for more sustainable regional development.

Essentially, the adoption of research results can provide an important competitive advantage for the traditional Greek industries that have been affected by the global economic downturn and industrial restructuring taking place in Europe and worldwide, and in addition protect them from the forthcoming new wave of economic crisis as an aftershock of the COVID-19 pandemic. Creating symbiotic relationships and adopting new, innovative and sustainable business models that take advantage of otherwise unused industrial flows may be a partial solution to disrupted supply chains as a result of natural disasters.

As for individual organisations participating in an ISN network and adopting the proposed business model, the impacts are numerous and multifaceted. First of all, IS exchanges can potentially generate significant cost savings, by reducing the cost of waste management and purchasing of raw materials while at the same time reaping benefits from the sale of by-products or the reuse and recycle of waste materials. Other, more difficult to assess, economic opportunities are related to the strengthening of the environmental position of the company and enhancing its Corporate Social Responsibility (CSR) profile, which can be translated as a tangible competitive advantage leading to the increase of the company’s customer base. Furthermore, adopting a strong environmental commitment and a pro-active attitude towards the introduction of further environmental improvements will build a moral high stand for both management and employees, which in turn contributes to strengthening the company commitment, by providing resources on a continuous basis to invest in environmental improvements, thus benefiting the environment and the community as a whole.

Finally, one should not overlook the benefits of adopting the proposed business model in management and cooperation culture of participating companies. Although as displayed in Figure 1, the absence of communication and cooperation is one of the main obstacles for the development of environmental ISN initiatives, by embracing the proposed business model companies are expected to take positive steps to improve communication with other agents at the intra-organisational level.

Furthermore, the progressive integration of the environmental variable in the process of decision-making of companies and its growing relevance in strategic terms, will provide an excellent opportunity for the further development of IS and collaboration projects once the environmental gains of such a strategy are fully recognised.

5. Conclusions

In order to address the challenges inherent to implementing blockchain-based solutions and overcome the well-known obstacles of ISN development as shown in Figure 1, the research proposed in this article will proceed in a set of action steps, presented in Figure 3. These steps are in line with the European Commission's ambitious Circular Economy Action Plan [23] and Agenda of Sustainable Development adopted by all United Nations Member States in 2015 and more specifically, Sustainable Development Goal (SDG) 12 under the heading of 'Responsible Consumption and Production'. Among other targets, SDG 12 seeks to substantially reduce waste generation through prevention, reduction, reuse and recycling and encourage companies to adopt sustainable practices and integrate sustainability information into their reporting cycle, with the aim of achieving sustainable management and resource efficiency by 2030 [24].



Figure 3: Research Action Steps

Finally, the research proposed in this article has unavoidable limitations, propagated mostly by the barriers of ISN development presented in Figure 1, with the most prominent ones being the lack of technical expertise by potential participants and the uncertainty regarding legislation and regulations in support of ISN initiatives and blockchain adoption in specific regions. In terms of technical implementation, the proposed research is again limited by 'soft' issues that may arise during the initiation phase, such as the persisting lack of trust in the technology, which most of the times comes as a result of its inherent complexity leading decision makers to a deficient understanding of underlying concepts and mechanisms. To that end, the lack of blockchain standards further impedes the research efforts for blockchain technology adoption and signing off of similar research projects. In order to mitigate the effects of lack of trust in the technology, the proposed research aims to develop and disseminate right from the start, a proposed business plan for creating symbiotic relationships supported by two white papers, the first detailing a roadmap for potential business stakeholders and the second including guidelines and suggestions towards ISN policy makers and regulatory bodies. The early identification of limitations or enablers of the in effect – at the time of the study – legislative and regulatory framework can be of great significance, especially when it comes to attract investors and influencing initial participants.

References:

[1] Y. Guan, G. Huang, L. Liu, C. Z. Huang, and M. Zhai, "Ecological network analysis for an industrial solid waste metabolism system," *Environmental Pollution*, vol. 244, pp. 279–287, 2019.
 [2] Y. Guan, G. Huang, L. Liu, M. Zhai, and B. Zheng, "Dynamic analysis of industrial solid waste metabolism at aggregated and disaggregated levels," *Journal of Cleaner Production*, vol. 221, pp. 817–827, 2019.
 [3] P. Viorel and C. Rudinchi, "Status and trends in the global manufacturing sector," *Create a culture of innovation with IIoT World!*, 26-May-2020. [Online].

Available: <https://iiot-world.com/connected-industry/status-and-trends-in-the-global-manufacturing-sector/>. [Accessed: 14-Sep-2020].
 [4] A. Neves, R. Godina, S. G. Azevedo, and J. C. O. Matias, "A comprehensive review of industrial symbiosis," *Journal of Cleaner Production*, 04-Nov-2019. [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0959652619339836>. [Accessed: 14-Sep-2020].
 [5] "Greenhouse gas emissions by country and sector (infographic): News: European Parliament," *Greenhouse gas emissions by country and sector (infographic) | News | European Parliament*, 17-Oct-2019. [Online]. Available: <https://www.europarl.europa.eu/news/en/headlines/society/20180301STO98928/greenhouse-gas-emissions-by-country-and-sector-infographic>. [Accessed: 14-Sep-2020].
 [6] F. Sariatli, "Linear Economy Versus Circular Economy: A Comparative and Analyser Study for Optimization of Economy for Sustainability," *Visegrad Journal on Bioeconomy and Sustainable Development*, vol. 6, no. 1, pp. 31–34, 2017.
 [7] V. Moreau, M. Sabakian, P. V. Griethuysen, and F. Vuille, "Coming Full Circle: Why Social and Institutional Dimensions Matter for the Circular Economy," *Journal of Industrial Ecology*, vol. 21, no. 3, pp. 497–506, 2017.
 [8] N. Nakajima, "A Vision of Industrial Ecology: State-of-the-Art Practices for a Circular and Service-Based Economy," *Bulletin of Science, Technology & Society*, vol. 20, no. 1, pp. 54–69, 2000.
 [9] S. Erkman and R. Ramaswamy, "Industrial Ecological Solutions," *Environmental Solutions*, pp. 297–310, 2005.
 [10] J. Ebnfeld and N. Gertler, "Industrial Ecology in Practice: The Evolution of Interdependence at Kalundborg," *Journal of Industrial Ecology*, vol. 1, no. 1, pp. 67–79, 1997.
 [11] "ForWeb Industrial Symbiosis F01 sustainable way and contributes to the creation of a circular economy - [PDF Document]," *vdocuments.mx*. [Online]. Available: <https://vdocuments.mx/amp/forweb-industrial-symbiosis-f01-sustainable-way-and-contributes-to-the-creation.html>. [Accessed: 14-Sep-2020].
 [12] L. Kosmol and L. Otto, "Implementation Barriers of Industrial Symbiosis: A Systematic Review," *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.
 [13] A.S. Donnavis, P. Kafasis and N. Davos, "Using an online platform for the improvement of industrial symbiosis and circular economy (in Western Macedonia, Greece)," *Issue 1 Global NEST: the international Journal Global NEST Journal*, vol. 21, no. 1, pp. 76–81, 2019.
 [14] S. K. Bebera, J.-H. Kim, S.-Y. Lee, S. Sub, and H.-S. Park, "Evolution of 'designed' industrial symbiosis networks in the Ulsan Eco-industrial Park: 'research and development into business' as the enabling framework," *Journal of Cleaner Production*, vol. 29-30, pp. 103–112, 2012.
 [15] L. Zhang, Z. Yuan, J. Bi, B. Zhang, and B. Liu, "Eco-industrial parks: national pilot practices in China," *Journal of Cleaner Production*, vol. 18, no. 5, pp. 504–509, 2010.
 [16] W. Cohen, "Absorptive Capacity: A New Perspective on Learning and Innovation," *Strategic Learning in a Knowledge Economy*, pp. 39–67, 2000.
 [17] M.K. Nallapaneni, & S.S. Chopra, "Blockchain-based Online Information Sharing Platform for Improving the Resilience of Industrial Symbiosis-based Multi Energy Systems", *Actionable Science for Urban Sustainability 2020 (AS&US-2020)*, Segovia, Spain, 2020.
 [18] M. D. Le Sève, N. Mason, and D. Nassiry, "Delivering blockchain's potential for environmental sustainability," *Briefing Note*. [Online]. Available: <https://www.odi.org/sites/odi.org.uk/files/resource-documents/12439.pdf>.
 [19] T. Domenech and M. Davies, "The social aspects of industrial symbiosis: the application of social network analysis to industrial symbiosis networks," *Progress in Industrial Ecology, An International Journal*, vol. 6, no. 1, p. 68, 2009.
 [20] D. R. Lombardi and P. Laybourn, "Redefining Industrial Symbiosis," *Journal of Industrial Ecology*, vol. 16, no. 1, pp. 28–37, 2012.
 [21] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts". *Proceedings of the IEEE international conference on consumer electronics*, pp. 467–468, 2016.
 [22] "A Sustainable Europe by 2030," *European Commission - European Commission*, 02-Sep-2019. [Online]. Available: https://ec.europa.eu/commission/publications/reflection-paper-towards-sustainable-europe-2030_en. [Accessed: 14-Sep-2020].
 [23] "First Circular Economy Action Plan," *First Circular Economy Strategy - Environment - European Commission*. [Online]. Available: <https://ec.europa.eu/>

environment/circular-economy/first_circular_economy_action_plan.html. [Accessed: 14-Sep-2020].

[24] "About the Sustainable Development Goals – United Nations Sustainable Development," United Nations. [Online]. Available: <https://www.un.org/sustainabledevelopment/sustainable-development-goals/>. [Accessed: 14-Sep-2020].

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

I am the sole author of this paper.

Funding:

Not applicable.

Acknowledgements:

The present work is co-funded by the European Union and Greek national funds through the Operational Program "Competitiveness, Entrepreneurship and Innovation" (EPANEK), under the call "RESEARCH-CREATE-INNOVATE" (project code: T1EΔK-05095 and Acronym: TRACKPLAST).

The Relation between Tokens and Blockchain Networks: The Case of Medical Tourism in the Republic of Moldova

Marc Pilkington

University of Burgundy Franche-Comté, France

Correspondence: Marc.Pilkington@u-bourgogne.fr

Received: 15 October 2020 **Accepted:** 10 November 2020 **Published:** 30 November 2020

Abstract

The relation between blockchain tokens and the underlying networks as a determinant of success of use cases in the blockchain space is an insufficiently explored issue in the literature. In the first part, we examine the token/network relation strength of various DLT tourism projects. We find that non-monetary and non-financial use cases perform better than cryptocurrencies, and online coverage is a poor predictor of success. Secondly, we provide preliminary empirical support to blockchain for tourism in the Republic of Moldova, a country, which is interesting insofar as it features nascent medical tourism and blockchain industries with great potential. Thirdly, we further our analysis and investigate the intersection between medical tourism and blockchain technology. We provide evidence that untapped socio-economic potential exists in these sectors.

Keywords: *blockchain, Republic of Moldova, token, medical tourism, health care, use cases*

JEL Classifications: *I11, L83, O14, P27, Z30*

1. Introduction

Tourism is undergoing a wide-ranging process of transformation set in motion by digitalisation [1]. To meet emerging customer needs and build innovative platforms [2], the tourism industry combines money, technology and knowledge. Of particular interest is distributed ledger technology (hereafter DLT), a powerful driver of a technological revolution that creates new opportunities for tourism companies [3].

A blockchain is a distributed, shared, encrypted-database that serves as an irreversible and incorruptible public repository of information. It enables unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority [4].

First, we review token-based versus non-token-based growth drivers in the tourism industry and define a project's token/network relation strength accordingly. We are critical of tokens designed for pure monetary use cases. We analyse a tourism ecosystem-enhancing project on the island of Agistri in 2015, which has not passed the 'smell test' [5] since.

We then look at a failed initial coin offering (ICO) in the loyalty industry that bears resemblance to complementary currency systems. Some use cases are dressed in the clothes of mediatised success stories, but hype is seldom a good predictor of success. We therefore investigate more promising non-native token-based use cases with weaker network/token relation strength.

Secondly, we analyse the results of a small questionnaire-based survey in the Republic of Moldova (hereafter RM), a small and under-researched country where both tourism and blockchain sectors are embryonic. In spite of the small sample, our empirical survey serves as a stepping stone for Part 3.

Finally, we investigate the intersection between DLT and medical tourism, focusing on RM.

Table 1: Analysis of all cited DLT companies (external backing in the endnotes)

Blockchain project	Success/Failure indicator r^i (green, orange, or red)	Relation Strength
Destinia	Customer complaints (BTC acceptability) ⁱⁱ	Medium
CheapAir	\$5,000,000+ processed in BTC payments since 2013 ⁱⁱⁱ	Medium
AirBaltic	Growth in 2017, number of customers using BTC in 2018/2019 was stable ^{iv} .	Medium
Far Eastern Air	Has ceased operations ^v	Medium
aBitSky	Good reviews ^{vi}	Medium
Norwegian Air	Popular; low-cost policy ^{vii}	Medium
Marco Coino	1958 brick-and-mortar merchants listed ^{viii}	Medium
RippleNet	RippleNet Usage Surges 300% In 2020 Q1 ^{ix}	Medium
Nautiluscoin	Dead coin since Nov. 2017	Symbiotic
DT Token	Dead coin since 2017	Symbiotic
Chain of Points	Failed ICO on 31/03/2017	Medium to high
Fizzy (Axa)	Experienced ended in November 2019 ^x	Loose
Buuyers	Buuyers was removed from the Trade and Companies Register on 05/20/2019 ^{xi}	Loose
Microsoft + Webjet	Unveils Rezchain at World Travel Market (11/2019) ^{xii}	Loose
Amadeus IT	«Blockchain is overhyped» Rashesh Jethi, Head of innovation for Airlines ^{xiii}	Loose
Sihatech	Sihatech listed amongst the world's top 10 startups ^{xiv}	Loose

2. Four types of blockchain/token relations

Scholarly controversy exists as to whether or not ‘the coin is an integral part of the network’s incentive mechanism to maintain its security’, and if ‘the two have an existential symbiotic relationship’ [6]. We offer to shed light on this debate in this study. In Proof-of-Work systems, miners contribute to the network, and are rewarded with tokens if they first solve a mathematical puzzle, in order to validate a transaction’ [7]. Yet, not all blockchains are token-based, and not all tokens perform a monetary function [8]. We propose a classification of use cases depending on the strength of the relation between the token and the network: (1) symbiotic, (2) medium-to-high, (3) loose-to-medium and (4) weak. Table 1 features all surveyed DLT companies in this article.

Our clustering method draws on a simplified (and non-computed) Jenks optimization method [9] in order to classify blockchain features by creating homogenous classes, and using natural breaks in data values^{sv}. We provide a novel measurement space in order to quantify the extent to which use cases deploy a native token (a currency application). Our statistical arrangement is structured around two discontinuous discretionary variables (token/network relation strength and success indicator). Hence the value $r = 1$ (i.e. monetary use case) corresponds to a symbiotic relation featuring a native token. By no means does this maximal value imply that the underlying use case is flawless. Frequent flyer miles are a form of near money or quasi money [10]. Blockchain-powered loyalty points are native tokens redeemable in the form of discounts and rewards. Yet one cannot pay directly for the afferent services therewith, hence the value $r=0.8$. Some use cases enable (monetary) payment in BTC (or other cryptocurrencies), but the latter being non-native tokens, these use cases are not symbiotic in the sense defined above; hence, the value $r = 0.5$. Finally, smart contracts (e.g. automated compensation for insurance claims), certification, or record keeping use cases may involve a payment authorization. However, tokens perform a peripheral and non-monetary function, hence our chosen value $r = 0.2$. It may be argued that the statistical data featured in Table 1 and Figure 7 is not directly observable, and therefore difficult to interpret. We disagree with this claim insofar as the numerical assessment of the success/failure of the projects, and the token/network relation, was based on all public information available (press releases, articles and company reports; see fn from ii to xiv in Table 1) and the expertise of the author in the field of DLT.

Symbiotic relation

In the midst of a political crisis in June 2015 following a no-vote to a referendum with prolonged fears of a ‘Grexit’ [11], capital controls and defiance towards the banking sector, the Greek island of Agistri tested a cryptocurrency called Nautiluscoin [12], in order to kick-start the local tourism industry. In spite of the media coverage, the project was short-lived with allegations of scams with ramifications in RM [13]. DLT entrepreneur Antonopoulos has voiced criticism at Nautiluscoin, pointing to its absurdity in a tweet questioning the alleged superiority of a cryptocurrency solution to the Greek crisis over a mere cash-based one (Figure 1). While debunking the Nautiluscoin scam, Miller [14] criticizes the potential of any monetary crypto-instrument to boost tourism on the island of Agistri:

Kelly has struck a deal with the Mayor of Agistri to use the small island as a ‘pilot program’ [...] how will he convince merchants to accept Nautiluscoin? Kelly cites tourism as the vector for promoting Nautiluscoin. I don’t understand how an altcoin will promote tourism. My research indicates the island is already a tourist destination, so let’s assume that’s true. I have to imagine in times of crisis, merchants want what tourists already have: cold, hard cash.

Confirming the predictions of Antonopoulos [15] and Miller [14], Nautiluscoin crashed in late 2017 (Figure 2). DT Token [16], an altcoin issued by a developer affiliated to a Nautiluscoin stakeholder, promising massive discounts and loyalty rewards in the tourism sector, officially

became a dead coin the same year (Figure 3). Both displayed a symbiotic relationship: $r = 1$.



Figure 1: Tweet by Andreas Antonopoulos on 29 June 2015 Source: Twitter



Figure 2: Evolution of the Nautiluscoin price (2015–18) Source: <https://coinmarketcap.com/ko/currencies/nautiluscoin/>

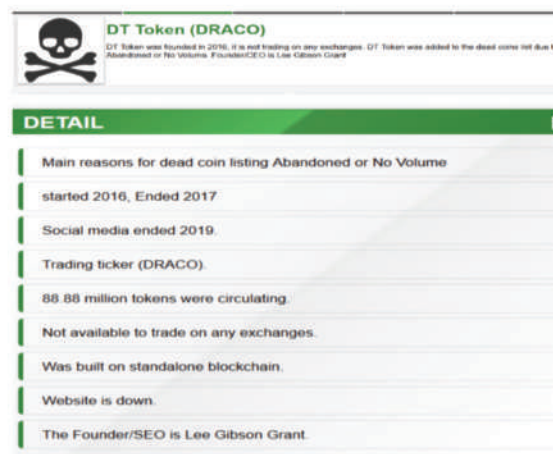


Figure 3: The death of DT Token Source: <https://www.coinopsy.com/dead-coins/dt-token/>

Medium-to-high relations (loyalty schemes)

Hereafter, a medium-to-high relationship $r = 0.8$ is posited for loyalty and rewards. DLT has a transformative potential for improving loyalty programs [17]. Considering that most accumulated points in loyalty programs, always very popular in the tourism sector, worth \$50 billion [18], are never redeemed, the startup Chain of Points had sought to use its own token to incentivize participation in loyalty schemes [19]. Tokenization experiments of loyalty and rewards programs mirror complementary currency systems:

a specific unit (or system) of account that complements the official currency and has been developed by a group of agents (individuals, economic and social structures, local authorities or banks) that has formed a local network with a view to accounting for and regulating exchanges of

goods and services [20].

These ambitious crowdsale announcements eventually proved delusional [21]. Figure 4 shows that the ICO has failed, while www.chainofpoints.com was inactive at the time of writing.


Name	Status	USD Raised	End of ICO	Token Sale Price	Current price	Telegram	Hype	Return(x)	Rating
 Chain of Points	Failed	\$0.00	31.03.2017	50	50			0.000	0

Figure 4: The failure of the Chain of Points ICO
Source: <https://www.icodata.io/ICO>

In Table 2, we document the intensive media coverage of both failed projects received over short periods of time (with $r=1$ and $r=0.8$). In light of these disappointing results, we claim that against the odds, the most fruitful DLT use cases in the tourism sector lie outside the financial and monetary sphere, and display weak or medium relation strength.

Loose-to-medium relation

For the following non-native token-based and financial use cases, $r = 0.5$ (Table 2). In Thailand, tourists are wary of credit card fraud and seek

Table 2: Online coverage for our two (near) monetary use cases

Digital currency project for Agistri island: media sources over a period of three months.	Initial Coin Offering of Chain of Points: pre-ICO period of six weeks
<p>A bitcoin-like solution for Greece CNBC Article 8th of May 2015 by Brian Kelly</p> <p>Drachmae: a Bitcoin-like Solution for Greece's Troubled Economy Bitcoin Magazine 14th May 2015 by Giulio Prisco</p> <p>Drachmae: Could bitcoin-inspired currency be the answer to Greece's economic woes? International Business Times Article 15th of May 2015 by Anthony Cuthbertson</p> <p>Could a digi-drachma avert a Grexit? Reuters BY JEMIMA KELLY June 5th 2015</p> <p>Electronic currency can rescue Greek economy, The Argus by Finn Scott-Delany Tuesday 9 June 2015</p> <p>Worried about Greece holidays? Should you go, where to stay, safety tips - facts to know, Sunday Express Newspaper 3rd July 2015 by FELICITY</p> <p>Greek Economic Crisis: Is A 'Parallel' Currency The Answer?, Forbes 5th of July 2015 Roger Aitken</p> <p>Greek island agrees to test digital currency, CNBC 8th of July 2015 by Brian Kelly</p> <p>Tourists nearly absent for Greece island's peak season, Greek islands, normally packed this time of year, are struggling to get by. CNN's Phil Black reports. 11th July 2015</p> <p>Criptomonedas y Blockchain formarán parte del show televisivo 'Athena' en la isla griega de Agistri, criptonoticias by Jaime Sandoval 24th August 2015</p> <p>Digital currency ecosystem tested on island, TechCityNews 23rd November 2015 Nia Williams</p> <p>Drachmae Preview and Interviews Agistri, Greece ecosystem tested in Agistri, Ikon Media 5th December 2015</p> <p>How Bitcoin Disrupts Telecommunications, 28th February 2016, by Kokkinos Marinou, Cointelegraph</p> <p>Drachmae Project plans blockchain based travel club Token Crowdsale, 2nd May 2016, Hans Lombardo, AllCoinsNews</p> <p>Chainreactor Beta-Testing Permissioned Blockchain with DT-Chain 16th May 2016, Hans Lombardo, Blockchain Finance</p> <p>Is A Blockchain Solution for 'Brexit' Voting & Transparency The Answer? Forbes 5th of July 2015 Roger Aitken</p>	<p>Chain of Points Launches Crowdsale to Help Small Businesses with Loyalty, Finance Magnates, Avi Mizrahi, 18 January, 2017</p> <p>Can Blockchain Help Loyalty Programs? Bitcoin Magazine 27th February 2017 by Michael Scott</p> <p>iPayYou CEO Kavner Joins Blockchain Loyalty Startup Chain Of Points Coin Telegraph 27th February 2017 by William Suberg</p> <p>Chain of Points Announces Start of POINTS Token Crowdsale with 21 Million POINTS Available, Finance Digest (non dated)</p> <p>Blockchain loyalty startup Chain Of Points adds iPayYou CEO to board of advisors Block Tribune Article by David Pimentel 6 March 2017</p> <p>iPayYou Founder Gene Kavner Joins Chain of Points Board of Advisors Finance Magnates by Avi Mizrahi 28th February 2017</p>

merchants accepting Bitcoin [22]. Destinia, in 2013–14, began to list its prices in Bitcoin. Online booking site CheapAir, Latvian national airline AirBaltic, Taiwan's Far Eastern Air [23], aBitSky, Norwegian Air all accept payment in Bitcoin. In Southeast Asia, there is increasing acceptance of Bitcoin Cash [24]. Marco Coino is an application that helps locate brick and mortar stores accepting Bitcoin Cash (Figure 5). With Bitcoin and Bitcoin Cash being already established cryptocurrencies, these use cases are devoid of native blockchain tokens and do not qualify for symbiotic token/network relation. Rather, we opted for medium relation strength (Table 1).

A resilient banking system provides reassurance to tourists, and enhances the competitiveness of tourism destinations. DLT financial applications [25] pertain to compliance costs, clearing and settlement, Know-Your-Client (KYC) and Anti-Money-Laundering (AML), and help strengthen banking operations.

Comment: in spite of substantial media coverage and hype, both projects have failed to live up to expectations.



Figure 5: Bitcoin Cash Map
Source: <https://map.bitcoin.com/>

RippleNet is a global network of more than 300 financial institutions worldwide enabling faster, lower-cost payments. Recently, Ripple Inc. announced an upgrade of RippleNet, and the launch of 'Easy App', a QR code-based application enabling tourists in Thailand to pay for goods and tourism services without needing to change currencies beforehand [26]. Although it uses a native cryptocurrency called XRP, RippleNet is best seen as a challenger of the SWIFT network, relying on established banking institutions and fiat currencies to sustain its cross-border operations ($r = 0.5$).

Weak relation

For smart contracts, review certification, online booking and e-healthcare, $r = 0.2$. Smart contracts are blockchain-powered programmes, for deciding whether an operation should be permitted. They can send an acknowledgement or (non-monetary) token access mechanism to the physical asset, or a user e-wallet, to open a rental car or hotel room [27]. Fizzy [28] was a web and mobile insurance cover experiment for flight delays that ended in November 2019 [29]. The compensation of a loss is no longer based on expert assessments of customer claims, but on data stored on the blockchain. Axa ended the experiment in November 2019.

Travel sites often aggregate reviews and ratings about tourism service providers [30]. These online user-generated reviews tend to dramatically reshape the tourism industry [31]; controversy surrounding verified opinions, distorted rankings, and satisfaction rate authenticity has not ended [32]. Buuyers (Figure 6) set out to offer a customer review management tool, in order to monitor the online reputation. It offered professionals an

innovative and collaborative label that would ensure the most transparent customer relationships. By certifying reviews before registering them on the blockchain, transparency and credibility could have been increased [33].

Microsoft and Webjet have designed a blockchain proof-of-concept travel solution, facilitating booking data processing [34]. The new blockchain called Rezchain powered by Microsoft Azure, consisting in a smart contract solution and data reconciliation service [35], was successfully launched by Webjet [36]. It helps streamline processes, and reduces costs across the industry with substantial reduction in losses associated with transaction disputes. The travel industry has suffered massively from the 2020 coronavirus pandemic; the Webjet share price is nonetheless showing signs of resilience.

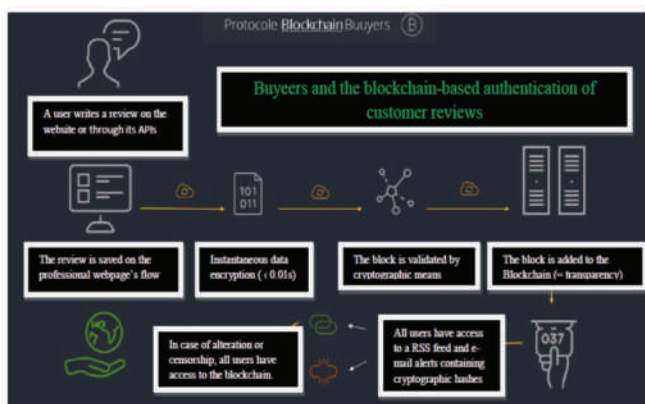


Figure 6 Authentication of customer reviews
Source: Buayers

Authenticity in tourism [37] [38] comes under many forms. Tourists in search of authenticity in a restaurant can keep an eye on the food supply chain [39] [40].

Travelers are required to show their ID at multiple stages of their journey from booking to boarding to checking in at the hotel. DLT increases security while simplifying traveller identification [41].

Gamification is the process of layering game-like features onto a platform. Combined with DLT and mobile services, it enables early-stage innovation and engagement in the creative process [42]. Destination marketing organisations and tourists benefit from gamified mobile experiences [43].

In case of emergency, access to a permissioned blockchain helps detect a competent expert, who has access to the healthcare data remotely in case of a rare condition. Patients can store encrypted vital information and instruct who has access to the private key and the medical information. The ledger stores medical procedures and advanced directives, such as not-to-resuscitate orders [44]. Sihatech is funded by Saudi Aramco (worth \$2 trillion) through the Aramco Entrepreneurship Ventures Fund. Sihatech has built the largest database of private doctors in Saudi Arabia and has launched an elective medical procedure financing module called Jamalek. Sihatech is listed amongst the world's top 10 start-ups [45].

Interpretation: Successful projects cited in this study display weak or loose network/token relation strength. Furthermore, there is no correlation between online coverage measured by Google search results, and the two discretionary variables (success/failure and token/network relation strength).

3. Questionnaire-based survey on DLT in Moldova

We conducted a small online survey on the potential of DLT for tourism in RM for a segment of the tourism industry, namely medical tourism. We

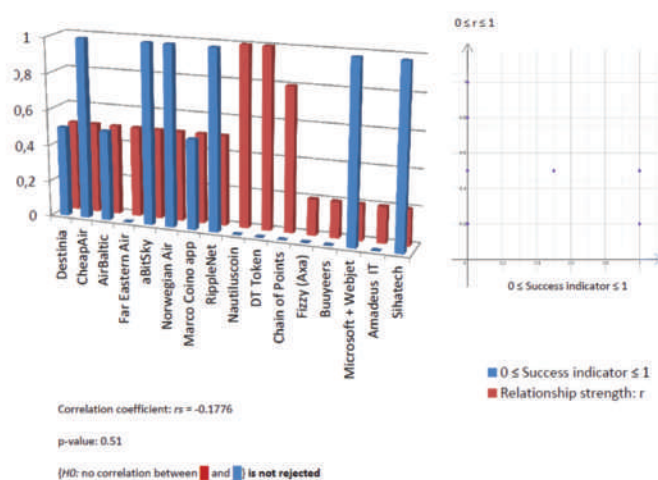


Figure 7: 3D representation of all use cases

collected the answers to ten questions by (only) four respondents, who all hold a senior management function bearing an either direct or indirect relationship to the Moldovan tourism industry^{xxi}. Of course, the small size of the sample prevents us from inferring any statistical significance therefrom. Yet, given a combination of limiting factors such as country size, the embryonic tourism market [46] and the nascent technology [16], the turnout remains acceptable for qualitative research purpose, and justifies the inclusion of the results thereafter. Three respondents admitted to a poor understanding of the technology, against one who claimed to have a good one. Regarding the upgrading potential of business models, the answers were equally split between process automation, enhanced transparency, and improved trust. Regarding the (open-ended) question of the impact of DLT on existing and new business intermediaries in RM, a single respondent stated that some tourism agencies would be compelled to adjust their portfolio of products and tourism services in the future. No respondent stated that their employer currently had a budget for DLT. One stated that it will be the case in the future, and another did not know. To the (open-ended) question of the impact on the level of disintermediation entailed by this technology, one stated a lack of technical knowledge while another thought that disintermediation carried some opportunities. Regarding the potential on medical tourism, the object of the next section, one respondent identified good potential, one believed the contrary, and the two others either did not know, or did not answer. To the question of the potential of blockchain tokens in order to improve the attractiveness of the tourism industry in RM, three did not know what blockchain tokens referred to, and one respondent believed that they could be used as a customized strategic promotion tool for the industry. To the ultimate open-ended question of the main obstacles to technology adoption one respondent stated that DLT implementation is the by-product of a proactive mindset; (s)he mentioned the small size of the market, and lack of knowledge about the technology and its advantages.

4. Medical tourism in Moldova: Can DLTs help?

We now deliberately focus on a non-financial use case. Our selected destination is an audacious bet, voted the least visited country in Europe in 2013 [47]. RM is a rather unknown country with an embryonic tourism sector that could draw on the success of other developing countries, which have succeeded in improving their attractiveness levels, enhancing the welfare of local population [46].

Within four years, Lonely Planet's outlook drastically improved. RM was placed on the hotlist of the best destinations in Europe: 'Europe's final frontier: little visited, lost in time and always surprising'. It warns 'experienced travelers to Europe', likely to be 'amazed and disoriented by Moldova' [48].

A landscape of low, rolling hills and a secretive cave monasteries are a few of the gems you'll discover. The capital Chişinău, is wonderfully slow, but the countryside is where you'll feel most at peace. Take a trip to Orhei, an hour's drive north of Chişinău, for a hike through fields and forests and a glimpse at the sacred Orheiul Vechi. [49]

Starting in 4000 B.C., the Sumerians built a place around a thermal spring, visited by travellers for its healing properties. In India, there have been Yoga and Ayurveda healing techniques for 5000 years, attracting thousands of persons looking for health improvement. In Japan, people have travelled for over 1000 years for medical purposes to the 'Onsen' mineral springs. In Greece, pilgrims used to travel to Epiduria, considered the 'Sanctuary of the healing God – Asklepios'. Starting in the 16th century, Europe became a destination looked for medical tourism, due to roman baths or spa. Amidst the popularity of worldwide travel, a growing number of people are today aligning their trips with healthcare services. The basis of this movement is known as medical tourism. The medical tourist is someone who travels outside the borders of their country, in order to benefit from medical services. This notion excludes expatriates, medical emergencies, and companions of medical tourists. Medical tourism is a particular form of patient mobility, where patients travel across borders or to overseas destination to receive treatments including fertility, cosmetic, dental, transplantation and elective surgery [50]. The scope of medical tourism is widening due to the customization of consumer expectations [51].

There is no consensus on the size of the global medical tourism market. Research companies provide estimates of the market turnover and growth potential. Allied Market Research [x] stated that the global medical tourism market was valued at \$53.77 billion in 2017 and is estimated to reach \$143.46 billion by 2025, registering a 12.9% growth rate from 2018 to 2025. Based on research conducted by this organization, it was estimated that around 20 million people travel across the world each year for medical tourism purposes, spending an average of \$3410 per visit [57]. The global medical tourism market was valued at approximately only USD 15.5 billion in 2017, and is expected to generate revenue of around USD 28.0 billion by the end of 2024, growing 8.8% between 2018 and 2024 [58]. Regardless of these major variations between estimates, we encourage researchers to revise their projections downwards in light of the Coronavirus pandemic [59].

Table 3: Benefits, drivers and consumers expectations
Sources: [52] [53] [54] [55] [56]

Benefits	Drivers	Consumer expectations
Lower cost	Powerful Market-drivers	Quality (real or perceived)
Avoiding queues	Globalization trends	Affordability
New treatments become available	Strength of the demand-side	Availability
Some treatments are illegal at home	Empowered patient base	Accessibility
Welfare-enhancing sector, source of comparative advantage for developing countries	ICT revolution	Trust in the staff and clinic
Faster adoption of innovation	Decreasing cost of travel and transport liberalization	Confidentiality

In February 2020, the Medical Tourism Association [61] organized a webinar titled 'The Coronavirus & Its Impact to Medical Tourism', in which Karen Timmons, CEO of Global Healthcare Accreditation, warned against the slowdown of airlines resulting in unprecedented levels of diligence for the risk of travelling. In the context of a pandemic, high-quality accreditation will become a sine qua none for travel agencies offering medical tourism services so as to ensure compliance with WHO

guidelines and national health regulatory standards. The impact of the pandemic is likely to be enormous as periods of quarantine before entering some countries might deter medical tourists in the future. In a post-COVID-19 world, countries will undergo massive training efforts by health professionals, and implement procedures related to infection control of travellers. Compliance with health standards will become the new markers of competitiveness. In this respect, small medical facilities will come under closer scrutiny [61].

Medical tourism in RM is a nascent and unstructured industry. We present hereafter the relevant data supplemented by a SWOT analysis, and draw some perspectives. Data in Table 4 was obtained on the website of the National Bureau of Statistics that publishes yearly information on all tourism agencies and tour-operators providing tourism services in RM. Tourist flows are broken down into (1) recreational and leisure purposes, (2) business and professional, and (3) treatment. The website of the statistical Bank (another state institution) provides detailed information about the activity of travel agencies and tour operators, by purpose of visit, from 2000 to 2019.

Table 4: Statistics on medical tourism (2015–2019)

Year	% of total incoming tourism	Number of medical tourists
2015	3.1	480
2016	3.9	612
2017	4.5	788
2018	3%	584
2019	2.8	550

Table 5: Strengths/Weaknesses/Opportunities/Threats analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> Medpark in Chişinău is a worldclass hospital Rich tradition of providing health-related services in Central and Eastern Europe: medical, therapeutic and wellness (Smith et al. 2016). In former USSR, the dignitaries from the regime used to come to Moldova to receive treatment (it enjoyed the best healthcare system of all socialist republics) Some hospitals / private clinics take foreign patients. Dental medical tourism is popular among foreigners. Dental services cheaper than other European countries <p><u>Example of prices</u></p> <ul style="list-style-type: none"> The restoration of frontal tooth - EUR 63 Ceramic crown - EUR 180 Tooth whitening /bleaching - EUR 73 Dental implant - up to EUR 300. 	<ul style="list-style-type: none"> 3 and 5% of the total market, absence of any blatant growth trend, not very popular at the moment, total of 100 hospitals in RM, a handful (all private) offer high quality internationally competitive health services. Medical tourism went unnoticed in Moldova Competitiveness Project funded by USAID / government of Sweden: "the tourism sector could grow 10-fold in the next 10 years, contributing up to 3% in GDP growth by stimulating business development, job creation and attracting foreign tourist dollars". The best healthcare system under USSR has suffered from corruption practices in the faculties of medicine
Opportunities	Threats
<ul style="list-style-type: none"> Current potential: between 500 and 1000 / year Coronavirus crisis (restructuring of the tourism industry; massive public and private investment to help health establishment obtain international accreditations), ANTRIM offering legal assistance to tour agencies On 19/03/2020, Prime Minister Ion Ciucu announced a list of measures that will be taken to help business entities from RM during the pandemic situation blockchain technology pivotal to the transformation of the medical tourism sector (confidential health records) ANTRIM is currently reconsidering its promotional strategy which could be beneficial to medical tourism. "more creative solutions are needed" (Turcanu, 2020) State U of Medicine & Pharmacy "N. Testemiţanu", very popular among foreign students, much cheaper than any other European country, e.g. undergraduate studies cost €2900-3500. Fees for preparatory language courses and other materials needed not included 	<ul style="list-style-type: none"> Some private clinics double prices for foreigners Coronavirus : slowdown of airlines, travel and tourism industry = most affected industry worldwide, expected losses in the range of millions of lei (Turcanu, 2020), quarantine for travelers upon arrival, fear of traveling, etc. Fiscal crisis: the pandemic has depleted the fiscal resources of the State (Ciucu cited in ipn, 2020) that requested an emergency loan (IMF, 2020), impeding massive public and private investment (see opportunities). Fragile parliamentary alliances, recurrent political uncertainty, formerly under oligarchical rule

After one year of evaluation and with 1500 indicators tested, Medpark International Hospital, a Chisinau private hospital was the first medical institution to become Joint Commission International accredited in 2014, in RM, and in Eastern Europe with 94 out of 100 points, a near-perfect score [62]. Dr Olga Schiopu Medical Director of Medpark describes the outstanding modern facilities of this cutting-edge establishment that includes four specialized operating theatres (cardiac surgery, neurosurgery, trauma and general surgery) and an in vitro Fertility Centre. There is a high level of medical expertise of doctors who have all undergone postgraduate training in elite universities in Europe or North America. The cardiac centre offers treatment against acute myocardial infarction and cardiac surgery). Other popular areas of intervention include hip replacement and ophthalmology.

Medpark International Hospital is a top destination on medical tourism market. This is possible due to advantages such as accessibility in terms of transportation (air, road), highly qualified medical staff, state of the art medical equipment, comprehensive care under one roof, care for the patient, affordable prices and the list could go on [63].

Another asset of RM is the excellent language skills characteristic of an educated workforce. At Medpark, doctors communicate with patients in English, Romanian, Russian, and Turkish. Other languages are made available upon payment of an interpreter's fee [63]. Dr Schiopu recognises that the biggest challenge facing the growth of medical tourism in RM is reassurance about the country, its safety for travel and tourism purposes. In this regard, the initiative of Moldova Tours 2.0 [46] is timely and welcome, as it sets forth to promote tourism and educate people about what RM, once the least visited country in Europe [47], has to offer. With the help of video calls and exchange of information prior to the first visit, the pricing of healthcare services for medical tourism purposes (for complex surgery) could be more accurate and reinforce trust. As explained by the Medical Tourism Quality Alliance [64]:

Patients looking for medical care and treatment abroad need accurate up-to-date reliable information. Whether a website or a medical tourism company can provide the sort of information that will answer concerns about best quality or high standards of patient safety and care management is often a concern. Some patients consider accreditation status and word of mouth recommendations before they make their choice of hospital, it's a definite improvement over relying only on the internet for information or choosing the lowest cost.

5. DLT solutions and Electronic Health Records (EHR)

Not all consumption of healthcare services abroad is medical tourism, for instance, the occurrence of emergencies while travelling abroad. Clinicians often find themselves in a critical, if not perilous, situation when lacking any health record on their foreign patient. The delivery of quality healthcare is always at stake, and in some emergency situations, human lives are too [44]. When a person is travelling outside their home country, and is treated for an emergency, a blockchain ledger could help detect a competent expert, who would have access to the healthcare data remotely in case of a rare condition. Due to privacy concerns related to EHRs, patients could store encrypted (therefore confidential) vital information on blockchain-powered Internet-of-Things (IoT) medical devices, and instruct who has access to the private key and the patient's medical information. It could store medical procedures and more advanced directives, such as not-to-resuscitate orders [65]. This amounts to patient-centric care (the self-management of healthcare conditions by patients). The stakes are high both for healthcare clinicians and patients: 'in modern societies, cultures and organized groups, the dissemination of medical data has been perceived to be a breakthrough for the discovery of new techniques and therapies for curing diseases' [66]. How about digitising currency circulating in the health micro-economy? Abid Hospital in Islamabad, Pakistan, was the first Asian hospital to accept the PakCoin cryptocurrency. Technological feat is never an end in itself; this unique experiment had no impact on healthcare quality and medical tourism flows. A more effective application would

be to reach out to the unbanked population [67]. In a post-COVID-19 world wherein pockets of poverty are expected to worsen, the reinvention of tourism shall involve this massive segment of the world population. Blockchain tokens prove useful by helping store and securely transfer patient-related and legal information. Usually, the healthcare provider, not the patient, retains access to past data. The siloed nature of healthcare data scattered across various healthcare organisations poses the issue of interoperability between different healthcare providers. Of course, issues of fragmentation and lack of cohesiveness of health records are not limited to medical tourism in developing countries, as they also pertain to large and developed countries such as the USA: 'it's no exaggeration to say that our EHR systems' lack of interoperability is the single strongest barrier to nationwide population health management' [68]. MedRec is a decentralised EHR management system [69]. EHRs are signed digitally, thereby ensuring the existence of an unaltered copy. It is the signature, not the record itself, which is stored on the blockchain ledger. MedRec notifies to the patient the read and write permissions over the EHR. A cryptographic hash of the record protects against tampering, thereby guaranteeing data integrity to all network participants. The block content is made of healthcare data ownership and viewership permissions, while the healthcare community forms the thrust of P2P network. The objective of MedRec is to develop a user-friendly interface that simplifies direct interaction between patients and EHRs that span over different healthcare providers. The next step will be to increase the complexity level of the interface by introducing a richer dataset comprising more data types, contributors and users. DLT, through a decentralized control mechanism, allows the healthcare system to do away with another layer of middlemen, and enhances the control of the patient over medical data. Furthermore, healthcare blockchain ledgers become time-stamped, auditable and programmable with the help of Ethereum-based smart contracts that help automate and track state transitions (e.g. change in viewership rights and entry of a new record in the system).

Digital identity, paramount in healthcare management can be tackled today by DLT [70], is enhanced by the association of widely accepted forms of identity with public key cryptography [71]. After referring a blockchain to confirm permissions via the database authentication server, a syncing algorithm handles 'off-chain' data exchange between a patient database and a provider database [72]. The use of multiparty off-chain channels solves the scalability problem of the Ethereum blockchain and, by extension, other blockchains [71]. Given the size of EHR, this breakthrough proves useful for the incentivisation and enforcement of smart contracts between actors of the healthcare system across institutions and countries. The adoption of DLT could help promote decentralized medical travel solutions, and improve HER management. Health connected objects could foster smart medical devices. For instance, a surgical device linked to a blockchain through a smart contract could trigger preventive maintenance. IoT-enabled temperature loggers would transmit the temperature parameters of drugs to a blockchain during shipment, while a smart contract monitors its stability. DLT could help create tamperproof certificates of medical necessity in a trustless environment, thereby stipulating which healthcare services are necessary for the patient by a certified clinician. IoT devices and blockchain smart contracts can become tools facilitating diagnosis [73] when connected to a machine-learning algorithm (e.g. glucose levels and diabetes). DLT-powered EHR are well adapted to cloud-based environments, which have attracted substantial interest from patients, health institutions and researchers alike [74].

Concluding remarks

We have shed light on the ongoing debate in DLT research of an existential symbiotic relationship between the token and the network [6]. We have provided a counter-intuitive and evidence-based view by arguing that promising tourism use cases lie outside the monetary and financial sphere. The expansion of the DLT space has paved the way for a wide range of non-monetary use cases displaying looser relation strength. A multitude of use cases with a weak relation draw on the capability to securely store

and transfer information/data. In Table 1, successful projects display weak or loose token/network relation strength. After conducting a correlation test, the null hypothesis ($r_s = 0$, no correlation between relation strength and success indicator) is not rejected (Figure 7). These preliminary results warrant caution as correlation and/or lack thereof do not imply causation. Room exists for future successful monetary use cases in the tourism sector, although we wish to warn against media hype.

In medical tourism, lower medical costs, international accreditations, competent and multilingual doctors are the building blocks of enhanced attractiveness. In the French philosophical tradition of Althusser [75], the infrastructure, namely the economic base, is the foundational layer of the social system while the superstructure (i.e. the upper layers) is both the essence of the visible structure and the ideological governance of the infrastructure. Along these lines, the evolution of the infrastructure determines that of the superstructure. Arguably, Nakamoto [76] favours the opposite stance with his ground-breaking analysis of decentralisation. In the case at hand, the infrastructure, namely healthcare facilities and professionals, is determined by the superstructure, namely organisational protocols and technological projects. We note that the superstructure of RM still lacks a decentralised technological layer pivotal in creating an environment of trust and transparency; hence, our rationale for blockchain technology.

Finally, let us mention the 2020 coronavirus pandemic:

At this moment we are realistic: now is not the right time to travel to and from many places. All travelers should follow government advice and as a further measure consider if their journey is responsible and essential in the current context [77].

Vicol and Mogildea [78] explain that an EU-wide recession will reduce exports and remittances, and put pressure on the national currency. Yet, 'the tourism sector, like no other economic activity with social impact, is based on interaction amongst people' [79]. RM would hence benefit from an organizational platform channelling the forces capable of combining DLT, big data analytics, cloud storage and IoT medical devices in a creative fashion, thereby conducive to welfare-enhancing innovation based on data-sharing, higher accessibility and an attractive medical tourism sector.

References:

- [1] A. I. Ozdemir, I. M. Ar and I. Erol, "Assessment of Blockchain Applications in Travel and Tourism Industry", *Quality & Quantity*, pp. 1–15, 2019.
- [2] I. Önder and U. Gunter, "Blockchain: Is it the Future for the Tourism and Hospitality Industry?", *Tourism Economics*, 2020, September. Available: [10.1177/1354816620961707](https://doi.org/10.1177/1354816620961707).
- [3] E. Colombo and R. Baggio, "Tourism Distribution Channels: Knowledge Requirements", in *Knowledge Transfer to and within Tourism: Academic, Industry and Government Bridges*, N. Scott, M. De Martino and M. Van Niekerk, Ed. Bingley, UK: Emerald, 2017, pp. 289–301.
- [4] A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015. Available at SSRN: <https://ssrn.com/abstract=2580664>.
- [5] R. Solow, "Building a Science of Economics for the Real World", *House Committee on Science and Technology*, July 20, 2010.
- [6] T. Swanson, "Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems". Working Paper, 6 April, p. 8, 2015. Available: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers>.
- [7] M. Pilkington, "Blockchain Technology: Principles and Applications", in *Handbook of Research on Digital Transformations*, Chapter 11, F. Xavier Olleros and Majlinda Zhegu. Cheltenham: Edward Elgar, 2016, p. 228.
- [8] P. Tasca and C. J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification", *Ledger*, vol. 4, 2019.
- [9] G. F. Jenks, "The Data Model Concept in Statistical Mapping", *International Yearbook of Cartography*, vol. 7, pp. 186–190, 1967.
- [10] M. Chan, S. Kemp and J. Finsterwalder, "The Concept of Near-Money in Loyalty Programmes", *Journal of Retailing and Consumer Services*, vol. 31, pp. 246–255, 2016.
- [11] C. Ziotis, P. Tugwell and N. Chrysoloras, "Greece Imposes Capital Controls as Fears of Grexit Grow", *Bloomberg*, 29 June, 2015. Available: <https://www.bloomberg.com/news/articles/2015-06-29/greece-imposes-capital-controls-banks-close-to-contain-fallout-ibb781b7>.
- [12] B. Kelly, "Greek Island Agrees to Test Digital Currency", *CNBC*, 8 July, 2015. Available: <https://www.cnn.com/2015/07/08/greek-island-agrees-to-test-digital-currency-commentary.html>.
- [13] *Bitcoin cryptocurrency.com*, "CNE Drachmae Market: Moldova's Cryptocurrency Exchange?", 2020. Available: <https://bitcoincryptocurrency.com/cne-drachmae-market/>.
- [14] N. Miller, "Is Nautiluscoin a Scam?", 11 July, 2015. Available: <https://www.cnn.com/is-nautiluscoin-a-scam/>.
- [15] Antonopoulos, "Tweet", 29 June, 2015. Available: <https://twitter.com/aantonop/status/615571506630905856>.
- [16] M. Pilkington, R. Crudu and L. G. Grant, "Can DLT and Bitcoin Lift a Country Out of Poverty? The Example of the Republic of Moldova", *International Journal of Internet Technology and Secured Transactions*, 2017.
- [17] D. Kowalewski, J. McLaughlin and A. Hill, "Blockchain Will Transform Customer Loyalty Programs", *Harvard Business Review*, March 14, 2017.
- [18] S. Crnojevi and I. Katzela, "Chain of Points: Transforming Loyalty into Rewards", *White Paper*, 2017. Available: https://chainofpoints.com/cop_whitepaper.pdf.
- [19] S. Anderson, "Nearly Four Billion Customers in Loyalty Programs", *Payment Week*, 5 March, 2017. Available: <https://paymentweek.com/2017-7-5-nearly-four-billion-customers-loyalty-programs/>.
- [20] M. Fare and P. O. Ahmed, "Why Are Complementary Currency Systems Difficult to Grasp within Conventional Economics? *Revue Interventions économiques*", *Papers in Political Economy*, vol. 59, 2018.
- [21] M. Pilkington, "The Emerging ICO Landscape - Some Financial and Regulatory Standpoints", February 8, 2018. Available at SSRN: <https://ssrn.com/abstract=3120307>.
- [22] K. Helms, "Bitcoin Adoption in Thailand Led by Tourism Industry", *Bitcoin.com*, 18 April, 2017. Available: <https://news.bitcoin.com/bitcoin-adoption-thailand-tourism-industry-scaling-debate/>.
- [23] A. Costello, "Travel Sites that Accept Cryptocurrencies", *blogpost*, 23 November, 2019. Available: <https://medium.com/bashmart-blog/travel-sites-that-accept-cryptocurrencies-d1ad55c6bd0a>.
- [24] L. Tassev, "These Tourist Destinations Welcome Bitcoin Cash Enthusiasts", *Bitcoin.com*, 25 May, 2019. Available: <https://news.bitcoin.com/these-tourist-destinations-welcome-bitcoin-cash-enthusiasts/?omhide=true>.
- [25] Deloitte, "Blockchain: An Introduction and Use-Cases", 12 June, 2018. Available: <https://www2.deloitte.com/content/dam/Deloitte/be/Documents/finance/BE-Blockchain%20for%20the%20financial%20industry.pdf>.
- [26] J. Simmons, "Thailand's Largest Bank Works on Ripple Based App for Tourists", 27 March, 2020. Available: <https://www.crypto-news-flash.com/thailands-largest-bank-works-on-ripple-based-app-for-tourists/>.
- [27] M. Swan, *Blockchain: Blueprint for a New Economy*. Cambridge, MA: O'Reilly Media, 2015.
- [28] Axsa, "Fizzy, Smart Insurance. Automatic Compensation", 13 September, 2017. Available: https://www.youtube.com/watch?v=xJZuZ_CMI.
- [29] J. Raynal, "Clap de fin pour Fizzy, l'application phare d'Axsa dans la Blockchain", 8 November, 2019. Available: <https://www.latribune.fr/entreprises-finance/banques-finance/assurance/clap-de-fin-pour-fizzy-l-application-phare-d-axsa-dans-la-blockchain-832676.html>.
- [30] M. Bassig, "Hoteliers and Tourism Business Owners: Travel, Tourism, and Hotel Review Sites You Should Monitor?", *Review Trackers*, 13 November, 2012. Available: <https://www.reviewtrackers.com/hoteliers-tourism-business-owners-travel-tourism-hotel-review-sites-monitor/>.
- [32] R. Weston, H. Hamel, M. Balas, R. Denman, A. Pezzano, G. Sillence, K. Reiner, A. Grebenar and M. Lawler, "Research for TRAN Committee – European Tourism Labelling, European Parliament", *Policy Department for Structural and Cohesion Policies*, Brussels, 2018. Available: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/617461/IPOL_STU\(2018\)617461_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/617461/IPOL_STU(2018)617461_EN.pdf).

- [33] Finyear, "Buyers: la blockchain garantit la fiabilité des avis clients", 21 July, 2016. Available: http://www.finyear.com/Buyers-la-blockchain-garantit-la-fiabilite-des-avis-clients_a36787.html.
- [34] Microsoft, "Webjet and Microsoft Build First-of-a-Kind Travel Industry Blockchain Solution", November 8, 2016. Available: https://news.microsoft.com/en-au/2016/11/08/webjet-and-microsoft-build-first-of-a-kind-travel-industry-blockchain-solution/#_ftn1.
- [35] Microsoft, "Webjet Uses Blockchain to Simplify Transaction Disputes in the Travel Industry", 30 March, 2018. Available: <https://customers.microsoft.com/fr-fr/story/webjet>.
- [36] Webjet, "News Release, Webjet Launches Rezchain, New Blockchain Technology Enables Error Free Hotel Bookings", 7 November, 2019. Available: <https://webbedsuploadstorage.blob.core.windows.net/uploads/2019/10/Rezchain-WTM-Launch-Release.pdf>.
- [37] L. Lu, C. G. Chi and Y. Liu, "Authenticity, Involvement, and Image: Evaluating Tourist Experiences at Historic Districts", *Tourism Management*, vol. 50, pp. 85–96, 2015.
- [38] F. A. Salamone, "Authenticity in Tourism: The San Angel Inns", *Annals of Tourism Research*, vol. 24, pp. 305–321, 1997.
- [39] L. Coleman, "Ethereum-Based Swiss Blockchain Startup Readies Tech for the Food Supply Chain", *cryptocoinsnews.com*, 26 April, 2017. Available: <https://www.cryptocoinsnews.com/ethereum-foodblockchainxyz-supply-chain/>.
- [40] P. Rizzo, "An Asia-Pacific Blockchain Consortium is Forming around Food Supply Chain", *CoinDesk*, May 22, 2017. Available: <http://www.coindesk.com/pwv-teams-up-with-alibaba-for-food-supply-blockchain-test/>.
- [41] Amadeus IT Group, "Blockchain for Travel", 18 October, 2017. https://www.youtube.com/watch?v=YpS0zgj9wCU&feature=emb_logo.
- [42] R. Patricio, A. C. Moreira and F. Zurlo, "Gamification Approaches to the Early Stage of Innovation", *Creativity & Innovation Management*, vol. 27, no. 4, pp. 499–511, 2018. Available: <https://doi.org/10.1111/caim.12284>.
- [43] J. Swacha, "Architecture of a Dispersed Gamification System for Tourist Tractions", *Information*, vol. 10, no. 1, p. 33, 2019.
- [44] M. Scott, "The Blockchain and Global Health", *Nasdaq.com*, 9 May, 2017. Available: <http://www.nasdaq.com/article/the-blockchain-and-global-health-cm786796#ixzz4jgi3NSUN>.
- [45] Zanya, "Sibatech Listed Amongst the World's Top 10 Startups", Press Release, 13 November, 2019. Available: https://www.zanya.com/mena/en/press-releases/story/Sibatech_listed_amongst_the_worlds_top_10_startups-ZAWYA20191113082106/.
- [46] M. Pilkington, "Tourism for Development in the Republic of Moldova: Empowering Individuals and Extending the Reach of Globalization through an Innovative 2.0 Digital Platform", in *Handbook of Research on Individualism and Identity in the Globalized Digital Age*, Francis Sigmund Topor, Ed. Japan: Keio University. IGI Global E-Editorial Discovery, 2016, pp. 500–531.
- [47] Pettersen, "Moldova: Embracing Its Status as Europe's Least-Visited Country", *Lonely Planet*, 2 July, 2013. Available: <https://www.lonelyplanet.com/articles/moldova-embracing-its-status-as-europes-least-visited-country>.
- [48] Lonely Planet, "Best in Europe, Our Hotlist of European Destinations", 2017. Available: <https://www.lonelyplanet.com/best-in-europe>.
- [49] J. Bishop, "The 10 Best Places to Visit in Europe in 2017", 23 May, 2017. Available: <https://www.forbes.com/sites/bishopjordan/2017/05/23/best-places-to-visit-in-europe/#50ba7a133bdc>.
- [50] N. Lunt, D. Horsfall and J. Hanefeld, "Medical Tourism: A Snapshot of Evidence on Treatment Abroad", *Maturitas*, vol. 88, pp. 37–44, 2016.
- [51] I. G. Cohen and E. Prall, "Medical Tourism", in *The Wiley Blackwell Encyclopedia of Consumption and Consumer Studies*, T. Cook and J. M. Ryan Ed. Chichester: WileyBlackwell, 2015, p. 168. Available: 10.1002/9781118989463.wbecs168.
- [52] V. Rannels and P. M. Carrera, "Why Do Patients Engage in Medical Tourism?", *Maturitas*, vol. 73, no. 4, pp. 300–304, 2012.
- [53] J. Y. Han, E. M. Choi and K. Y. Ji, "An Analysis of the Importance-Satisfaction of Convergent Medical Tourism Service Quality", *Journal of Digital Convergence*, vol. 13, no. 7, pp. 403–412, 2015.
- [54] J. Connell, "Contemporary Medical Tourism: Conceptualisation, Culture and Commodification", *Tourism Management*, vol. 34, pp. 1–13, 2013.
- [55] C. L. Andrei, G. Tigu, R. M. Dragoescu and C. J. Sinescu, "Analysis of Medical Tourism for Cardiovascular Diseases", *Amfiteatru Economic Journal*, vol. 16, no. 8, pp. 1136–1150, 2014.
- [56] A. Labowiecki-Vikuk and D. Dryglas, "Medical Tourism Services and Medical Tourism Destinations in Central and Eastern Europe—the Opinion of Britons and Germans", *Economic Research-Ekonomska istraživanja*, vol. 32, no. 1, pp. 1256–1274, 2019.
- [57] Allied Market Research, "Medical Tourism Market by Treatment Type (Dental Treatment, Cosmetic Treatment, Cardiovascular Treatment, Orthopedic Treatment, Neurological Treatment, Cancer Treatment, Fertility Treatment, and Others): Global Opportunity Analysis and Industry Forecast, 2018–2025", January, 2019. Available: <https://www.alliedmarketresearch.com/medical-tourism-market>.
- [58] Edelheit, "State of the Medical Tourism Industry", 2020. Available: <https://www.magazine.medicaltourism.com/article/state-of-the-medical-tourism-industry>.
- [59] Zion Market Research, "Medical Tourism Market by Treatment Type (Cancer Treatment, Orthopedic Treatment, Fertility Treatment, Cardiovascular Treatment, Neurological Treatment, and Others): Global Industry Perspective, Comprehensive Analysis and Forecast, 2017–2024", Press Release, 22-June, 2018. Available: <https://www.zionmarketresearch.com/report/medical-tourism-market>.
- [60] Express Healthcare, "COVID-19 Proving Fatal for Medical Tourism Industry", 1 April, 2020. Available: <https://www.expresshealthcare.in/covid19-updates/covid-19-proving-fatal-for-medical-tourism-industry/418100/>.
- [61] Medical Tourism Association, "The Coronavirus & Its Impact to Medical Tourism", Youtube video, 13 February, 2020. Available: https://www.youtube.com/watch?time_continue=1670&v=6FujalPhz5Q&feature=emb_logo.
- [62] G. Pramod, "Medpark Is the First and Only JCI Accredited Medical Facility in Moldova", 15 August, 2014. Available: <https://www.placidway.com/article/1453/Medpark-Is-the-First-and-Only-JCI-Accredited-Medical-Facility-in-Moldova>.
- [63] PlacidWay, "Interview with Dr. Olga Schiopu Medical Director of Medpark International Hospital", 11 December, 2013. Available: <https://www.placidway.com/article/1347/Interview-with-Dr-Olga-Schiopu-Medical-Director-of-Medpark-Moldova>.
- [64] Medical Tourism Quality Alliance, "Getting the Best Care and Best Value in Medical Tourism", 2020. Available: <https://mtqua.org/medical-tourism-quality>.
- [65] C. M. Angst and R. Agarwal, "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion", *MIS Quarterly*, vol. 33, no. 2, pp. 339–370, 2009.
- [66] Q. Xia, E. B. Sifab, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain", *IEEE Access*, vol. 5, pp. 14757–14767, 2017. Available: 10.1109/ACCESS.2017.2730843.
- [67] A. Zubair, "Abid Hospital in Pakistan becomes the First Asian Hospital to Accept Cryptocurrency", *Pakwired*, 10 March, 2017. Available: <https://pakwired.com/abid-hospital-becomes-first-asian-hospital-to-accept-cryptocurrency/>.
- [68] G. D'Arcy Guerin, "Could DLT Be the Answer to Health IT Interoperability?", *HIT Consultant*, 23 March, 2017. Available: <http://bitconsultant.net/2017/03/23/blockchain-technology-healthcare-it-interoperability/>.
- [69] A. A. Ekblaw, J. Halamek and A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data", 2016.
- [70] G. Wolfond, "A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors", *Technology Innovation Management Review*, vol. 7, no. 10, 2017.
- [71] V. Buterin and J. Poon, "Plasma: Scalable Autonomous Smart Contracts", *White Paper*, 2017. Available: <http://plasma.io/plasma.pdf>.
- [72] A. Khatoun, "A Blockchain-Based Smart Contract System for Healthcare Management", *Electronics*, vol. 9, no. 1, p. 94, 2020.
- [73] R. Krishnamurthy, "The Voyage of Discovery: Blockchain for Pharmaceuticals and Medical Devices", *Beyond Standards is brought to you by the IEEE Standards Association*, 17 April, 2017. Available: <https://beyondstandards.ieee.org/general-news/voyage-discovery-blockchain-pharmaceuticals-medical-devices/>.
- [74] M. R. M. Assis, L. F. Bittencourt and R. Tolosana-Calasanç, "Cloud Federation: Characterisation and Conceptual Model", *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility Cloud Computing (UCC)*, pp. 585–590, December, 2014.
- [75] L. Althusser, *Idéologie et appareils idéologiques d'État* (pp. 263–306). Presses Universitaires de France, 2011.
- [76] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[77] Lonely Planet, "Ask Tom: Lonely Planet Expert Answers Your Pressing Travel Questions in Light of the Coronavirus Pandemic", Tom Hall, 12 March, 2020. Available: <https://www.lonelyplanet.com/articles/expert-travel-advice-coronavirus-covid-19>.

[78] D. Vicol and M. Mogildea, "Economic Impact of COVID-19: What Can We Expect in the Case of Moldova? Op-Ed", *ipn*, 21 March, 2020. Available: https://www.ipn.md/en/economic-impact-of-covid-19-what-can-we-expect-in-7978_1072344.html.

[79] UNWTO, "COVID-19, Putting People First", 2020. Available: <https://www.unwto.org/tourism-covid-19>.

Competing Interests:

Founder and Owner of Moldova Tours 2.0 (cited in the paper)

Ethical approval:

Not applicable.

Author's contribution:

I have conducted the totality of the research.

Funding:

None declared.

Acknowledgements:

Thank you to the respondents of the online blockchain survey in Moldova, MedPark Hospital for sending me updated information (for the COVID-19 crisis) and the JBBA reviewers for helping me improve this manuscript.

ⁱ $0 \leq r \leq 1$

ⁱⁱ https://www.reddit.com/r/Bitcoin/comments/8c8hc7/destinia_claim_they_accept_bitcoin_for_flights/

ⁱⁱⁱ <https://www.forbes.com/sites/lukefitzpatrick/2019/04/25/cheapair-to-accept-ethereum-payments/#d20deb7515dd>

^{iv} <https://www.phocuswire.com/Bitcoin-travel-companies>

^v <https://www.ch-aviation.com/portal/news/84297-taiwans-far-eastern-air-transport-ceases-operations>

^{vi} https://www.reddit.com/r/btc/comments/451il3/my_experience_with_abitsky/

^{vii} <https://www.bitcoin-accepted.com/bitcoin-now-accepted-norwegian-air/>

^{viii} <https://map.bitcoin.com/>

^{ix} <https://www.thecryptoassociate.com/riplenet-usage-surges-300-in-2020-q1/>

^x <https://www.latribune.fr/entreprises-finance/banques-finance/assurance/clap-de-fin-pour-fizzy-l-application-phare-d-axa-dans-la-blockchain-832676.html>

^{xi} <http://entreprises.lefigaro.fr/buyers-75/entreprise-792584872>

^{xii} <https://www.webbeds.com/webjet-limited-unveils-rezchain-at-wtm/>

^{xiii} <https://www.phocuswire.com/Technology-travel-experience>

^{xiv} https://www.zawya.com/mena/en/press-releases/story/Sihatech_listed_amongst_the_worlds_top_10_startups-ZAWYA20191113082106/

^{xv} A proper application of the Jenks optimisation method would require the minimisation of the squared deviations of each class means according to a pre-specified algorithm. However, our fixed choice of discretionary variables prevents us from calculating any intra-class standard deviation. We leave the refinement of this statistical treatment for future research as the number of tourism use cases and statistical observations expand.

^{xvi} The results of the questionnaire are available in Romanian here <https://docs.google.com/forms/d/1tQt9OVqyhBrMTz3aCttw9yNZT5ryIEvPeIRkdN6Qaw1/edit#responses>

Blockchain is dead! Long live Blockchain!

Joshua Ellul

Centre for Distributed Ledger Technologies, University of Malta

Correspondence: joshua.ellul@um.edu.mt

Received: 16 January 2021 **Accepted:** 14 March 2021 **Published:** 25 March 2021

Abstract

A decade on since Satoshi's Bitcoin paper, Blockchain is now considered to be sliding into the trough of Gartner's hype cycle. Claims in regard to Blockchain and Cryptocurrencies being dead are on the rise, whilst at the same time many claim the contrary. The vague statement encapsulates many different aspects and perspectives of a myriad of use cases, technology and platforms including both the technique as a whole and as individual instantiations.

In this paper, we unpack the statement, break it down and investigate objectively concrete factors which provide indication in regard to whether Blockchain is dead. We examine metrics including budgets and investment; company registries and data; community engagement, projects and source code repositories; academic research and programmes; social media posts; and public interest. We individually demonstrate metrics that indicate the respective measures' healthy activity and come to the conclusion that the collective statement 'Blockchain is dead' does not hold. A clear message extracted from the work proposed herein is that success is achieved where the community comes together rather than works in isolation.

Keywords: *blockchain, ecosystem, research, investment, analysis*

JEL Classifications: *A12*

1. Introduction

'Blockchain is dead?' – a question or statement which many have asked or claimed since the (first) 2017 rise and fall of Bitcoin and other cryptocurrencies. Is it the case that the blockchain field and related sectors are indeed dead? According to Gartner blockchain is now sliding into its hype cycle's Trough of Disillusionmentⁱⁱ in 2020 – depicted and expanded on in Figure 1. Will the technology make its way up the Slope of Enlightenment or will it exit towards its death? To answer the question of whether or not blockchain is dead and/or on its way there, we first need to understand what we mean by it and how we can determine the answer. In this paper, we aim to provide insight in regard to whether this is the case by investigating a number of different facets of the blockchain sector.

Whilst, death implies a permanent state of inactivity, a looser meaning will be used to determine whether or not blockchain is dead – if activity within the sector is drastically reduced (even if temporary) then for the sake of reaching a conclusion in the current period under investigation it will be assumed that it is dead or on its deathbed.

To determine this, activities within various facets of the blockchain sector will be investigated including cryptocurrencies, smart contracts, distributed ledger technology (DLT) and popular platforms including Bitcoin, Ethereum and Hyperledger. Activity of the following vitals will be looked into: (i) new companies being founded; (ii) investment into start-ups and companies; (iii) patents published; (iv) academic papers published; (v) research and development funding; (vi) online search trends; (vii) mining infrastructure and hash rates; and (viii) blockchain-related software development effort.

Indeed, the blockchain sector includes many applications beyond cryptocurrencies [1], and by including cryptocurrencies (and associated hype surrounding them) in this study, the results are influenced beyond

what is otherwise pertaining only to the non-cryptocurrency blockchain sector. However, in this first study, the aim is to look at the sector at the most abstract level (including cryptocurrencies).

It would be ideal to go into greater detail for each facet investigated; however, due to space limitation, initial insights in regard to the various aspects will be provided and deeper analysis of each aspect will be left for future work.

A lot of hype surrounded the sector when cryptocurrency prices had surged mid- to late 2017. This hype was short-lived and prices soon came crashing down. Many associate the surge and crash in price with the sector's position in Gartner's hype cycle – yet at the time of writing

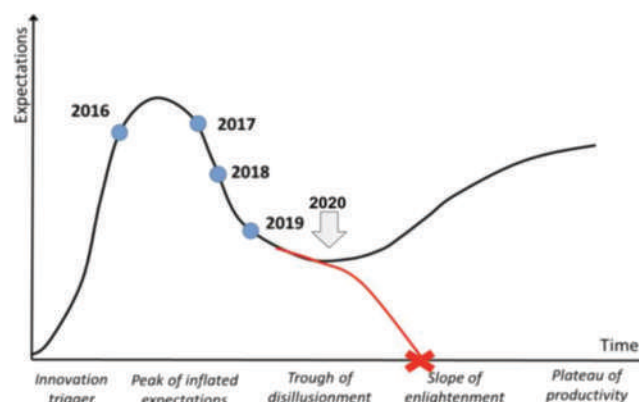


Figure 1: The Gartner Hype Cycle reproduced from [2] and modified.

this paper a second surge in price of cryptocurrencies is being seen. In this paper the period from January 2017 to December 2020 will be used

in undertaking the various data gathering and analysis required. Figure 2 depicts the prices of two popular cryptocurrencies, Bitcoin and Ether, for the aforementioned period. The hype period referred to can be seen starting around mid- to late 2017. Whilst, reference will be made to this hype period throughout the paper, in no way is the paper claiming that the Blockchain sector is dependent on cryptocurrencies' success solely (it is but just one factor) and indeed the Blockchain sector may survive independent of cryptocurrencies' success – however, reference is made to this period so as to be able to provide initial insight on potential correlations with the period.

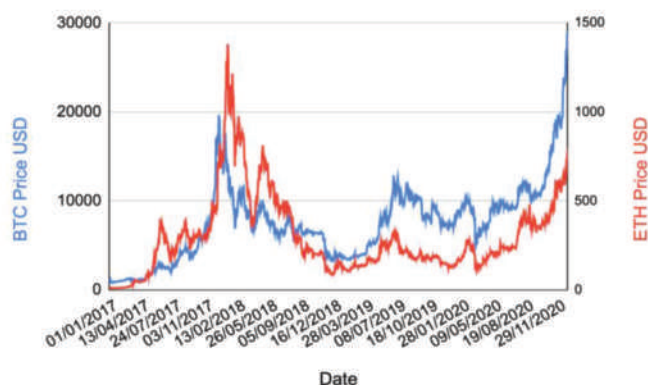


Figure 2: Bitcoin (BTC) and Ether (ETC) Price in United States Dollars (USD).

The paper will now follow by providing insight into the 8 aspects of blockchain activity mentioned above, where each section will describe its purpose, methodology-related aspects and results.

2. Companies Founded

Companies founded and services launched are indicators that demonstrate the private sector's belief in a technology's potential. Whilst it has proven difficult to find a registry or list of services which specify launch dates and activity, information relating to companies were retrieved from Crunchbase,ⁱⁱⁱ a publicly available and browsable database providing information about start-ups, companies and their financing [3]. It has been described as 'the premier data asset on the tech/startup world'.^{iv} An exercise was undertaken to determine the number of companies founded between 2017 and 2020 to provide an indication whether an increase or decrease in activity within the sector can be identified.

Methodology

Some companies in the dataset are not attributed with the full date they were founded but only the year – which end up being associated with 1st January of the respective year. It was decided to remove the companies listed as being founded on 1st January of each year since it would be impossible to identify which of those companies were actually founded on 1st January and which were founded during some other time in the respective year. Also, given that 1st January is a public or bank holiday in many countries it is unlikely that a high number of companies were founded on 1st January.

The data was gathered on 5 January 2021. All company data was retrieved for companies whose descriptions includes any of the following keywords and terms: 'blockchain', 'cryptocurrency', 'cryptocurrencies', 'DLT', 'DLTs', 'distributed ledger technology', 'distributed ledger technologies', 'bitcoin', 'ethereum', 'hyperledger', 'smart contract', 'smart contracts', 'cryptocurrency exchange' and 'crypto exchange'.

Results

Figure 3 depicts the number of blockchain-related companies (as per the terms listed above) founded per month between January 2017 and December 2020. The numbers show a peak of companies founded between late 2017 and early 2018 which coincides with the hype seen during that period. The question however is whether the post-hype data reflects an indication in regard to whether interest has been completely lost or not in the space. On initial glance one may conclude that the diminishing number of companies founded per month may indicate this.

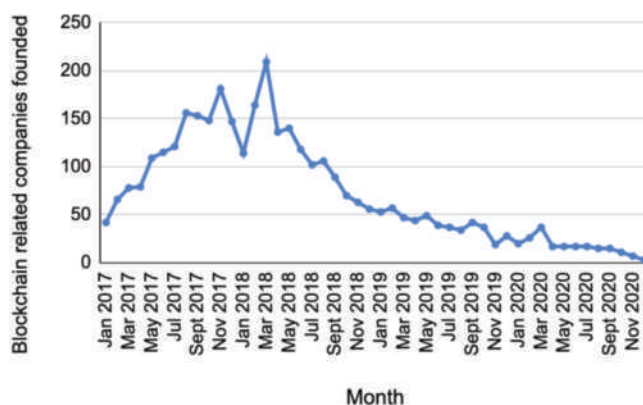


Figure 3: Blockchain-related companies founded between January 2017 and December 2020.

However, given how Crunchbase collects and processes data especially due to its crowdsourced nature of data collection, 'there is therefore a certain delay between the foundation of the company and its actual registration on Crunchbase' [4]. A company is likely to be listed on Crunchbase 'when it starts looking for investment, or has become part of the portfolio of an investor, or more generally wishes to gain greater visibility online' [4]. However, these numbers should be revisited in a year's time to see if 2020s numbers are around the numbers currently reported for 2019 to give an indication in regard to increasing or decreasing numbers of companies being founded.

To further support this argument, besides the depth to which this was discussed in [4], the same exercise was conducted for companies categorised under the keyword 'software' – a term that is likely to not have suffered from hype over the past few years. Figure 4 below provides support for this argument that the decreasing number of registered companies does not necessarily mean that companies are not being founded, just that they are not yet listed in the platform. However, what we can conclude is that figures currently reported for blockchain-related companies founded in 2019 were around the levels of companies founded prior to 2017's hype – and these figures should be revisited in a year's time.

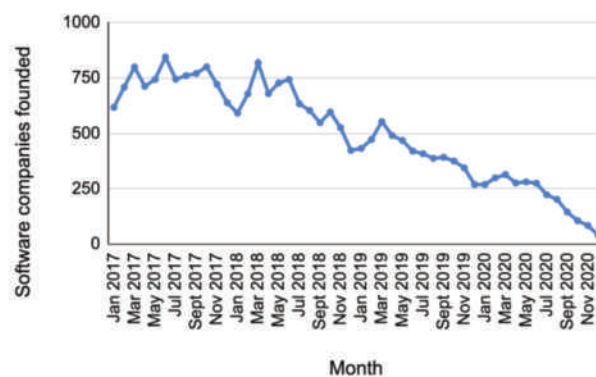


Figure 4: Companies categorised under 'software' founded between January 2017 and December 2020.

Whilst, it would be useful to see how many of these companies are still operating, and whilst Crunchbase data does indicate whether a company has closed, the figures are low and likely not representative of companies actually closed (likely due to the crowdsourced nature of data). The figures reported for closed companies for years 2017, 2018, 2019 and 2020 are 64, 40, 6 and 1, respectively. Whilst, accurate figures regarding whether companies are still operating would help to determine a more objective view of the success of the industry, the aim of this exercise highlights continual renewed interest to start companies in the sector, which is an indicator (albeit weaker) of the sectors potential success. That said, the general consensus is that many companies/projects initiated during the hype 'failed to materialize' [5], as would be the case for any initially hyped technology (just like the dotcom bubble). Whilst some originally cite a main problem being that blockchain is 'innovative technology in search for use cases' [6] Navqi and Hussain [5] highlight main problems which focus on the lack of applying an evidence-based practice approach. In their study 517 projects and start-up companies were analysed and their results clearly indicate that minimal evidence was used to establish whether a project's problem was actually a problem that needed solving.

Out of the 2778, 2552, 757 and 301 companies founded retrieved from Crunchbase for 2017, 2018, 2019 and 2020, respectively, 265, 259, 103 and 33 were companies that were listed as being from the following industries: private cloud, cloud infrastructure, cloud computing, cloud management, cloud storage, cloud data services, cloud security, artificial intelligence, machine learning, internet of things and quantum computing. That is around 10% of companies founded each year. This demonstrates the technology's cross pollination into other sectors which may also be seen as a testament to its future potential within other sectors.

The results heeded indeed provide a single holistic view including all cryptocurrency-related companies and other non-cryptocurrency blockchain companies together. The 2017 hype likely resulted in many cryptocurrency-based companies being founded the same and following year, which may drown out figures relating to those companies focused only on blockchain beyond cryptocurrencies. However, nonetheless cryptocurrency-focused companies also play a part within the sector and therefore it was decided to report the results in this manner. In future it could very well be that the number of companies founded are seen to be much less since interest to start a cryptocurrency after the hype ended may have diminished (though a second wave of interest in cryptocurrencies is being seen at the time of writing). Nonetheless, future work should go into further depth in regard to interest in the various sub-sectors (e.g. cryptocurrencies, supply chain applications, enterprise blockchain solutions, etc).

3. Investment

Amounts of investment raised are good indicators to identify technologies that have potential since entities (venture capitalists, investors, etc.) specialised in determining what technologies have potential, literally bet their money on the respective technology. Therefore, data has been gathered to determine how funding and investments have fared over the period.

Crunchbase is often claimed to be 'a primary data source for investors' [7] which may be due to its large investor network comprising of at least 3,000 global investment firms who 'submit monthly portfolio updates' [7]. Therefore, investments over the period will be analysed to provide insight with respect to this study. Since Crunchbase crowdsources its data, it was decided to also compare investment data from CB Insights' [8].

Methodology

For data retrieved from Crunchbase, the same keywords and terms used in the previous section were used to filter out the different investments made

to companies whose descriptions included the terms. The funding round datasets included exact dates for investment periods (unlike company foundation dates). The data was also gathered on 5 January 2021, and the investments were aggregated according to the month. For data retrieved from CB Insights, investments (categorised under deals) were retrieved from companies categorised under 'Blockchain' (i.e. in the 'Blockchain' collection) for the following investment stages: Seed / Angel, Series A, Series B, Series C, Series D, Series E+, Private Equity, Growth Equity, Other Venture Capital, and IPO. Data was retrieved from CB Insights on 6 March 2021.

Results

For data retrieved from Crunchbase, to get an overview of funding in the sector, all types of funding rounds were included – from pre-seed and seed funding, to all the different series funding and even Initial Coin Offerings (ICOs). Due to the different types of funding levels, depending upon the month and types of funding rounds made, different orders of magnitude for investments between the months are seen. Therefore, in depicting the total amount of funding (in USD) for the period in Figure 5, a logarithmic scale was used. The hype period can clearly be seen in the total amount of funding raised and the number of investments made, which are around an order of magnitude greater during the hype than before and after. It is worth noting that investments made include ICOs which allowed for the general public to 'easily' invest in various projects. Given the hype it is likely that quite a number of investments during the period were public investments fueled by nothing more than the hype. Given that Crunchbase feeds most of its investment-related data directly from its investor network, these results do not suffer from the lag seen in companies being listed in their dataset.

From the data it can be seen that whilst investments did peak during the hype period, they returned back to sustained pre-hype levels. This may indicate that indeed the sector has entered the Gartner hype cycle's Trough of Disillusionment and potentially on its way out towards the Slope of Enlightenment.

A similar exercise was conducted for investments reported on CB Insights depicted in Figure 6. Trend lines have been added to easily spot trends. Investments are seen to steadily increase till around the hype period, and thereafter tapers off, whilst indication of a potential increase in investments is seen towards the end of 2020. This corroborates the findings above and may also be an indication of potential upcoming increased investment interest in the sector.

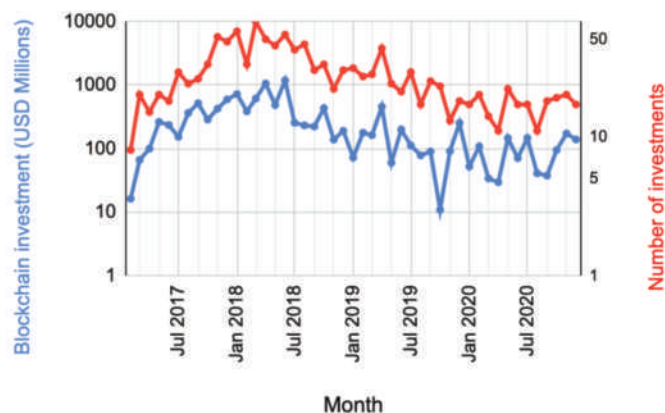


Figure 5: Investment raised (in USD) and number of investments made to Blockchain-related companies from Crunchbase.

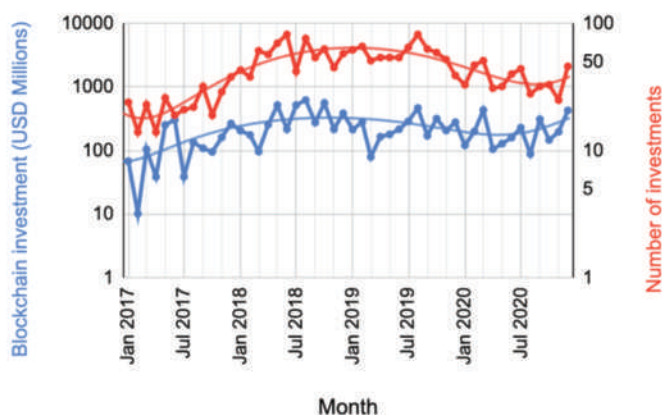


Figure 6: Investment raised (in USD) and number of investments made to Blockchain-related companies from CB Insights.

4. Patents

Patents, which provide companies with a manner to secure their intellectual property, can provide an indication in regard to innovation and development taking place, as well as to the sector's backing and investment to secure such innovation – which can be quite costly and therefore demonstrates the sector's belief that investing in securing such intellectual rights will bear fruit in the future.

The number of patents registered (worldwide) per month between January 2017 and December 2020 was extracted from Espacenet^{vi} run by the European Patent Office (EPO). Espacenet was chosen as it reportedly has the highest number of patents in its database and has the “best features for searching” [9] when compared with Patentscope and Depatisnet – two other popular patent search engines.

Methodology

The number of patents published per month in the period were extracted using the following query format (this particular query extracts patents published in January 2017):

```
(nftxt = 'Blockchain' OR nftxt = 'Cryptocurrency' OR nftxt = 'Cryptocurrencies' OR nftxt = 'Distributed Ledger Technology' OR nftxt = 'Distributed Ledger Technologies' OR nftxt = 'Bitcoin' OR nftxt = 'Ethereum' OR nftxt = 'Hyperledger' OR nftxt = 'Smart contract' OR nftxt = 'Smart contracts') AND pd within '2017-01-01, 2017-01-31'
```

The data was gathered on 14 January 2021.

Results

Patents can take quite some time until they are granted and published – even up to ‘three to five years from the date’^{vii} of application. Therefore, a lag will be seen in regard to a patent being granted and its publication. In fact, looking at Figure 7, which depicts the number of patents published on the subject matter per month, it can be seen that numbers substantially increase in November 2018 and continue to do so after. Further analysis has not been undertaken to determine whether this is due to a lag in patent publications post the 2017 hype period.

However, it can be noted that even if most of the patent publications granted in the more recent years were due to 2017's hype, the patent owners still saw utility in paying for the patent at the time of the grant/publication date (which is when majority of the patent registration costs are required to be paid).

Further analysis can be undertaken to determine whether a majority of the original dates of filing relate to the 2017 hype or not (though it does not

seem likely from an initial glance).

Irrespective of this, we can draw the conclusion that increasingly more money is being spent on finalising patent publication as the months go by – which is an indication that the private sector still sees the domain to be one worth investing in.

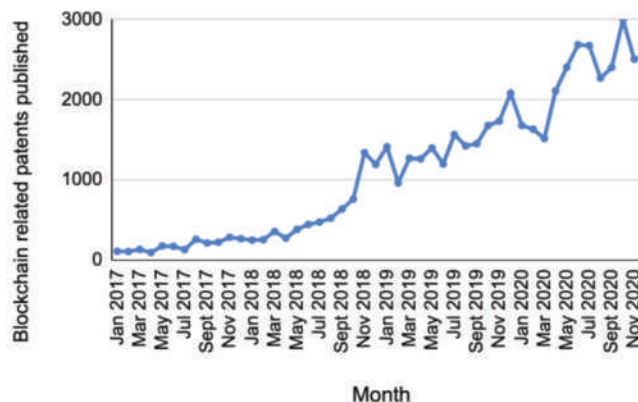


Figure 7: Blockchain-related patents published per month.

5. Academic Papers

The current and future success of a technological sector is dependent not only on the private sector but also upon further research and development from the academic sector – especially within an emerging sector such as this one.

To provide a picture of the academic interest within the sector, a primary output from academia, papers, have been investigated to provide an objective insight in regard to interest in the domain. The number of papers published each year has been extracted from the following popular academic paper indices and repositories which are known to have substantial overlap [10]: Google Scholar,^{viii} Web of Science,^{ix} Scopus^x and EBSCO^{xi} (including all its databases). Whilst results heeded from Google Scholar may well include non-academic sources (including patents, technical reports, and other documents that the Google Scholar engine determines to be a paper), the Web of Science, Scopus and EBSCO repositories only index material which they deem to be trustworthy in terms of their academic relevance, and therefore it was decided to include the different repositories.

Methodology

The number of papers published were extracted over a period of a year. This was due to most of the databases providing a search criterion that enables for searching by granularity of a year and not of a finer granularity. The number of papers were extracted by searching for the same following terms and keywords within the papers across the different databases: Blockchain, Cryptocurrency, Cryptocurrencies, DLT, DLTs, ‘Distributed Ledger Technology’, ‘Distributed Ledger Technologies’, Bitcoin, Ethereum, Hyperledger, ‘Smart contract’, ‘Smart contracts’, ‘Cryptocurrency exchange’, ‘Crypto exchange’. The results were extracted on 5 January 2021.

Results

Whilst the Web of Science, Scopus and EBSCO databases reported an exact number of papers that matched the search criteria, Google Scholar reported an indication of ‘about’ a number of resultant papers and therefore, the Google Scholar results are estimated values.

In Figure 8 a steady increase in the number of papers published can be seen across all the databases until 2019. Thereafter, for 2020, the number of papers reportedly published decrease slightly for Google Scholar, Web

of Science and EBSCO, yet they are seen to continue to increase in the Scopus database.

Albeit at a slightly lower rate than the year before. This reported decrease in papers is likely not due to an actual dip in papers being published but due to the fact that the databases can take quite some time to be updated with published papers.

Google Scholar regularly adds 'new papers several times a week' yet it could take up to '6-9 months to a year or longer' to update their records – and similarly the other databases can take a number of months to a year as well.

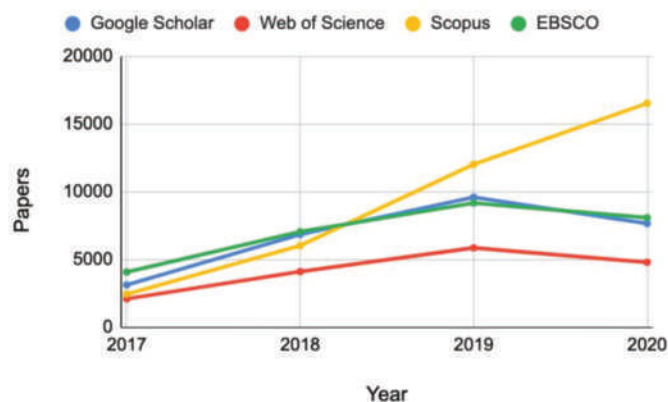


Figure 8: Blockchain-related papers published per year.

Therefore, these results should be revisited in a number of months to a year. Whilst, it cannot be definitely said that the number of papers published in 2020 increased compared to previous years, it is reasonable to assume that the number of papers will be roughly equal to 2019 if not more. Once enough time has passed to be able to get a full picture of 2020-related publications this can be confirmed. That being said the numbers indicate that there is not a significant dip in interest from the academic community, but in the least roughly the same level of interest. Whilst the rationale behind this exercise was to establish academic interest in blockchain (by surveying the numbers of papers published in the field), future work could be undertaken to establish how impactful the field's papers were (by looking at the number of times the papers have been cited).

6. Research and Development Funding

Academic papers can demonstrate academia's interest in the domain up till the recent past. Research and development funding can provide a picture of where academia and other research and development-based stakeholders will focus their time over the coming years. When funded by government it also provides an indication in regard to a government's support of a sector.

Research and development funding data was retrieved from the UK's national innovation agency, Innovate UK,³³ in aim of determining governmental interest in the sector by comparing amounts of blockchain-related project funding over the years. Indeed, this data is only representative of a single funding agency from a single country (the UK), and further research should be undertaken to be able to draw global analysis.

Methodology

Innovate UK's public transparency dataset on their funded projects³³ was used and projects were filtered out so that only the ones whose description or title contained the following terms were included: Blockchain, Cryptocurrency, Cryptocurrencies, DLT, DLTs, 'Distributed Ledger Technology', 'Distributed Ledger Technologies', Bitcoin, Ethereum, Hyperledger, 'Smart contract', 'Smart contracts', 'Cryptocurrency exchange', 'Crypto exchange'. The dataset also contains projects that were

withdrawn, which were excluded from this analysis. The version uploaded on 8 January 2021 was used^{33v}.

Results

Figure 9 provides a full view of the number of projects funded including the amount funded and starting date. The figure shows that 2019 and 2020 saw a substantial increase in the numbers of projects and size of projects funded. A number of these projects will be ongoing till August and November 2022. It can be assumed that many of these projects will contribute positively to the number of academic papers published within the domain. Indeed, again this is a single funding agency; however, the results are promising.

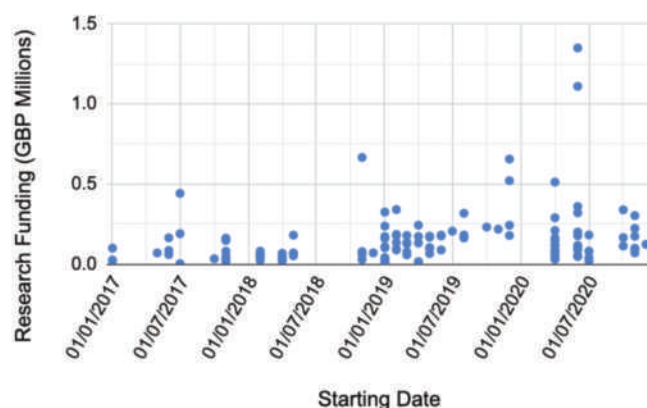


Figure 9: Innovate UK-funded blockchain-related research and development projects.

Figure 10 provides an overview for the different funding periods (2016/17 to 2019/20) that show total costs and grants issued for blockchain-related projects around doubling each year. The year 2019/20 saw a dip in awardees indicating larger-sized grants (as can be seen in Figure 9).

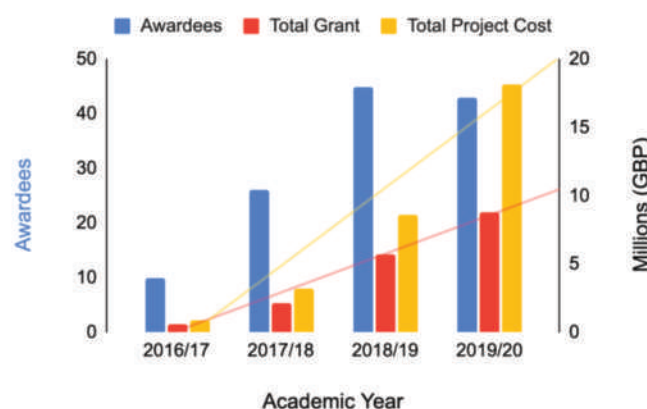


Figure 10: Innovate UK total blockchain-related project funding, costs and awardees.

7. Online Search Trends

A technology's success is dependent not only on innovation and public and private sectors' support for that technology, but it must also be adopted by its main stakeholders – which may or may not be the general public. In the case of blockchain, DLT and its various applications, the level to which the general public may be interested in it widely varies. Nonetheless it would be useful to provide insight in regard to the varying interest and trends surrounding the various terms over the period. Even if a term is likely to be used by a small stakeholder group then its popularity over time should

be representative of that stakeholder group (unless the term is used to mean something else or interest during some period is garnered by other groups).

Google Trends^{xy} provides insight in respect to a search term or topic's search interest over time. A search term is the exact text that users type into Google's search engine, whilst a topic encapsulates many different search terms that Google deems to be categorised under the specific topic computed using 'an automated classification engine' [11]. The various terms/topic trend results are scaled to a percentage compared to all the other terms/topics that are used within the same trend results, as per the site's description: 'the resulting numbers are then scaled on a range of 0 to 100 based on a topic's proportion to all searches on all topics'^{xyvi}.

Methodology

Given that the results provided by Google Trends are scaled to a range of 0–100, less popular terms/topic results end up being scaled down to <1 and even to 0 when compared with more popular terms/topics. Therefore, terms and topics were grouped together such that they would not result in scaling out relevant results. Whilst any search term can be used to generate trend results, topics are restricted to the ones that Google Trends has identified.

We gathered data for the following topics: Cryptocurrency, Bitcoin, Ethereum, Hyperledger, Smart contract and Distributed ledger; and for the following search terms: Blockchain, Bitcoin, Cryptocurrency, Cryptocurrencies, Ethereum, DLT, Hyperledger and 'Smart contract'. The results were retrieved for a Worldwide coverage of search popularity. The results were gathered on 5 January 2021.

Results

Bitcoin was the most popular topic and search term by a substantial difference. Figure 11 shows the Bitcoin topic and search time, along with the Cryptocurrency topic and Blockchain search term to be able to gauge the difference between them and the other topics and search terms discussed further below. The hype period in 2017 can clearly be seen, and both the Bitcoin topic and search term have practically the same results, except for a peak in the Bitcoin topic's trend during the beginning of September 2019. It is unclear why this topic has seen this peak and yet the search term itself does not see this increase in interest.

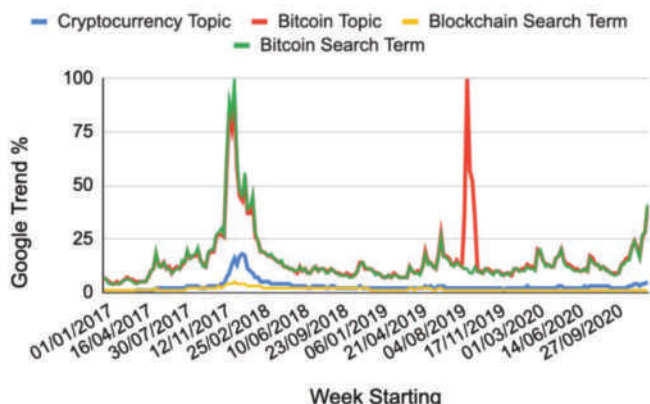


Figure 11: Google trend results for 'Cryptocurrency' and 'Bitcoin' topics, and 'Blockchain' and 'Bitcoin' search terms.

After the hype period, interest in Bitcoin is rather stable until the end of 2020 where the interest in Bitcoin can be seen to be peaking again – when Bitcoin's price started to peak again late 2020 (and eventually reach new all-time highs).

It is interesting to note that the Bitcoin search term and topic have substantially higher results than the other search terms and topics, indicating that the general public has been more interested in Bitcoin than the technology itself.

Results comparing the search terms Cryptocurrency, Blockchain and Ethereum are shown in Figure 12, whilst the results for the same topics are shown in Figure 13. Ethereum can be seen to peak during the beginning of the Initial Coin Offering (ICO) hype that started in Summer 2017, and then again in late 2017 when Bitcoin and cryptocurrencies in general had seen a peak of interest (and price surge).

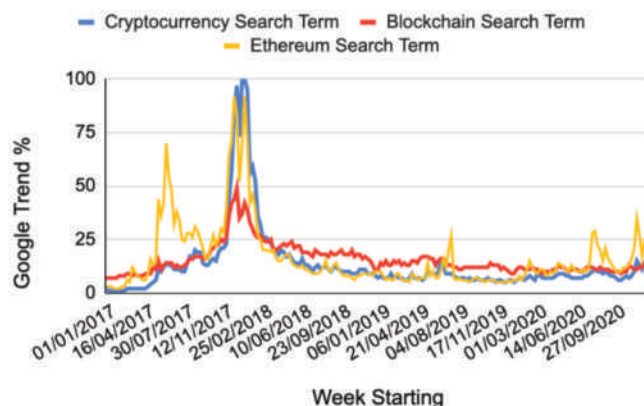


Figure 12: Google search term trend results for 'Cryptocurrency', 'Blockchain' and 'Ethereum'.

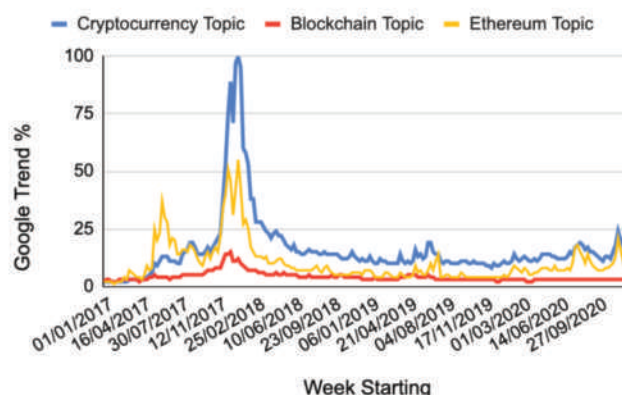


Figure 13: Google topic trend results for 'Cryptocurrency', 'Blockchain' and 'Ethereum'.

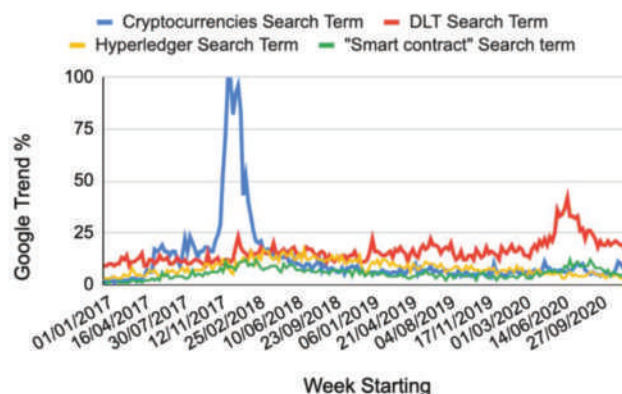


Figure 14: Google search term trend results for 'Cryptocurrencies', 'DLT', 'Hyperledger' and 'Smart contract'.

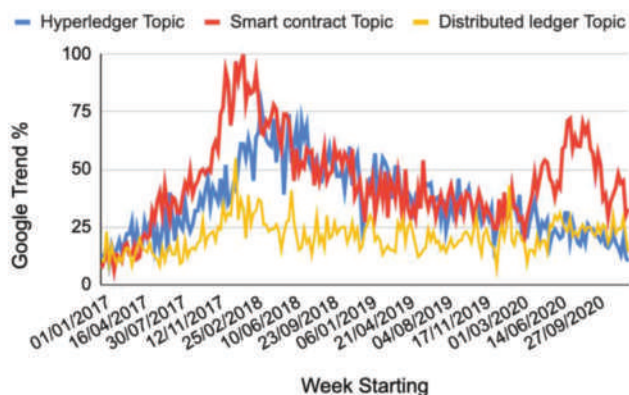


Figure 15: Google *topic* trend results for 'Hyperledger', 'Smart contract' and 'Distributed ledger'.

Figure 14 shows the trend results for the following search terms: Cryptocurrencies, DLT, Hyperledger and 'Smart contract'. Congruent with other results the cryptocurrencies term sees a peak of interest during the hype period in 2017. Smart contracts seem to increase in interest whilst it slightly lags after cryptocurrencies which could be due to specialists (developers and lawyers) wanting to learn more about the technology associated with the hype around cryptocurrencies. Similarly, the DLT search term sees more interest as time passes which could be due to specialists' interest in the broader area of DLT.

In Figure 15 we can see more clearly the smart contract topic peak after the initial hype had started in mid-2017. Again, this may be due to specialists showing interest in the technology supporting the previous hype. Hyperledger, a popular blockchain infrastructure framework used typically for private blockchains can also be seen to garner interest after the mid-2017 hype. The interest seems to peak in late 2018 and gradually diminish over time along with interest with smart contracts, though smart contracts see another peak of interest towards mid and end of 2020.

From the various results we can conclude that interest in the various aspects remain at stable levels after the 2017 hype. Some of which see renewed interest potentially due to the increase in cryptocurrency price.

8. Hash rate and Miners

When it comes to operating a blockchain network, especially a proof-of-work-based one, the number of miners and computational power backing the network is a testament to the interest in the particular network as well as support for the network's success – as the more computational power, the less likely it becomes to successfully undertake an attack on the network. Here, an analysis of two of the most popular proof-of-work-based cryptocurrency networks, Bitcoin and Ethereum, is provided.

Indeed, other consensus mechanisms are being proposed and used (such as proof-of-stake) which would be of interest to investigate; however, we leave this for future work.

Methodology

Hash rate datasets for the Bitcoin and Ethereum networks were retrieved from Coin Metrics^{viii} on 5 January 2021, for the period 1 January 2017 to 31 December 2020.

Results

Figure 16 depicts Bitcoin's and Ethereum's exahash per second and terrahash per second rates, respectively. Besides a slight dip in mid- to late 2018, Bitcoin shows steady growth in terms of computational power being

put into the network. This dip likely occurred due to a number of miners deciding to stop mining as the price of bitcoin had reached its lowest point around that time, deeming the operation to not be profitable enough for some miners. Despite price fluctuations the amount of computational power in the Bitcoin network sees steady growth which is an indicator that the number of miners and/or the amount of resources they are putting behind the network is increasing which is a testament to miners' and the network's success in spite of any claimed inefficiencies [12]. Ethereum sees a similar trend though on a smaller terrahash scale.

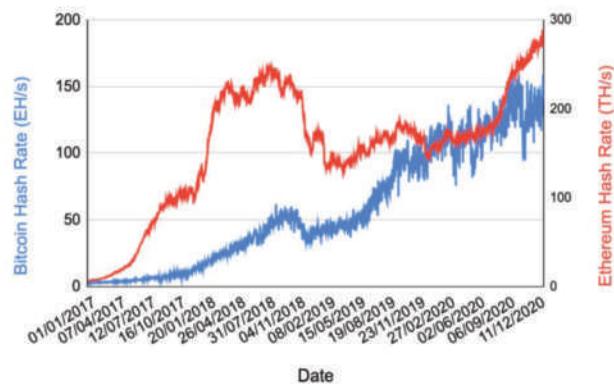


Figure 16: Bitcoin and Ethereum hash rates.

9. Code repository activity and Software developers

Having looked into various stakeholders from the private and public sectors, to academia and the general public to the miners supporting such networks, it would be ideal to provide insight in regard to an indication of activity amongst the software developers creating the technology. GitHub^{ix} is a popular code repository used by software developers around the world for both open-source software projects as well as private repositories.

To establish whether blockchain software development activity is deemed to be dead or alive, activity of open-source GitHub code repositories were analysed.

Methodology

GH Archive^{xix} provides an up-to-date archive of all activities that take place in public GitHub code repositories. The GH Archive data required was retrieved using the Google BigQuery dataset provided. To make use of the data, though, it was required to determine which projects were relevant.

The GitHub REST API^{xx} was used to retrieve repositories that were categorised under the 'blockchain' topic. A total of 11,893 repositories were categorised under the blockchain topic (as retrieved using the API). The API, however, only allows for retrieval of 1,000 results per search query. Therefore, a script was written to return results in batches of a maximum of 1,000 results for distinct queries. Searches were repeated for repositories containing words starting with 'a' to 'z' and '0' to '9'. To gather a larger list of projects the process was repeated for the different combinations of the second letter of a word contained within a project's name. Ultimately, this resulted in retrieval of the names of 11,605 distinct projects categorised under the blockchain topic. This means that a remaining 288 blockchain project names were not retrieved – yet just over 97% of project names were retrieved. In the interest of time, it was decided that enough data had been collected to undertake an initial investigation.

Using the list of blockchain-related project names retrieved using the GitHub REST API, the GH Archive was then used to extract the number of events that took place on the relevant projects per month between January 2017 and December 2020. All repository events and types were included. The types of events^{xxi} are: PushEvent, IssueCommentEvent,

IssuesEvent, CreateEvent, WatchEvent, MemberEvent, CommitCommentEvent, PullRequestEvent, DeleteEvent, ForkEvent, PullRequestReviewCommentEvent, PublicEvent, ReleaseEvent and GollumEvent.

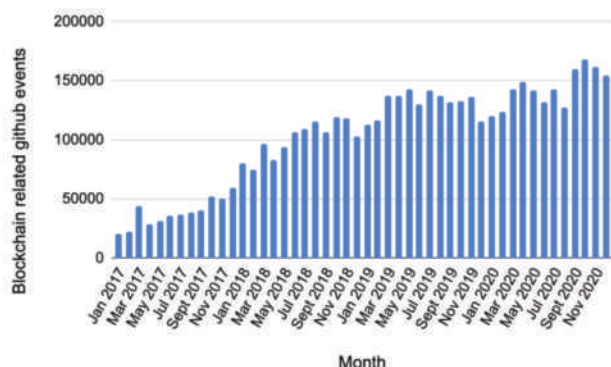


Figure 17: GitHub Blockchain-related code repository events.

Results

Figure 17 shows the total number of blockchain code repository events per month between January 2017 and December 2020. The figure shows a steady increase in activity across the different blockchain-related GitHub code repositories which indicates that the amount of work in developing and maintaining blockchain-related projects is ever increasing with time. Interestingly, effects pertaining to hype and/or related cryptocurrency pricing cannot be seen to affect the total development effort across the different projects. Blockchain-related development is far from dead, and seems to not be affected by neither surges nor drops in related cryptocurrency prices.

Whilst, it is very hard to determine why individual projects may survive or not since there are many different external factors at play, it would be ideal to identify traits of successful projects. Figure 18 depicts the number of contributors to a project against the number of days since a project was last active, and how long a project remained active for. As suggested in [13] the duration of activity is calculated as the difference between its first and last repository activity event.

Whether a project that is likely to be successful attracts more contributors, or whether having more contributors is more likely to make a project successful is hard to tell – yet it can be seen that the more contributors a project has the more active it is (i.e. around 0 days since the last activity) and the longer the project was/is still alive for.

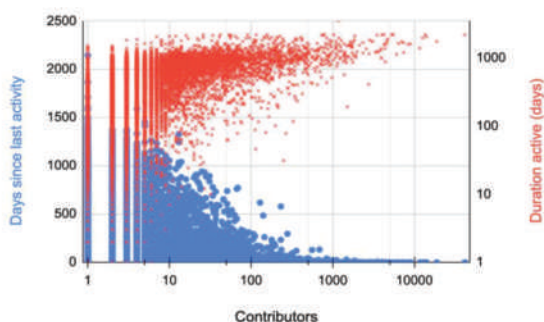


Figure 18: Number of GitHub Blockchain-related project contributors compared to the number of days since the projects' last activity and the project active lifetime.

10. Conclusions

Is Blockchain dead? We started off with the question, and in aim of answering it we investigated various aspects of the sector which may or

may not provide insight in regard to whether it is dead or alive. Points to highlight from above include:

- (i) Whilst the number of companies founded per month has decreased after the hype period according to a popular tech start-up/company registry (Crunchbase), the decreasing number of companies founded for a broader 'software' sector also decrease per month. An explanation behind this is congruent with claims that companies may not necessarily be registered on the site in their early stages until they desire to be listed or have already managed to attract investment. These results should be revisited in future to see if the numbers of companies founded in Crunchbase for 2019 and 2020 increase to support this claim;
- (ii) The 2017 hype saw an increase in investment in blockchain-related start-ups and companies. Though post-hype investment levels did drop slightly, they still remained at a stable level;
- (iii) Patents published has steadily increased since 2017. Whilst patents do take time to be granted and published, the main granting and publication costs are paid at the end – which means in the very least patent owners are still willing to invest substantial cost to secure their patents (which may be from a few years before), or that more patents are being submitted as time goes by;
- (iv) The number of academic papers has been steadily increasing since 2017 and reported numbers drop slightly for 2020. However, as discussed, academic databases and indices can take up to a number of months and even up to year to include some papers. Therefore, given that this paper was written at the very beginning of 2021, it is likely that a large number of papers had not been included yet in the reported numbers. Therefore, these figures should be revisited in future to see if the number of papers reportedly published for 2020 increase to more than that of 2019. Nonetheless, even if the slight drop in papers turns out to be the reality, the numbers are still stable;
- (v) Whilst data from only one governmental research and development funding agency was investigated and future investigation on other agencies around the world should be looked into, the amount of investment in blockchain-related projects can be seen to increase year on end;
- (vi) Public interest determined by search engine results pertaining to the sector may very well be swayed by hype as seen in the data presented herein. However, stable interest in the sector remains post-hype. The public, according to the search trend results, is generally more interested in cryptocurrency than blockchain technology. It may be deemed that there is a need for a stronger educational drive with respect to the technology and the benefits it provides beyond cryptocurrencies;
- (vii) Interest in mining for popular cryptocurrency blockchain networks, Bitcoin and Ethereum, can be seen to increase steadily – a testament to the success of both miners and the network as a whole;
- (viii) Software development effort is steadily increasing, without detriment from fluctuating currencies or hype, over time. A trait that can be seen from the data is that the more contributors a project has, the longer the project has lasted and also, the least amount of time has passed since the last activity was undertaken. This seems to be a case of strength in numbers. Projects of isolated developers may be less likely to succeed. Future work should be undertaken to establish whether collaboration, partnerships and/or code reuse between different projects provides any indication towards a project's success in staying alive.

Indeed, this work only provides an initial investigation into the various facets determining their activity. However, going into more depth in the various aspects is left as future work. Various results from this study and

future work will be disseminated online at <http://blockchainthings.io>. From the analysis undertaken it can be concluded that **either**: if *blockchain is dead* then substantial private investment continues to be made in vain, money is being wasted on securing intellectual property that is not worth the costs, academics are busy undertaking research and publishing papers in a field that is doomed, government money is being spent on furthering research and innovation that will not result in advancement, substantial stakeholders and the general public are still busy searching online in the domain finding information that will likely be irrelevant soon, funds are being spent in mining infrastructure to secure and support a network that will cease to exist as well as to make profits in a cryptocurrency that will be worthless, endless hours are being spent in developing software that will not be used; **or** *blockchain is not dead*. **Long live Blockchain!**

References:

- [1] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology - BEYOND BITCOIN," *Berkeley Eng.*, 2016.
- [2] J. Atherton, "Who is the Blockchain Employee? Exploring Skills in Demand using Observations from the Australian Labour Market and Behavioural Institutional Cryptoeconomics," *J. Br. Blockchain Assoc.*, vol. 3, no. 2, pp. 1–12, 2020, doi: 10.31585/jbba-3-2-(4)2020.
- [3] J.-M. Dalle, M. den Besten, and C. Menon, "Using Crunchbase for economic and managerial research," *OECD Sci. Technol. Ind. Work. Pap.*, 2017, doi: <https://doi.org/10.1787/18151965>.
- [4] F. Ferrati and M. Muffatto, "Using crunchbase for research in entrepreneurship: Data content and structure," *Proc. Eur. Conf. Res. Methods Bus. Manag. Stud.*, vol. 2020-June, no. July 2007, pp. 342–351, 2020, doi: 10.34190/ERM.20.120.
- [5] N. Naqvi, "Evidence-Based Blockchain: Findings from a Global Study of Blockchain Projects and Start-up Companies," *J. Br. Blockchain Assoc.*, vol. 3, no. 2, 2020, doi: 10.31585/jbba-3-2-(8)2020.
- [6] G. Fridgen, J. Lockel, S. Radszawill, A. Rieger, A. Schweizer, and N. Urbach, "A solution in search of a problem: A method for the development of blockchain use cases," 2018.
- [7] G. Tarasconi and C. Menon, "Matching Crunchbase with patent data," *OECD Sci. Technol. Ind. Work. Pap.*, 2017.
- [8] C. Longen, "CB Insights," *Journal of Business and Finance Librarianship*, vol. 22, no. 3–4, 2017, doi: 10.1080/08963568.2017.1372018.
- [9] B. Jürgens and V. Herrero-Solana, "Espacenet, Patentscope and Depatisnet: A comparison approach," *World Pat. Inf.*, vol. 42, pp. 4–12, 2015, doi: 10.1016/j.wpi.2015.05.004.
- [10] A. Martín-Martín, E. Orduna-Malea, M. Thelwall, and E. Delgado López-Cózar, "Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories," *J. Informetr.*, vol. 12, no. 4, pp. 1160–1177, 2018, doi: 10.1016/j.joi.2018.09.002.
- [11] S. Vosen and T. Schmidt, "Forecasting private consumption: Survey-based indicators vs. Google trends," *J. Forecast.*, vol. 30, no. 6, pp. 565–578, 2011, doi: 10.1002/for.1213.
- [12] A. Urquhart, "The inefficiency of Bitcoin," *Econ. Lett.*, vol. 148, pp. 80–82, 2016, doi: 10.1016/j.econlet.2016.09.019.
- [13] E. Kalliamvakou, L. Singer, G. Gousios, D. M. German, K. Blincoe, and D. Damian, "The promises and perils of mining GitHub," *11th Work. Conf. Min. Softw. Repos. MSR 2014 - Proc.*, pp. 92–101, 2014, doi: 10.1145/2597073.2597074.

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

Confirmed that I am the sole author responsible for all aspects of the paper.

Funding:

None declared.

Acknowledgements:

I would like to thank the team at the Centre for Distributed Ledger Technologies at the University of Malta, and all the Masters in Blockchain and DLT lecturers, and past and present students for engaging in various discussions that had lead me to undertake this study, particularly Prof. Gordon J. Pace with whom I have spent countless hours debating various related topics.

ⁱ <https://www.bloomberg.com/news/articles/2019-11-12/blockchain-is-dead-crypto-geeks-debate-merits-of-once-dear-tech>

ⁱⁱ <https://www.gartner.com/en/documents/3987450/hype-cycle-for-blockchain-technologies-2020>

ⁱⁱⁱ <http://www.crunchbase.com>

^{iv} <https://www.businessinsider.com/whither-techcrunch-2011-9> accessed on 12th January 2021.

^v <https://www.cbinsights.com/>

^{vi} <https://worldwide.espacenet.com/>

^{vii} <https://www.epo.org/service-support/faq/procedure-law.html>

^{viii} <https://scholar.google.com/>

^{ix} <https://webofknowledge.com/>

^x <https://www.scopus.com/>

^{xi} <https://www.ebsco.com/>

^{xii} <https://www.gov.uk/government/organisations/innovate-uk>

^{xiii} <https://www.gov.uk/government/publications/innovate-uk-funded-projects>

^{xiv} Ibid.

^{xv} <https://trends.google.com/>

^{xvi} <https://support.google.com/trends/answer/4365533?hl=en>

^{xvii} <https://coinmetrics.io/community-network-data/>

^{xviii} <https://github.com/>

^{xix} <https://www.gharchive.org/>

^{xx} <https://docs.github.com/en/rest>

^{xxi} <https://docs.github.com/en/developers/webhooks-and-events/github-event-types>

Investment Compliance in Hedge Funds using Zero Knowledge Proofs

Komal Kalra, Shubham Sahai, Sandeep Kumar Shukla

Department of Computer Science & Engineering, Indian Institute of Technology (IIT) Kanpur, India

Correspondence: komalklr@gmail.com

Received: 15 January 2021 **Accepted:** 24 March 2021 **Published:** 5 April 2021

Abstract

Financial Regulation is a form of compliance system that subjects financial institutions to certain requirements and restrictions. Investment Compliance is an example that involves investment restrictions and monitoring on behalf of investors. Hedge Funds differ from other traditional funds such as mutual funds because of their ability to employ complex investment and hedging techniques. These are private entities with few public disclosure requirements. This is useful in a way as the strategies used are confidential which allows financial agents to participate in the financial markets without any fear of information leakage, thereby promoting liquidity. However, this is often implied as the lack of transparency. Hedge Funds are expected to produce higher returns, but sometimes investors seek a risk guarantee in addition to higher returns. However, too much transparency rules out the incentives financial entities have by participating in the first place. On the other hand, too much secrecy may give rise to malicious entities that can break the rules due to a lack of compliance. We aim to solve this problem of protecting investors while ensuring the privacy of financial bodies using zero knowledge proofs. Proofs can be visualised as a way of providing enough information to investors while the zero-knowledge property of proofs maintains the privacy of the fund manager's strategies. We propose a protocol to address this scenario using Zokrates, a framework for verifiable computation using Zk-SNARKs on Ethereum, to encode the constraints and export the verifier. Based on our implementation and analysis, it can be concluded that zero knowledge proofs provide us with a variety of ways to develop compliance systems.

Keywords: *compliance, investors, fund manager, proofs, transparency*

JEL Classifications: *G11, G18, G28*

1. Introduction to Investment Compliance

In the financial context, the term hedge refers to placing limits on risk. The ability to employ complex trading strategies distinguishes hedge funds from other funds. Generally, these are considered risky investments, which is why only accredited investors, investors with high financial sophistication, can make investments in them. Although hedge funds are not subject to many restrictions that apply to regulated funds, guidelines were passed in some countries following the financial crisis of 2008 to increase government regulation of hedge funds. In addition, SEC and other regulatory bodies have requested more transparent hedge fund practices over the years [34, 38].

Hedge Funds are privately owned funds that face relatively fewer regulations and conditions than other funds (e.g. mutual funds and equity funds). To protect investors, there are strict guidelines from regulatory bodies, such as SEC. Few examples would be that only investors with income more than a particular value are allowed, only investors with a net worth exceeding a particular value are allowed, etc. However, investors would also like to ensure that fund managers are behaving properly and that their investments do not exceed the level of risk. On the other end, the fund manager might not want to disclose all their portfolio characteristics as this may lead to leakage of the strategies used by them. Portfolio characteristics for a particular fund describe the allocation of investments in different assets.

We begin by defining zero knowledge proof systems [36], a scheme in which the prover convinces the verifier about the fact that they have knowledge about a particular statement without revealing anything about

the statement. Section 2 describes the zero knowledge proofs in detail. Due to the confidential nature of the portfolio and the need to regulate the investment process to protect interest of investors, this problem can be reduced to zero-knowledge proofs. Proofs can be visualised as a way of providing enough information to investors while the zero-knowledge property of proofs helps to maintain the privacy of the fund manager's strategies.

1.2 Related Works

To solve the problem of conflict of interest between investors and fund managers, Szydlo [31], in 2005, described a protocol between investors and fund managers. Precisely, he described the portfolio characteristics and risk factors for each asset and defined a linear condition that is to be proven by the fund manager to convince investors that their risk measure does not exceed any predefined risk threshold. For this, he used Pederson Commitments [36] and Interval Proofs using Shoup's NTL package [37]. Another related work is given by Gowravaram [18] which uses the same method of commitments and Interval Proofs.

1.3 Our Contribution

As there is a lack of trust between the fund manager and investors, there needs to be a way to solve this problem of conflict of interest between parties. Here comes the role of blockchain smart contracts to verify that the fund manager follows the rules specified by the investor (or predefined by the fund manager) without depending upon any central authority. We use Ethereum smart contracts as a form of agreement between two parties

such that investors can verify that funds follow the specified guidelines and are behaving properly. For this, we use a zero-knowledge proof systems framework Zokrates (SNARKS for Ethereum), which uses libsnark by Pinocchio protocol (or bellman for Groth16). Libsnark is a C++ library for SNARK systems and provides mechanisms to encode most of the problems in the form of Rank-1 Constraint Systems(R1CS) and then into Quadratic Arithmetic Programs (QAP), from which proofs are generated such that bilinear maps can be used for verification which makes it efficient to verify. To summarise,

- Zokrates framework provides us with the ability to generate the Solidity Contract which can be deployed directly on Ethereum and verification can be performed by calling a method on the contract.
- One can specify any condition (that can be encoded in libsnark) and encode it into constraints so that verification can be performed in constant time and with constant proof size.
- Using this method to encode the constraints also gives us an added advantage to encode quadratic (and higher-degree) constraints that might be required from the financial point of view.

We begin with the definition of zero knowledge proofs and cryptographic preliminaries required for the protocol in Section 2. Section 3 describes Pinocchio Protocol and Zokrates architecture. In Section 4, the problem statement is explained in detail. Section 5 describes the protocol workflow and implementation details using Zokrates. Section 6 presents the evaluation results of the proposed protocol. Finally, in Section 7, we conclude this article and suggest some scope of future work for this application.

2. Zero-Knowledge Proof Systems

The concept of zero-knowledge was first introduced by three MIT researchers, Shafi Goldwasser, Silvio Micali and Charles Rackoff [35], where they were working on interactive proof systems in which the prover convinces the verifier that some statement holds by sending interactive messages. Previously, the research work in this context was assumed to have an honest verifier where a malicious prover tries to convince the verifier about the correctness of some statement. These researchers turned the problem and gave a new aspect in which a verifier can also be malicious. Precisely, they emphasised; how much extra information the verifier can derive from the proof transcripts other than the fact that the statement holds.

Any ZKP proof system must have the following three properties:

- **Correctness:** If the statement is true, the prover should be able to convince the verifier with overwhelming probability.
- **Soundness:** If the statement is false, the prover should not be able to convince the verifier at any cost.
- **Zero-Knowledgeness:** The verifier must not be able to learn anything except that the statement holds.

Proving correctness can be done easily by playing multiple rounds of the protocol interactively giving a probabilistic guarantee to the proof system. To prove soundness, we make use of the existence of a knowledge extractor that interacts with the prover and can extract the witness from the transcripts if the protocol is completed successfully. The fact that the extractor can retrieve the witness from transcripts implies that the witness was injected into the transcripts by the prover.

The challenging part comes in proving the last property. Researchers have argued that zero-knowledgeness can be proven by using the concept of Simulation. If it can be proven that there exists a simulator that has no information and whose transcript is identically distributed to the real prover, then the verifier can extract the same amount of knowledge from

the real transcripts as can be extracted by simulated transcripts; however, as the simulated transcripts have no information in the first place, the verifier cannot extract any information from the real transcript as well.

2.1 Embedded Curves

Zk-Snarks uses many cryptographic primitives [2,6,7,8,12,17,30]. Besides, we discuss here the embedded curve used in Zokrates to link the identity with the prover [12].

In Zokrates, all arithmetic operations are defined on a finite field [30], specifically, a Galois Field, $GF(p^n)$ with $n = 1$. This means all operations are modulo p where p is the order of a group of elliptic curves [7]. In Zokrates, this p is defined as

$p = 21888242871839275222246405745257275088548364400416034343698204186575808495617$

This value is taken so that, it is equal to the group order of the BN128 curve used in Ethereum. This makes verification on the blockchain much cheaper as Ethereum provides precompiled contracts for the BN128 curve. As elliptic curve operations such as addition and multiplication involve modular arithmetic and modulo operations are inefficient in SNARKs, incorporating elliptic curve cryptography becomes very expensive in the Zokrates system.

This is solved using an embedded curve in Zokrates, BabyJubJub, which has parameters such that the order of the field over which it is defined becomes equal to the group order of the system curve. This way elliptic curve operations get reduced to the simple field arithmetic in Zokrates and make elliptic curve operations nearly free.

- P_s = Field Order of System Curve
- P_e = Field Order of Embedded Curve
- r_s = Group Order of System Curve
- r_e = Group Order of Embedded Curve

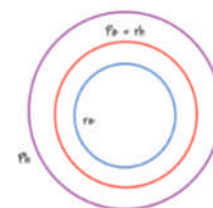


Figure 1: Embedded Curve

3. Understanding Zokrates

Zokrates is a toolbox that uses SNARKs for verifiable computations. It provides us with all the tools from specifying the constraints in DSL to export the verification code to Solidity smart contract. In this section, we discuss the details of the Pinocchio Protocol by PGHR13[26] and, finally, we discuss Zokrates.

3.1 Pinocchio Protocol

A verifiable computation contains three algorithms (**Setup**, **Compute**, and **Verify**). **Setup** takes the computation function, a security parameter, and converts it to Common Reference String (CRS). This will output a proving and verification key. **Compute** will take the computation function, inputs and proving key and gives the output to computation and proof. **Verify** will verify the proof using the verification key. Proof needs to be zero knowledge for our case.

We consider four important aspects of this protocol.

- **Correctness:** For any function F and any input u , if we run $(EK_F, VK_F) \leftarrow (F, I^k)$ and $(y, \pi_y) \leftarrow \text{Compute}(EK_F, u)$, then we always get $1 = \text{Verify}(VK_F, u, y, \pi_y)$. Here EK_F and VK_F are the evaluation and verification keys. This comes from

- the completeness property of proof systems.
- Security:** For any function F and any probabilistic polynomial-time adversary A , $\Pr[(u, y, \pi_y) \leftarrow A(EK_F, VK_F) : F(u) = y \text{ and } 1 = \text{Verify}(VK_F, u, y, \pi_y)]$ is negligible.
- Zero-Knowledgeness:** If $F(u, w)$ is a function with u as the public input and w as the private input, then given a proof π_y and output y for the given function F , there must not be any way of extracting w from the given information.
- Efficiency:** **Verify** must be cheaper as compared to **Compute**. **Setup** is also important but this depends on the underlying constraints, so the amortised cost is reasonable.

KEA Assumption (Knowledge of Exponent Assumption): For any adversary A , taking input g, g^a and returns (X, Y) with $Y = X^a$, there always exists a knowledge extractor K which given the same inputs as A , returns x such $g^x = X$. Additionally, if given two points A and B where $B = A^c$ and a point P , then the only way to calculate P^c is when P is derived from A ; that is, there exists some γ that is $\gamma A = P$.

Quadratic Programs: Now, we assume an arithmetic circuit and define a Quadratic Arithmetic Program (QAP). For simplicity, we assume a simple circuit as shown in Figure 2 with four inputs and two outputs from multiplication gates. p_1 and p_2 are the inputs to gate G_1 , p_3 , p_4 and p_5 are the inputs to gate G_2 (addition gates are not considered). p_5 and p_6 are the outputs of gates G_1 and G_2 , respectively.

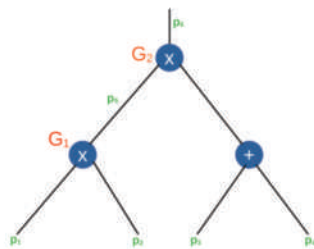


Figure 2: Circuit for QAP

QAP is defined as:

Q: Let $V = \{v_k(x)\}$, $W = \{w_k(x)\}$, $Y = \{y_k(x)\}$ for $k \in \{0..m\}$ be three sets of $m+1$ polynomials and $t(x)$, a target polynomial. Let F be a function taking n elements of F , giving n' outputs and let $N = n + n'$. Then, Q computes F if (p_1, p_2, \dots, p_n) is a legal assignment of F , iff \exists coefficients $(\pi_{N+1}, \dots, \pi_m)$ such that $t(x)$ divides $p(x)$. Here $p(x)$ is defined as

$$p(x) = \left(v_0(x) + \sum_{k=1}^m c_k(x) \cdot v_k(x) \right) \cdot \left(v_0(x) + \sum_{k=1}^m c_k(x) \cdot w_k(x) \right) - \left(y_0(x) + \sum_{k=1}^m c_k(x) \cdot y_k(x) \right)$$

The size of Q is m and degree is $\text{degree}(t(x))$.

Now we select a root $r_g \in F$ for each multiplication gate and express the target polynomial $t(x)$ as $\prod_g (x - r_g)$. V , W and Y are defined such that V encodes the left input for each multiplication gate, W encodes the right input and Y encodes the outputs. Also, we define

$$v_k(r_g) = \begin{cases} 1, & k^{\text{th}} \text{ wire is a left input to gate } g \\ 0, & \text{otherwise} \end{cases}$$

$w_k(r_g)$ and $y_k(r_g)$ are defined in a similar way. Now if we look at a specific gate G_i and its root r_g . Equation 4.1 becomes

$$\begin{aligned} & \left(\sum_{k=1}^m c_k(x) \cdot v_k(x) \right) \cdot \left(\sum_{k=1}^m c_k(x) \cdot w_k(x) \right) \\ &= \left(\sum_{k \in \text{left}} c_k \right) \cdot \left(\sum_{k \in \text{right}} c_k \right) \\ &= c_g \cdot y_k(r_g) = c_g \end{aligned}$$

which simply means that for any multiplication gate product of inputs is equal to the output.

Trusted Setup: We take KEA Assumption and extend it further by saying that if we have n pair of points $(P_1, Q_1), (P_2, Q_2), \dots, (P_n, Q_n)$, where $\forall i, P_i \cdot k = Q_i$ and we need to come up with two points (P, Q) such that $P \cdot k = Q$. Now if k is known, this becomes very trivial; therefore, k needs to be hidden or thrown out after using so that it cannot be used again. This dumping of toxic waste is important and the whole task of generating these points is known as a trusted setup and must only be performed by someone trustworthy. Considering this, the only way to come up with a point (P, Q) such that $P \cdot k = Q$ is when P is a linear combination of (P_1, P_2, \dots, P_n) and Q is a linear combination of (Q_1, Q_2, \dots, Q_n) which implies that the coefficients are known by the prover.

Verifiable Computation: In a real-world scenario, most of the time the polynomials V , W and Y are very large; therefore, we cannot use them directly. To solve this problem, polynomials are converted into elliptic curve points. Using elliptic curve points also helps in verifying the correctness. Formally, instead of sending polynomials V, W and Y , we send elliptic curve points in the form:

- $G * v_1(t), G * v_1(t) * k_v$
- $G * v_2(t), G * v_2(t) * k_v$
-
- $G * w_1(t), G * w_1(t) * k_w$
- $G * w_2(t), G * w_2(t) * k_w$
-
- $G * y_1(t), G * y_1(t) * k_y$
- $G * y_2(t), G * y_2(t) * k_y$
-

Here t, k_v, k_w and k_y are toxic wastes. Now assuming the extended KEA assumption, the prover needs to send the following values:

- $\pi_v = G * V(t), G * V(t) * k_v$
- $\pi_w = G * W(t), G * W(t) * k_w$
- $\pi_y = G * Y(t), G * Y(t) * k_y$

To make sure all these linear equations are using the same coefficients, this value is also added to the setup: $Q = G * (V(t) + W(t) + Y(t)) * b$. b is again the toxic waste. Then, we use elliptic curve pairings to verify that $V * W - Y = H - P$. We check that

$$e(\pi_v, \pi_w) / e(\pi_y, G) = e(\pi_h, G * P(t))$$

To check that all combinations are using the same coefficients, we again use the pairings and verify that Q matches with the provided $V + W + Y$.

3.2 Zokrates

Zokrates uses the idea of the delegation of computation. Computation is delegated to a single node rather than all nodes traditionally and that node executes the logic and publishes the result on-chain (Figure 3). This method gives two advantages.

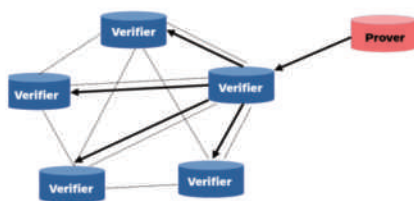


Figure 3: Delegated Computation in Zokrates

- The delegate node can use private information to execute the computation and publishes only the result. This is not possible in the traditional blockchain setting.
- Delegate Node only writes the result to the blockchain which increases efficiency in a way that all the nodes only store the result.

However, the problem here is any delegated node needs to be trusted. Therefore, the idea of verifiable computation is employed using Pinocchio Protocol. Delegated Node becomes the prover and computes the proof for computation, which is then verified by nodes on the blockchain. Privacy can be maintained by using zero-knowledge proofs.

3.2.1. Architecture

Zokrates supports writing the code in high-level language and converting it to a verification smart contract so that it can be deployed and the proofs verified on-chain. It has some inbuilt components for its processes. Below is the summary of each component in Zokrates.

- **Compiler:** Parsing and Flattening of Code is done by the Compiler inside Zokrates. After flattening, the constraints are transformed into a format that can be easily converted into R1CS constraints.
- **Witness Generator:** Before executing the program and generating the proof, the code must be given a valid assignment of input variables. The witness generator takes the valid inputs, interprets the flattened code and generates the witness.
- **Circuit Importer:** Sometimes, flattened code is hand optimised by developers. The circuit importer supports the functionality of importing the constraints directly into the Zokrates toolbox.
- **Setup and Proof Generator:** Setup takes the code and witnesses generating an evaluation and verification key. These keys are used in proof generation and verification.
- **Contract Generator:** According to the verification key, a solidity contract is generated which has all support for ECC operations using bn256g2 library and for providing elliptic curve pairing operations in verifyTx method which is called to verify the transaction.

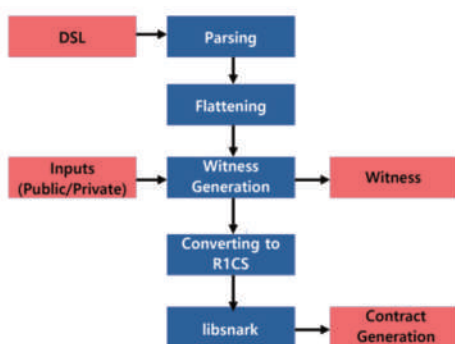


Figure 4: Zokrates Components

Zokrates internal processes are summarised in Figure 4. Zokrates can be used with three proving schemes currently, namely, PGHR13, Groth16 and GM17. In our application, we have mainly used PGHR13 and Groth16. Groth16 has some variations like shorter proof size (only 3 curve points are given as proof as compared to 8 in PGHR13) which makes it more efficient.

4. Problem Statement

Hedge Funds are more private investment firms. The fund manager after collecting the investment from all investors starts investing it. They use different strategies and statistical techniques to allocate the amount in different assets. This allocation is private to a firm and not disclosed by the fund managers as this might leak the strategies used by them. We define a set **A** containing all the assets in which a fund manager makes any investment.

$$A = \{A_1, A_2, \dots, A_n\}$$

Such that $|A|=n \in \mathbb{Z}$.

For any investor, his/her investment is allocated in different assets in **A**. We define these allocations by weight w_i (fraction of total investment assigned in a particular asset). These are also called portfolio weights. An allocation for an investor in different assets defines their portfolio. Portfolio weights are kept private by fund manager. Here **W** is the portfolio, w_i is the fraction of total investment invested in asset A_i .

$$W = \{w_1, w_2, \dots, w_n\}$$

Note that,

$$\sum_{i=1}^n w_i = 1$$

An example of 3-fund portfolio (having only 3 assets) is:

Table 1: Example 3-Fund Portfolio

Asset(A)	Allocation (w_i)
U.S. 'Total Market' Index Fund	0.6
International Stock 'Total Market' Index Fund	0.3
Bond 'Total Market' Index Fund	0.1

Investors in these funds expect the higher returns but they also expect that amount of risk should not be too high. For example, investing too much of an investment amount in an asset that has a higher risk degree might introduce a conflict of interest with the investors. An investor might not be comfortable with too much amount assigned to a single asset. To estimate the risk for each asset in the market, fund manager calculates the risk factor f_i . These quantities are public.

The fund managers need to convince the investor that they are following the guidelines and not investing too much of their money into a risky investment. So, the condition defined is

$$X \leq t = \sum_{i=1}^n w_i f_i \leq Y$$

where **X** and **Y** are the limits specified by investor. Sometimes risk factors are specified as the correlation between any two assets such that f_{ij} specifying the risk factor if both A_i and A_j are used

in high or low proportion. Correspondingly, non-linear conditions can be defined as

$$X \leq t = \sum_{i=1}^n w_i w_j f_{i,j} \leq Y$$

Sometimes, the investor also wants portfolio weights not to exceed a certain quantity for a single asset. This gives us the following (individual condition):

$$\forall i \in [1 \dots n] \quad w_i \leq h$$

where h is the individual risk threshold for each asset.

5. Protocol Workflow

In this section, we present a protocol to be used by the fund manager and investors that allows investors to be convinced that fund managers are behaving properly. After that, we discuss some implementation details.

5.1 Participants

- **Fund Manager/Prover:** Fund Manager needs to follow the protocol to convince the investor of specified conditions. (Or the Financial body may employ an auditor to accomplish this task of proving.)
- **Investor/Verifier:** Investors will give the conditions or agree upon predefined conditions, participate in the protocol and wait for the prover to convince him/her.
- **Government Regulatory Body:** Regulatory Body provides all the necessary guidelines that need to be followed by the fund manager/prover to avoid any conflict of interest with the investors and ensure transparency in some way.

5.2 Protocol

There are two phases in this protocol. Initial Phase and Use Phase.

5.2.1. Initial Phase

- The fund manager will publish the details of portfolio characteristics including the universe of assets(A), risk factors(F) and the public key to be used for convincing the verifier.
- Investors will only invest if they agree upon these points. Fund Manager deploys Record contract and publishes the contract address and ABI.
- Investors register themselves on Record smart contract and send the obtained ID to the Fund Manager on a secured private channel confirming their participation.

5.2.2. Use Phase

- Investors will compile the DSL specifying all conditions, the public key of the prover and export the verification smart contract by specifying their constraints.
- Investors deploy the contract on the blockchain, set the contract address and proving key hash on the Record smart contract.
- Investors can also provide their custom conditions and limits if agreed by the fund manager initially(optional).
- The prover/fund manager will compile the imposed DSL and make sure that the bytecode matches with the smart contract deployed. Prover, then computes the witnesses generating the proof in JSON format using their private key and proving key shared by the investor.
- The prover will upload the proof as JSON and call the verifyTx method on the smart contract.

- Verifier will watch for Success Event on the smart contract deployed to get convinced that all the conditions are satisfied, and that proof was generated by the fund manager only. If the event is not triggered, investor can report to the regulatory body.

Figure 5 gives a basic illustration of the protocol.



Figure 5: Protocol between Fund Manager and Investor

5.3 Implementation

The record contract deployed by the Fund Manager is written in pure Solidity. Full code can be found in Appendix A. The contract has three methods.

- **Register ():** This method is called by investors in Initial Phase. It generates a unique ID for each investor incrementally, stores the ID in the mapping with the investor address and returns the ID.
- **Set ():** This method is also called by an investor in Use Phase to set the Verifier address and proving key for them. It also verifies that only investors should be able to call this method for themselves.
- **Get ():** This method is called by the Fund Manager in Use Phase. It returns the Verifier address and proving key for a given Investor ID. It also verifies that only the fund manager(owner) should be able to call this method.

The DSL for Zokrates is prewritten and contains values like the public key of the fund manager, risk factors and so on. Values like X, Y and h are injected by the investor before compiling. As proving key is very large, storing it on the smart contract is not viable, so investor first uploads the key file on IPFS and stores the obtained IPFS hash on Record Contract. The prover then retrieves it by the given hash. There are n+1 private arguments for n portfolio weights. One input is the private key generated from BabyJubJub Curve. ECC library provides us with cryptographic support with Edwards Curve (embedded curve in Zokrates) which fits well within the context of Zokrates.

After compiling, constraints are converted to QAP and finally exported to Solidity smart contract. This contract is deployed on Ropsten Testnet by the investor sharing contract address and key hash on Record Smart Contract. The Fund Manager gets the contract address from the Record Contract. The Record Contract is compiled such that only the fund manager (owner) can get this data of investor and nobody else other than the investor can set their details like contract address etc. After getting the address, the fund manager computes the witnesses and generates the proof in the form of JSON which is used directly to call verifyTx function.

6. Evaluation and Results

In this section, we analyse and evaluate the processes involved in our protocol. We divide our evaluation into two parts: (1) On-chain verification and (2) off-chain processes like generating keys, generating proof, etc.

6.1 Verification on-chain

The most significant part of the protocol is on-chain verification. We performed our testing on Ropsten Testnet. As verifyTx method is dependent on proof and the number of public inputs, verification will take constant time in our application irrespective of the size of the asset list. Therefore, even with many constraints in our application, verification will always be efficient. We compared the verification for two protocols, PGHR13 and Groth16. As in Groth16, proof size is smaller as there are only three elliptic curve points, we found that Groth16 performance is better than PGHR13 with ≈ 0.2 million gas used in Groth16 as compared to ≈ 0.5 million in PGHR13. Also, in deployment, gas used by Groth16 is ≈ 0.9 million whereas, in PGHR13, it is ≈ 1.4 million. These values are the average of 20 transactions on Ropsten Network.

6.2 Off-chain Processes

Off-chain processes include compilation, key generation, exporting the verifier, computing witnesses and proof generation. PGHR13 scheme in Zokrates uses libsark as its backend. Compilation and exporting the verifier are the core Zokrates processes while generating keys and proofs are done by libsark in its components. First, we tested these steps using PGHR13 proving scheme on Zokrates and obtained the constraint system data for each number of assets.

Table 2: Constraints System Data in Zokrates

Assets #	Constraints #	Inputs(Private /Public) #	Variables #
10	17892	11	16005
20	29602	21	26144
50	64732	51	56565
100	123282	101	107265
200	240382	201	208665

Then to measure performance, we run a profiling routine for key-generation and proof generation on PGHR13 proving scheme using libsark as given in [29] with the data obtained. This layout uses a dense synthetic RICS structure, so all these results are the upper bound. For other processes like compilation, exporting the smart contract, and computing witnesses, we used time command on Linux Machine. Below is the data we obtained.

These results are calculated by taking the average runtime of 3 execution rounds for each step. From these results, we found that setup is the bottleneck for the verifier and takes most of the time.

Table 3: Profiling Results for Verifier

Assets #	Compile Time(X) (s)	Setup(Y)	Export-Verifier(Z)
10	0.069	6.816	0.009
20	1.427	11.342	0.011
50	2.519	20.600	0.063
100	4.961	51.536	0.509
200	7.717	97.342	0.143

Table 4: Profiling Results for Prover

Assets #	Compile Time(X) (s)	Compute-Witness(Y)	Proof-Gen(Z)
10	0.042	0.395	2.256
20	1.347	0.485	3.399
50	2.532	0.787	6.202
100	4.942	1.132	11.572
200	7.943	2.279	22.302

From the graph in Figure 6, we conclude that for a few hundred assets, the verifier can complete execution in approximately 8–9 minutes and the whole process can be completed in about a minute for a single investor.

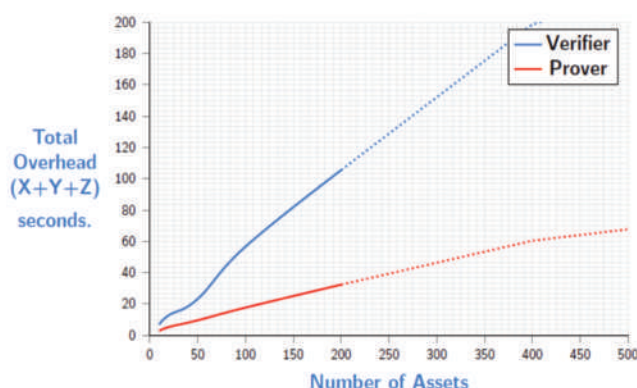


Figure 6: Total Overhead for Prover and Verifier

7. Conclusion

The protocol presented provides us with the ability to use zero-knowledge proofs in the financial regulatory system. Based on our implementation and analysis, we conclude that using Zokrates (or SNARKS) offers us a variety of ways to come up with the compliance system. Using this, a lot of real-world bottlenecks like paper trails and account-keeping can be avoided. Also, as every financial organisation must be compliant with a regulatory body, such as SEC, this use-case serves as an introductory solution to many regulation environments.

7.1 Scope for Future Work

In our implementation, we have made some assumptions that can be handled to improve the application and explore some other opportunities. For example, we assumed the precision of up to 10 bits for weight quantities. This can be further extended if the number of assets is lower in number such that the resulting risk measure can fit well in Zokrates field type. Also, we can try other types of conditions which might be important from the financial point of view. In addition to this, we can also come up with a different protocol that uses other proving schemes like Bulletproofs integrated with some refereed delegation approach to make the verification cheaper.

Appendix A

A.1 Record Contract

```

pragma solidity >=0.4.0 <0.7.0;
pragma experimental ABIEncoderV2;
contract Record {
    uint ID;
    address owner;
    struct cust_type {
        address addr;
        bytes key;
    }
}

```



```

mapping (uint => address) ad;
mapping (uint => cust_type) dta;
constructor () public {
owner = msg. sender;
ID = 0;
}
function register () public returns (uint){
uint t = ID;
ID=ID +1;
ad[t]= msg. sender;
return t;
}
function set (uint id, address sa, bytes memory ev_key) public {
assert (ad [id]== msg. sender);
dta [id]= cust_type ({
addr: sa,
key: ev_key
});
}

```

Reference:

- [1] (Last Amended, 2017). SEBI (Alternative Investment Funds Regulations, 2012). https://www.sebi.gov.in/legal/regulations/apr-2017/sebi-alternative-investment-funds-regulations-2012-last-amended-on-march-6-2017_34694.html.
- [2] Benarroch, D. (2019). Diving into the zk-SNARKs Setup Phase. <https://medium.com/qed-it/diving-into-the-snarks-setup-phase-b766024a0d7>.
- [3] Blog (2004). Witness-Indistinguishability. <https://www.isical.ac.in/~rbose/internship/lectures2016/r02feigshamir.pdf>.
- [4] Blog (2018). Decentralized Applications dApps. <http://blockchainhub.net/decentralized-applications-dapps/>.
- [5] Bootle, J., Cerulli, A., Chaidos, P., Groth, J., and Petit, C. (2016). Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In Fischlin, M. and Coron, J.-S., editors, *Advances in Cryptology {EUROCRYPT 2016}*, pages 327-357, Berlin, Heidelberg. Springer Berlin Heidelberg.
- [6] Buterin, V. (2016). snarks. <https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-ber0-f6d558cca649>.
- [7] Buterin, V. (2017a). Exploring Elliptic Curve Pairings. <https://medium.com/@VitalikButerin/exploring-elliptic-curve-pairings-c73c1864e627>.
- [8] Buterin, V. (2017b). Zk-SNARKs: Under the Hood. <https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6>.
- [9] Bunz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., and Maxwell, G. (2018). Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (SP), pages 315-334.
- [10] Math.columbia.edu. 2021. [online] Available at: <<http://www.math.columbia.edu/~rf/extensionfields>>.
- [11] Lexology.com. 2021. Maintaining confidentiality in fund documents: a realistic expectation? | Lexology. Available at: <<https://www.lexology.com/library/detail.aspx?g=49d88904-352d-4ad7-8a33-a9534443158a#:~:text=Fund%20managers%20are%20typically%20keen,they%20disclose%20to%20potential%20investors.&text=Hedge%20fund%20managers%20and%20others,be%20reassured%20by%20the%20result>>.
- [12] Deml, S. (2019). Efficient ECC in zkSNARKs using ZoKrates. <https://medium.com/zokrates/efficient-ecc-in-zk-snarks-using-zokrates-bd9ae37b8186>.
- [13] Eberhardt, J. and Tai, S. (2018). ZoKrates - scalable privacy-preserving off-chain computations. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1084-1091.
- [14] Ethereum (2019). Learn about Ethereum. <https://ethereum.org/learn/>.
- [15] Feige, U. and Shamir, A. (1990). Witness indistinguishable and witness hiding protocols. In *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, STOC '90*, page 416-426, New York, NY, U.S.A. Association for Computing Machinery.
- [16] Flood, M. D., Katz, J., Ong, S. J. J., and Smith, A. (2013). Cryptography and the economics of supervisory information: Balancing transparency and confidentiality. *Microeconomics: Asymmetric Private Information eJournal*.
- [17] Fondation, Z. (2017). zk-snarks. <https://z.cash/technology/zksnarks/>
- [18] Govravarum, N. R. (2018). Zero Knowledge Proofs and Applications to Financial Regulation. <http://nrs.harvard.edu/urn-3:HUL.InstRepos:38811528>
- [19] Green, M. (2014). Zero Knowledge Proofs: An illustrated primer. <https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/>.
- [20] Green, M. (2017). Zero Knowledge Proofs: An illustrated primer2. <https://blog.cryptographyengineering.com/2017/01/21/zero-knowledge-proofs-an-illustrated-primer-part-2/>.
- [21] Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Fischlin, M. and Coron, J.-S., editors, *Advances in Cryptology {EUROCRYPT 2016}*, pages 305-326, Berlin, Heidelberg. Springer Berlin Heidelberg.
- [22] JonathanKatz (2004). Witness-Indistinguishability. <http://www.cs.umd.edu/~jkatz/gradcrypto2/NOTES/lecture21.pdf>.
- [23] Lutkebohle, I. (2008). BWorld Robot Control Software. <http://aiveh.techfak.uni-bielefeld.de/content/bworld-robot-control-software/> [Online; accessed 19-July-2008].
- [24] matter lab (2020). Awesome zero knowledge proofs (zkp). <https://github.com/matter-labs/awesome-zero-knowledge-proofs>.
- [25] Menezes, A. (2005). *An introduction to pairing-based cryptography*.
- [26] Parno, B., Howell, J., Gentry, C., and Raykova, M. (2013). Pinocchio: Nearly practical verifiable computation. In 2013 IEEE Symposium on Security and Privacy, pages 238-252.
- [27] Pass, R. and Venkatasubramanian, M. (2010). Private coins versus public coins in zero-knowledge proof systems. In Micciancio, D., editor, *Theory of Cryptography*, pages 588-605, Berlin, Heidelberg. Springer Berlin Heidelberg.
- [28] scipr lab (2020a). C++ library for zkSNARKs. <https://github.com/scipr-lab/libsnark>.
- [29] scipr lab (2020b). Profiling Libsnark. https://github.com/scipr-lab/libsnark/tree/master/libsnark/zk_proof_systems/ppzk-snark.
- [30] Stanford (2014). Finite Fields. <https://web.stanford.edu/class/ee392d/Chap7.pdf>.
- [31] Sztybel, M. (2005). Risk assurance for hedge funds using zero knowledge proofs. In Patrick, A. S. and Yung, M., editors, *Financial Cryptography and Data Security*, pages 156-171, Berlin, Heidelberg. Springer Berlin Heidelberg.
- [32] Teutsch, J., Straka, M., and Boneh, D. (2019). Retrofitting a two-way peg between blockchains.
- [33] ZoKrates (2019). ZoKrates. <https://github.com/ZoKrates/ZoKrates>.
- [34] SEC.gov | Hedge Funds – A New Era of Transparency and Openness
- [35] S Goldwasser, S Micali, and C Rackoff. 1985. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing (STOC '85)*. Association for Computing Machinery, New York, NY, USA, 291–304. DOI: <https://doi.org/10.1145/22145.22178>
- [36] Damgård, Ivan & Nielsen, Jesper. (2008). Commitment Schemes and Zero-Knowledge Protocols (2007). *Lecture Notes in Computer Science - LNCS*.
- [37] NTL: A Library for doing Number Theory (libntl.org)
- [38] <https://www.sec.gov/news/statement/aguiar-effective-regulatory-oversight-and-investor-protection.html>

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

Komal Kalra is the main author responsible for writing the manuscript, collecting data, proofreading, etc.

Funding:

National Blockchain Project Funds by National Security Council Secretariat, Government of India.

Acknowledgements:

Not applicable.

CONFERENCE PROCEEDINGS

3rd Blockchain International Scientific Conference 15 March 2021, ISC2021, UK

1. Blockchain Matters – on the phenomenon of disembodiment in blockchain law

Katrin Becker
University of Luxembourg
Category: Oral Presentation

Abstract

My paper will examine the phenomenon of disembodiment that underly the conceptions of law and subjectivity in the context of blockchain technology. The term disembodiment is here to be understood in the broadest sense, i.e. as an abstraction from body, corpus and nomos – in compliance with the blockchain-based conceptions of a disembodied e-subject, of a de-territorialized law, i.e. a law dissociated from both the territorial and the textual body, and the creation of cloud, i.e. matter-free, communities. Starting from a legal philosophical reflection on the relationship between body, corpus and nomos, I will analyze the consequences that the tendencies of disembodiment in the context of blockchain applications have for general questions of law and legal subjectivity. My paper sets out to show to what extent blockchain technology, with its conception of a robotic, decentralized and personalized law (*lex cryptographica*) as well as of a disembodied self-sovereign identity concerns not only the virtual sphere of blockchain applications. But by creating two different – and conflicting – worlds of legal execution, it develops an acute relevance for the "real world" that urgently needs to be addressed by both the traditional legal system as well as by the blockchain world.

Keywords: *Blockchain – disembodiment – legal subjectivity – representation – legal philosophy*

2. Identity of Things – applying concepts from selfsovereign identity to IoT devices

Tim Weingärtner
Blockchain Lab, Lucerne University of Applied Sciences
Category: Oral Presentation

Oskar Camenzind
Building Technologies Division, Siemens Schweiz AG
Category: Oral Presentation

Abstract

The rapidly growing number of devices used for the Internet of Things (IoT) is raising concerns about the origin and history of these devices. Identity becomes a crucial property of IoT devices. So far there are primarily proprietary solutions. In a multi-provider environment those kinds of approaches have major disadvantages since the customer himself is responsible for administration.

Our research addresses this issue by proposing an approach based on blockchain and decentralized identifiers (DID). It is inspired by the concepts of self-sovereign identity (SSI) and bootstrapping of remote secure key infrastructures (BRSKI). Devices are equipped by the manufacturer with an identity stored in a trusted execution environment (TEE) and secured by a blockchain. This identity can be used to trace back the origin of the device. During the bootstrapping process on the customer side, the identity registration of the device is updated in the blockchain. This process is performed by a so-called registrar. Smart contracts prevent unsolicited transfer of ownership and track the history of the device. Besides proof of origin and device security our concept can be used for device inventory and firmware upgrade.

A prototype implementation was realized to validate the concept. Six use cases have been implemented and tested using an Ethereum blockchain. JSON Web Tokens (JWT) have been used as signed artefacts to transfer information between the stakeholders. This enables an asynchronous communication needed in an offline environment. The proposed infrastructure can be provided by an independent association and can be used by all manufacturers.

Keywords: *Blockchain, Internet of Things, Identity, DID, JWT*

3. Investment Compliance in Hedge Funds using Zero Knowledge Proofs

Komal Kalra

Indian Institute Of Technology Kanpur, India

Category: Oral Presentation

Abstract

Financial Regulation is a form of compliance system which subjects financial institutions to certain requirements and restrictions. Investment Compliance is an example of this which involves investment restriction monitoring on behalf of investors. Hedge funds differ from other investment funds like mutual funds due to their ability to employ complex investment and hedging techniques. These are private entities having few public disclosure requirements. Confidentiality is good as it allows financial agents to participate in the financial markets without any fear of information leakage, hence promoting liquidity. But, this is often implied as a lack of transparency.

Hedge Funds are expected to produce higher returns as compared to other funds, but sometimes investors also seek a risk guarantee in addition to higher returns. But too much transparency rules out the incentives that financial entities have by participating in the first place. On the other hand, too much secrecy may give rise to malicious entities that can break the rules due to a lack of compliance. We aim to solve this problem of protecting the investors while ensuring the privacy of financial agents using zero-knowledge proofs. Proofs can be visualized as a way of providing sufficient information to investors while the zero-knowledge property of proofs maintains the privacy of fund managers' strategies. We propose a protocol to address this scenario using Zokrates, a framework for verifiable computation using Zk-SNARKs on Ethereum, to encode the constraints and export the verifier. Based on our implementation and analysis, it can be concluded that zero-knowledge proofs offer us a variety of ways to come up with the compliance systems.

Keywords: *compliance, investors, fund manager, proofs, transparency, financial, funds*

4. Model-driven development of blockchain-based platforms in the algebraic virtual machine environment

Dr. Oleksandr Letychevskyi

LitSoft, Ukraine

Category: Oral Presentation

Abstract

The paper is dedicated to the analysis of blockchain-based platforms with the purpose of verification and for exploring their resistance to possible attacks during the development process. It uses the algebraic approach realized in the Algebraic Virtual Machine (AVM) created by our team that accepts blockchain system models on different levels of abstraction. The variety of algebraic methods allows the resolution of verification problems and the detection of vulnerabilities in blockchain-based systems by using symbolic modelling and algebraic matching of behaviours.

The behaviour of blockchain systems can be presented as a model in behaviour algebra specifications. We can thus consider the algorithm of consensus, smart contract or some slice of the design of a blockchain-based platform, especially the token economy aspect. A blockchain is a distributed system, and the methods of resolving behavioural equations in the scope of theory of agents and environment interactions implemented in the AVM are applicable. This can resolve the problem of reachability of undesirable behaviour or possible attacks from the external environment.

Such practices could be used in the development of safety critical or reliable blockchain applications and be part of a development process. The use of models on different levels of abstraction could also be applied in testing activities for test suite generation and symbolic test execution. The first experiments with the AVM application were realized with attack resistance in POS consensus algorithms testing, Ethereum smart contract (Solidity) verification and token economy projects analysis.

Keywords: *algebraic modelling, symbolic execution, smart contracts, consensus algorithms, distributed systems, formal verification, model-based testing*

5. A Conceptual Model for Constant Storage Blockchain

Yuvaraj Rajendra, Sachin Sahu, Venkatesan Subramanian, Sandeep Kumar Shukla

Indian Institute of Information Technology, Allahabad

Category: Oral Presentation

Abstract

The growing storage requirements are always an issue with blockchain platforms, and devices may not be able to allocate the required storage to replicate an entire blockchain instance. There are applications that use blockchain and are not required to maintain the old transaction details throughout their life-cycle. In such applications, there is no need to maintain the complete growing blockchain, only recent sets of blocks are sufficient. The IOTA tangle provides a solution through snapshots. However, nodes such as permanent and developer nodes maintain the entire tangle or IOTA transactions. Only keeping recent blocks would create possibilities of false chain replacement attack and a false block insertion attack if all nodes store only a random part of the blockchain. To overcome this false block insertion and chain replacement attack, while all nodes store a random part of the blockchain, we propose a conceptual model that divides the growing blockchain into fixed-size sets of blocks, excluding the genesis block. In case a node decides to not replicate a few sets of blocks to accommodate the blockchain according to its storage availability, it stores the corresponding set's last block hash. Nodes that receive blocks, equivalent to the omitted blocks, from other nodes will validate the set's last block hash with the received set's first block parent hash. If they match, it will accept the equivalent set of deleted blocks. This will provide guarantee towards avoiding any insertion and replacement attacks. It is mandatory for the nodes that send blocks, equivalent to omitted blocks, to include all the blocks in a set. This model can save more than 99% of storage usage if we consider the header size of 500 Bytes and a set size of 10. It further saves if we increase the set size.

Keywords: *Less Storage, Blockchain, Chain Replacement Attack*

6. HoneyBadgerBFT as an ordering service in Hyperledger Fabric

Deepak Yadav

IIT Kanpur

Category: Oral Presentation

Abstract

We are living in a blockchain era where both academic and industry people are interested in blockchain technology. It all started with the introduction of bitcoin by Satoshi Nakamoto; the world's first decentralized cryptocurrency, it can be termed as the first phase of blockchain technology. In the second phase, Ethereum got the success more people got interested in blockchain technology. Now we are in the third phase of the blockchain revolution that is the blockchain for enterprise. Now, every business is trying to take advantage of blockchain technology for their use case, and in this phase, Hyperledger Fabric is the most promising modular enterprise blockchain. It is proven to be very useful, but we noticed that official hyperledger fabric implementation still doesn't support any BFT protocol for consensus (or ordering service) and above all, there is no practical implementation of a Byzantine fault tolerant consensus protocol that can perform in network settings, such as the Internet where the user of the blockchain can not provide network guarantees. In this thesis, We present an alternative, HoneyBadgerBFT as a consensus option in Hyperledger Fabric's Ordering service, the first practical asynchronous BFT protocol, which guarantees liveness without making any timing assumptions about the network. HoneyBadgerBFT can handle up to one-third malicious nodes in the network. We present an implementation and experimental results to show that our protocol can achieve throughput comparable to Raft (a CFT protocol) in standard scenarios and makes progress even when the underlying network is not stable.

Keywords: *Blockchain, Consensus, Hyperledger, HoneyBadgerBFT, async BFT*

7. Strategic Value Creation Through Enterprise Blockchain

A. Aziz, Y. Sarason and K. Yuthas

Colorado State University (Aziz and Sarason) and Portland State University (Yuthas)

Category: Oral Presentation

Abstract

Blockchain and other distributed ledger technologies have enormous potential for creating business value. When used collaboratively, these systems can remove friction and increase security across a business network and create value by verifying the origin of data and tracking data through workflows. Despite their potential, these systems have not been widely adopted, which we attribute to incomplete assessment of their potential returns. Enterprise blockchain systems are often promoted as solutions to existing operational problems or ‘pain points’ and their potential strategic value is not well understood. Drawing from literature on strategic alliances and the resource-based view of the firm, we demonstrate how enterprise blockchain systems can contribute to a firm’s strategic capabilities and, as a result, to sustained competitive advantage. We provide a framework for understanding how participation in blockchain projects can enable companies to strengthen existing strategic capabilities and to build new collaborative and blockchain-specific capabilities. The framework can be useful to firms and service providers for incorporating strategic outcomes into the evaluation of blockchain investment opportunities.

Keywords: *resource-based view, strategic alliance, enterprise, strategic capabilities, consortium*

JEL Classification: *M15 IT Management*

8. Consortium Capabilities For Enterprise Blockchain Success

S. Heister, M. Kaufman, and K. Yuthas

Portland State University

Category: Oral Presentation

Abstract

Enterprise blockchain projects great promise. They can cut costs and promote efficiency through disintermediation, increase transparency for tracking inter-company transactions, expand knowledge through consortia databases, and improve workflows through shared business processes. Despite its potential, blockchain technology has failed to produce promised benefits for enterprise networks. While the underlying technology has advanced rapidly, managerial capabilities needed to form and manage blockchain consortia have lagged, and few consortia have succeeded. We provide a framework that identifies foundational conditions that precede effective consortium formation, capabilities required for effective consortium functioning and evolution, and partner and ecosystem-level outcomes associated with successful blockchain projects.

Keywords: *enterprise blockchain, strategic capabilities, consortium, success factors*

JEL Classification: *M15 IT Management*

9. Biosample Tokens, Identity Tokens, and Permission Tokens, the Symphony of Private and Secure Health Care

W. Entriken¹, D. Uribe²

¹Private Consultant, Philadelphia, PA, United States ²GenoBank.io, Palo Alto, CA, United States.

Category: Oral Presentation

Abstract

Three interrelated token models are introduced—using a blockchain registry it is possible to record self-sovereign identities, well-known identities and permissions to share data. This meets the requirements to deploy a secure and anonymous data sharing system and privacy framework. We explore how file sharing can be built on top of this trust framework which allows anonymous individuals to share information with well-known entities and have confidence that it will not be shared outside of what they have permitted. Practical implementation details are reviewed such as using commercial off-the-shelf file storage and creating commercial relationships between the well-known parties. By allowing this secure file exchange and anonymous self-sovereign file creation, we hope to allow new applications in the health care sector. Overall, patients in health care in the United States have been abused with data breaches and endless HIPAA forms that grant no-recourse permanent data sharing. By providing an alternative that collects no identifying information and restricts data sharing, we hope to enfranchise more patients that may have previously been hesitant to participate.

Keywords: *privacy, patient care, data management, health information, health information system, HIPAA, data security, patient confidentiality, non-fungible tokens, identity management, public-private key, elliptic curve cryptography*

10. Implementation of Blockchain Technology to the International Trade and Custom Regulations

Bedrettin Gürcan

University of Sıgeed Faculty of Law and Political Science

Category: Oral Presentation

Abstract

Blockchain is a technology, which has several advantages to be used in quite wide areas such as payment solutions to transportation. Using blockchain technology in international trade may have impressive promises and potentials.

In our research, we aim to discuss the potential and existing implementation of blockchain technology into international trade and custom practices. It is important to make comprehensive due diligence of the blockchain technology in order to determine which functions of the blockchain technology can be implemented in the international trade environment.

Parties of international trade are traders, governments, business consortiums, insurance companies, financial bodies as banks or creditors. Custom procedures are one of the most bureaucratic steps of international trade. The problem that both side of the import and export customs should check the documentation of shipping, country of origin proofs, the validity of the whole documents from beginning to end. For instance, manual cross valuation of the customs declarations takes plenty of time and human force during international trade transactions. Blockchain can automate the procedures.

The first role of blockchain in this example can come with its traceability feature, which enables parties to record a chain of transactions to trace the movement of goods internationally with instant and accurate information. The multiple parties of the international trades claim huge paperwork load either for traders or government agencies and 3rd parties as banks and carriers. There are middlemen to check and record payments, movements, details of the good. Blockchain has the potential to solve these complexities of the procedures simultaneously.

Blockchain platforms can globally manage records import-export declarations, bills of lading, invoices and certificates of origin, and any sort of documents. Customs documents can be processed and tracked through blockchain solutions. Hence it provides better audibility and expedites the processing of international trade. The biggest motivation to use blockchain technology in custom procedures is cost reduction and safer trade. Blockchain decentralized and transparent features can be used against fraudulent documents and fake signature submissions.

Self-executing contracts (Smart Contracts) enables small-medium enterprises to join international trade by means of low cost and less bureaucratic barriers of the trade. It may reduce the legal and procedural costs of the process and secure against the risk of non-payment. Blockchain-based custom practice can provide access to trade finance and facilitating trade procedures for small-medium enterprises.

The basic premises of the blockchain technology for international trade are workflows across organizations of the trade and simplified business processes, secure by design, transparency, and immutable audit trails. It is important to bear in mind that blockchain can track and guarantee that uploaded data is not tampered with, nevertheless do not guarantee that the recorded data is accurate.

There has been an inconclusive debate about whether blockchain technology is reliable or not. Interoperability and scalability of early-stage technology have been discussing by relevant authorities. Hence, regulatory and legal acceptance is still a big question.

The underlying argument against using blockchain technology in the custom procedure is that interoperability of standardization. It is important to have standardized software in order to be accessed and accepted by international traders and by both sides of custom bodies.

In sum, private permissioned blockchains managed by parties of international trade bring business-friendly, fast, accurate, and low-cost international trade procedures. It is important to standardize the infrastructure and make authorities to accept to use of these platforms.

11. Blockchain Technology For Supply Chain: Challenges and Architectural Design Processes

Gokhan Kirbac, Ph.D
 Istanbul Kültür University, Turkey
 Category: Oral Presentation

Abstract

Today, as a result of the rapid development of technology, the concepts of information technologies and digital transformation have become crucial for supply chain. Therefore, the responsiveness, complexity, and number of actors involved in supply chain have also increased. Here, lots of technologies, software and methods exist to support the flow of the products in supply chain processes. The effectiveness of these technologies is key to making sure supply chain remain efficient. Blockchain as a disruptive technology may ensure support for an innovative structure of supply chain management. However, as with any new technology, there are some implementation challenges and stages for the installation architecture in blockchain technology. The aim of this study presents a comprehensive and descriptive case study for applying blockchain technology in supply chain. For methodology part of the study, semi structured and in-depth interviews are conducted with supply chain managers and blockchain technology experts. According to analyzes and dimensions gathered from interviews are discussed in detail. In this context, it has been noted that businesses may face a number of significant challenges when they want to implement blockchain technology in their current workflow processes. Furthermore, when businesses want to get support and consultancy for blockchain technology from a technology company, the architectural setup and prerequisites of the blockchain are determined from beginning to end. Lastly, it is important for businesses to provide these blockchain design processes and steps to ensure rapid technology adaptation and competitive advantage. This paper is a descriptive study that serves as a roadmap for businesses that want to implement blockchain technology in supply chain operations.

Keywords: *Blockchain technology, supply chain, blockchain architectural design, blockchain challenges*

12. Blockchain and Supply Chain Finance: A Critical Literature Review from a Business and Management Perspective

Ilias Ioannou
 Queen Mary University of London
 Category: Oral Presentation

Abstract

This review summarises and synthesises existing research on the interaction between Blockchain technology and Supply Chain Finance (SCF). In the current state of affairs, where the Covid-19 pandemic has exposed the vulnerabilities of our paper-based trade and supply chain finance systems, digital transformation seems to be the only way forward. The purpose of this submission is to explore the status, theoretical perspectives and industry applications regarding Blockchain as the medium toward digitalisation, and to underline how specific features of this disruptive technology can address existing inefficiencies in SCF. The study conceptualises and theorises that, as the difficulty of accessing reliable supply chain data is the main challenge to innovation in the SCF sphere, the increased visibility of supply chain movements provided by Blockchain can provide better SCF solutions. As a first step toward Blockchain adoption, it considers the conditions necessary for Blockchain-enabled trade and supply chain finance to emerge. It further argues that future research should focus on the implementation process, suggesting a transformation in business practice toward more collaborative business models. The review contributes to understanding the current state of research in the field, highlights the identified gaps and, by providing an analytical basis for future empirical research on Blockchain and SCF, it provides exploratory directions and assists in the theory-building process.

Keywords: *Blockchain – Distributed Ledger Technology– Supply Chain Finance – Trade Finance – Supply Chain Management – Ecosystem*

JEL Classification: *K20, K22, K24, L14, L81, L91, O31, G38, F13, F23, F44*

13. Stamping Out Counterfeits with Blockchain E-commerce - A Study based on Theory and Laboratory data

David Lee Kuo Chuen^a, Yang Li^b, Fan Liu^b, Weibiao Xu^a

^a*School of Business, Singapore University of Social Sciences*

^b*School of Finance, Nankai University*

Category: Oral Presentation

Abstract

33% of buyers suffered from fake products based on a survey of users who transact on a Blockchain-based online shopping platform provided by Origin Protocol Inc, raising the question of whether and how Blockchain will be an effective and efficient solution to tackle the counterfeiting problem for E-commerce. In this paper, we construct a novel Blockchain-based trading model in which the seller may deliver a fake product and the buyer can verify its quality by paying a cost. Besides creating a tamper-proof chain of transaction data, in our proposed model, Blockchain is able to record sellers' fraudulent behavior and make it available to the public. We prove that, in a dynamic game theory framework, disclosing seller's misconduct can reduce the incentives of selling counterfeiting goods compared to the mechanism with no such disclosure. This crucial result is also identified in a trading experiment. Less or even none subjects sell counterfeits when sellers' records of fraud are made public. This paper theoretically and experimentally shows how Blockchain can actively reduce fraudulent transactions and create a better E-commerce market.

Keywords: *Blockchains, E-commerce, Fraud, Trust, Game Theory*

JEL Classification: *D47, D8, F14, G4*

14. Stamping Out Counterfeits with Blockchain E-commerce - A Study based on Theory and Laboratory data

David Lee Kuo Chuen^a, Yang Li^b, Fan Liu^b, Weibiao Xu^a

^a*School of Business, Singapore University of Social Sciences*

^b*School of Finance, Nankai University*

Category: Oral Presentation

Abstract

33% of buyers suffered from fake products based on a survey of users who transact on a Blockchain-based online shopping platform provided by Origin Protocol Inc, raising the question of whether and how Blockchain will be an effective and efficient solution to tackle the counterfeiting problem for E-commerce. In this paper, we construct a novel Blockchain-based trading model in which the seller may deliver a fake product and the buyer can verify its quality by paying a cost. Besides creating a tamper-proof chain of transaction data, in our proposed model, Blockchain is able to record sellers' fraudulent behavior and make it available to the public. We prove that, in a dynamic game theory framework, disclosing seller's misconduct can reduce the incentives of selling counterfeiting goods compared to the mechanism with no such disclosure. This crucial result is also identified in a trading experiment. Less or even none subjects sell counterfeits when sellers' records of fraud are made public. This paper theoretically and experimentally shows how Blockchain can actively reduce fraudulent transactions and create a better E-commerce market.

Keywords: *Blockchains, E-commerce, Fraud, Trust, Game Theory*

JEL Classification: *D47, D8, F14, G4*

15. Blockchain-hosted Data Access Agreements for Remote Condition Monitoring in Rail

Rahma A Alzahrani and Simon J Herko
University of Birmingham and TravelSpirit Foundation
 Category: Oral Presentation

Abstract

Through advanced sensor technologies, satellite-based authentication, and high bandwidth data networks, Remote Condition Monitoring (RCM) systems are now an essential 'Internet of Things' (IoT) resource for efficient operation of railway infrastructure. However, the full potential of this big data has yet to be realized. Data is currently collected and used in siloes, with limited visibility of all possible datasets for exploitation. The RSSB on behalf of the UK Rail Industry established a cross-industry research program, T1010, to build stronger cooperation between stakeholders in sharing RCM data. This research builds upon T1010, to explore the use of blockchain and smart contracts to automate, in an auditable and tamper-proof way, the commercial agreements and payment processes for data trading. By removing the limitations of paper-based agreements, our goal is to enable innovation in shared business processes and an IoT data marketplace. Building on existing smart contract-based schemes for trading and sharing IoT data over blockchain networks, this research identifies novel ways to enforce agreements and ensure fair cost attribution between parties, without a Trusted Third Party. The initial design of a blockchain-based framework is presented, oriented around the data provider, consumer, and smart contracts. Blockchain-hosted data access agreement and accounting models are specified in detail. The processors in the efficient permissioned blockchain platforms Hyperledger Fabric, Sawtooth, and Iroha have been analyzed for their suitability for implementation. We then outline our future work to evaluate and validate two industrial use cases: monitoring systems for unattended overhead line equipment and axle bearings.

Keywords: *Big data, Blockchain, Remote Condition Monitoring, Cost attribution, Process automation*

JEL Classification: *L92, O31*

16. Understanding the synergies between GNSS and Smart Contracts for enabling Micro-logistics applications

Simon J Herko
TravelSpirit Foundation
 Category: Oral Presentation

Abstract

The UK domestic parcels market is highly fragmented with 16 major national carriers, delivering in excess of 2.5 billion parcels in 2020. Covid-19 pandemic has accelerated home-working and e-commerce trends. Many local deliveries remain unconsolidated, and therefore generate higher driver mileage than necessary, creating inefficiencies and negative environmental impacts. Even if a customer orders two items from the same retailer, they often receive two separate deliveries. The Galileo program is Europe's initiative for a state-of-the-art global satellite navigation system (GNSS), providing a highly accurate, guaranteed global positioning service under civilian control and the first to offer authenticated navigation messages to all civilian users in the world, free of charge; i.e. open-source. Blockchain technology and its Smart Contract capabilities is already well-established as a promising solution for governments and the supply-chain; to enable shared business processes that require high levels of trust, transparency and accountability. This includes major government backed programs by the EU, US, India and China. Our proposed research explores the feasibility of a micro-logistics platform for last-mile delivery consolidation operations. Increased real-time visibility and transparency of contractual arrangements and parcel tracking data will enable greater efficiency in managing deliveries and minimise the overall transport costs and carbon footprint. It examines new capabilities arising from fusion of satellite based authenticated timing and positioning with blockchain technology, combining the baked-in cryptography of both systems to provide a secure and efficient micro-logistics solution. An initial design of a blockchain-based framework will be developed, oriented around the consumer, retailer, carriers, local couriers, micro-consolidation-centre (MCC) and smart contracts. With the cities of Stratford-upon-Avon and Canterbury as our test-bed locations, we set out to prove: How many trips can we save? How can we improve the transparency, accountability and data authenticity of parcel orders? How can we enable trusted contractual arrangements? How can we lower the cost barrier for establishing MCCs?

Keywords: *Blockchain, Logistics, GNSS, E-Commerce, Freight Consolidation*

JEL Classification: *L91, O31*

THE BBA STUDENT FORUM

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

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

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

REASONS TO START THE BBA STUDENT CHAPTER

Encourage student collaboration

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

Connect to industry professionals and career opportunities

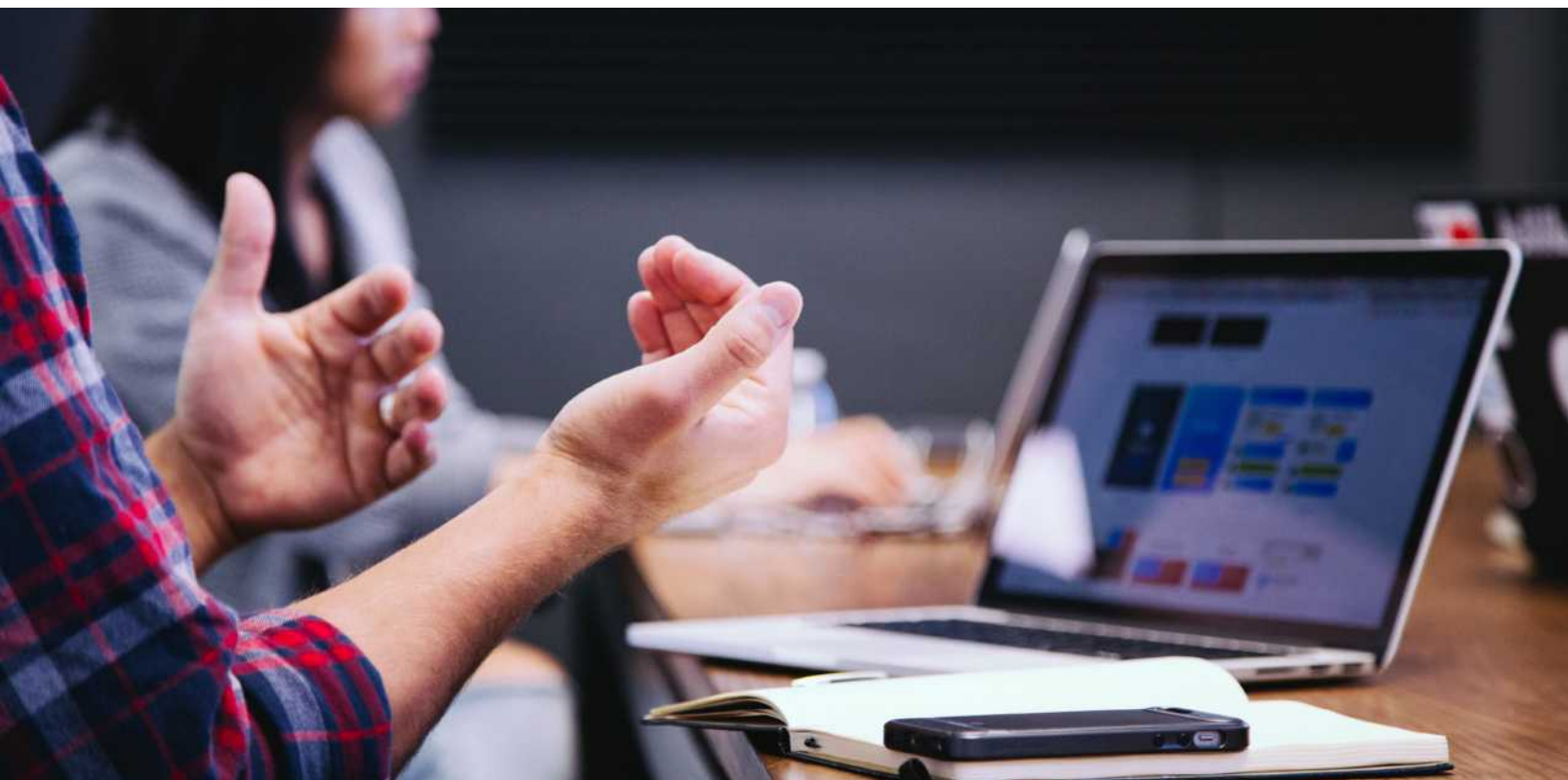
Obtain leadership experience driving BBA student chapter activities

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

Compete in hacking events

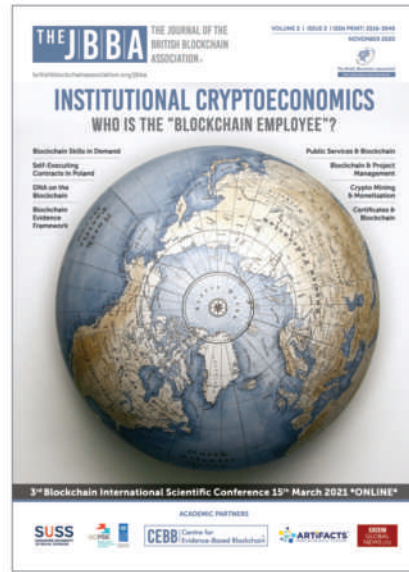
Publish papers in the JBBA

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





Volume 3 - Issue 1
May 2020



Volume 3 - Issue 2
November 2020



Volume 2 - Issue 1
May 2019



Volume 2 - Issue 2
October 2019



Volume 1 - Issue 1
July 2018



Volume 1 - Issue 2
December 2018

DISCLAIMER

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

© The British Blockchain Association and The JBBA. All rights reserved.



is a trade mark of the Journal of the British Blockchain Association.

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

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

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



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: jba.scholasticahq.com

Advertising

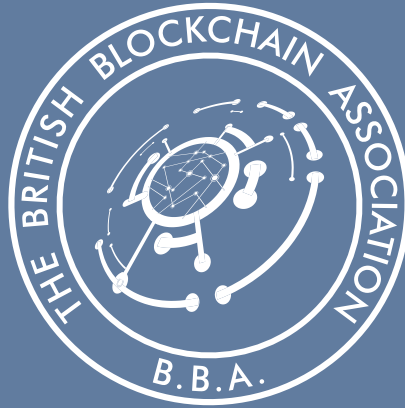
All advertisements and sponsorships are expected to conform to ethical and business standards. The appearance of an advertisement or sponsorship material does not constitute an endorsement by the British Blockchain Association or by the Editor of this Journal.

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:
britishblockchainassociation.org/jbba



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
- Free 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 August 2021)

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

WHY BECOME AN ACADEMIC PARTNER OF THE JBBA?

Your logo will appear on the front cover 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

HIGHLIGHT



Your organization's position as a leader in the Blockchain community

ENHANCE



Your organization's exposure in the Blockchain arena

CONNECT & NETWORK



With an esteemed group of eminent researchers, scholars, students and academics in Blockchain space

CREATE



An investment value for your organization through co-branding with world's premiere Blockchain Research journal

BUILD



Long term relationships with key stakeholders and market leaders in the field of Blockchain, Distributed Ledger Technology and Cryptocurrencies

MAXIMISE



Your organisation's visibility, make new contacts and reach your target audience by putting your name prominently in front of each and every reader of the JBBA

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 | admin@britishblockchainassociation.org

Follow us on:





The British Blockchain Association[®]

Advocating Evidence Based Blockchain

www.britishblockchainassociation.org