THE JBBA
THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®
britishblockchainassociation.org/jbba

VOLUME 3 | ISSUE 2 | ISSN PRINT: 2516-3949
NOVEMBER 2020

The British Blockchain Association®
Advocating Evidence Based Blockchain

INSTITUTIONAL CRYPTOECONOMICS

WHO IS THE "BLOCKCHAIN EMPLOYEE"?

Blockchain Skills in Demand

Self-Executing Contracts in Poland

DNA on the Blockchain

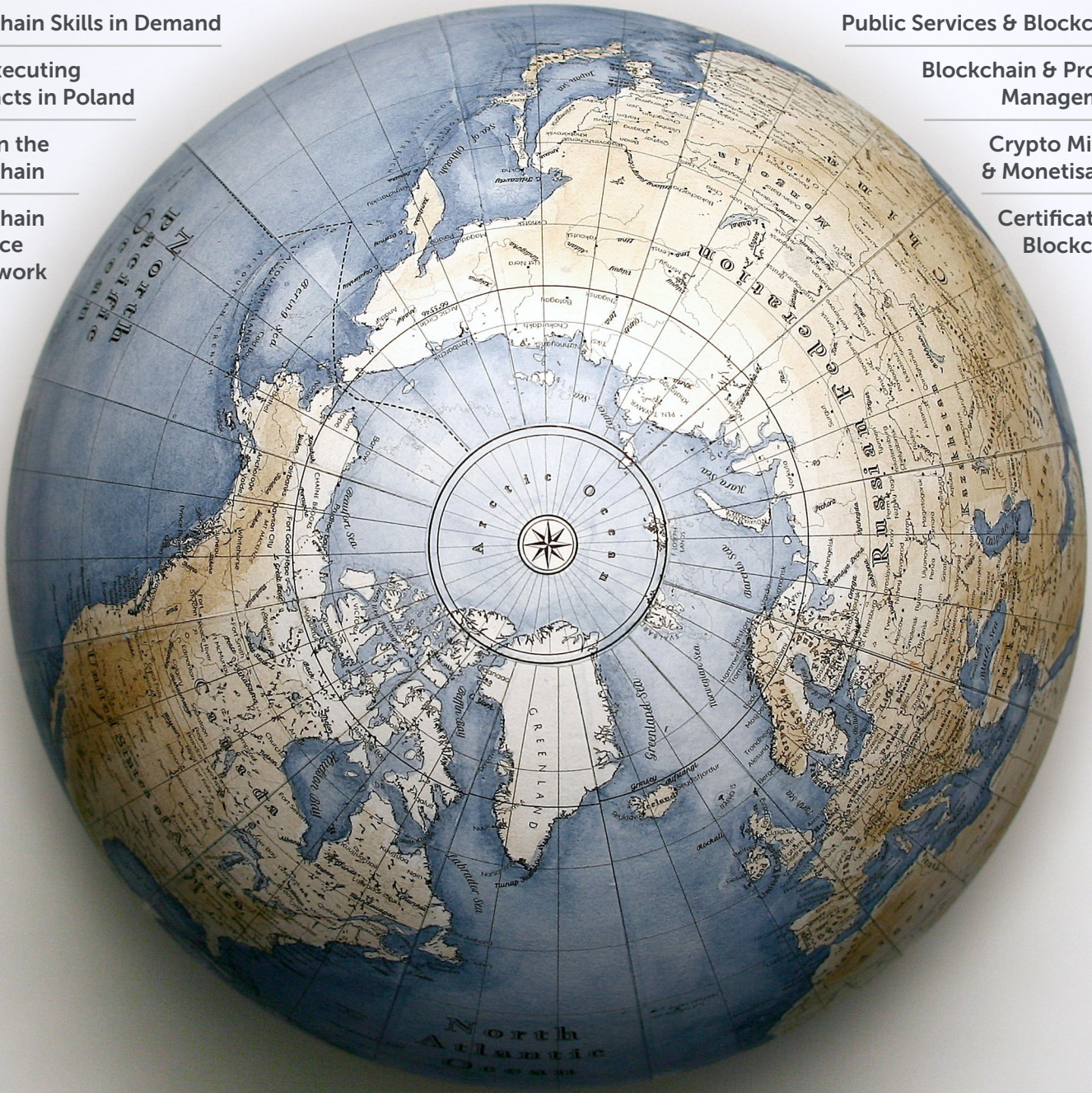
Blockchain Evidence Framework

Public Services & Blockchain

Blockchain & Project Management

Crypto Mining & Monetisation

Certificates & Blockchain



3rd Blockchain International Scientific Conference 15th March 2021 *ONLINE*

ACADEMIC PARTNERS

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

GCPSE Global Centre for Public Service Excellence

UNDP Empowered lives. Resilient nations.

CEBB Centre for Evidence-Based Blockchain®

ARTiFACTS® Researcher Recognition, Accelerated

BBC GLOBAL NEWS LTD

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 awaraness 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:

appg BLOCKCHAIN

Department for International Trade

British Embassy Lisbon

INATBA

GCPSE Global Centre for Public Service Excellence

UNDP

ENTERPRISE ETHEREUM ALLIANCE

Isle of Man Government

FEATURED MEMBERS AND PARTNERS

ARTiFACTS Researcher Recognition, Accelerated

patientory association

ARABIANCHAIN TECHNOLOGY

Baker McKenzie.

Blockchain 121

BitNaj

Aren Strategy

Join Now at britishblockchainassociation.org/membership

TABLE OF CONTENTS

PEER-REVIEWED RESEARCH

3RD BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE

ISC 2021 *ONLINE*

15TH MARCH 2021

WHY ATTEND ISC 2021?

Network Online with some of the Most Eminent Blockchain Scholars

Meeting point Conference of Blockchain Industry & Academia

International Recognition of your work by Blockchain Scientific Community

Prizes for Best Abstract Presentation

Connect with Enterprises & Institutions looking for Blockchain innovators

Publish your work in The JBBA

Pitch your ideas and research to Policy Makers and Enterpreneurs

CALL FOR PAPERS

Researchers, academicians, technologists, blockchain developers, policy makers and other stakeholders are welcome to submit their original research papers, pilot projects and case studies to ISC 2021

For more information visit

www.britishblockchainassociation.org

WHY JBBA?

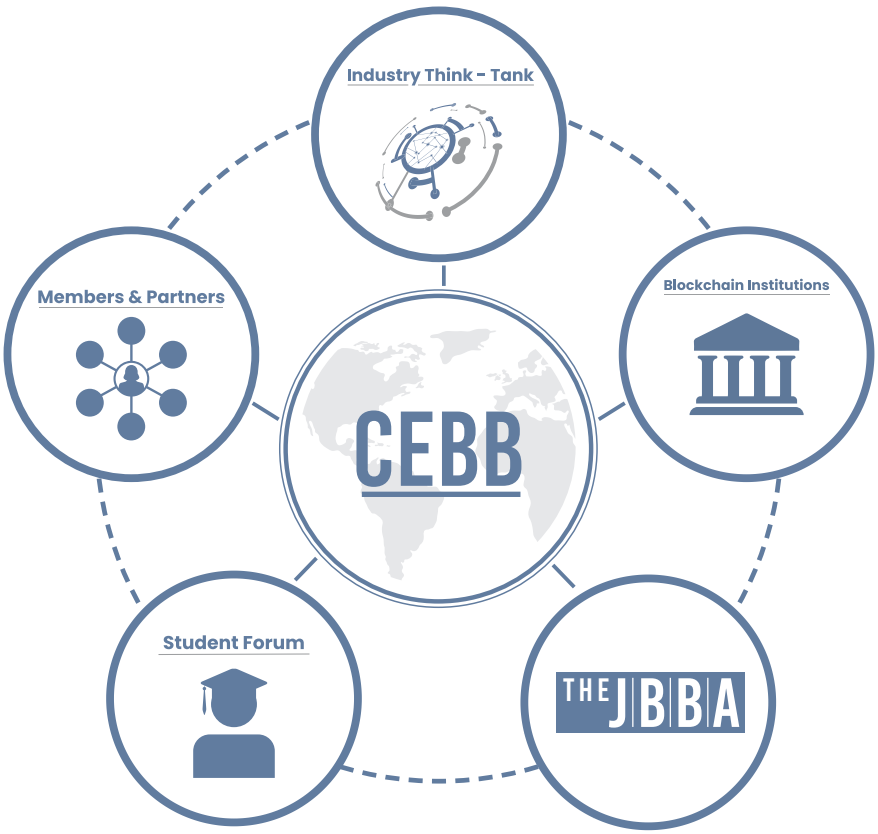
- We publish in real-time, online, as well as in **PRINT - THE HARD COPIES ARE DISTRIBUTED WORLDWIDE**
- Print copies are available at some of the largest libraries in the world including **BRITISH LIBRARY** and over 100+ more **AROUND THE GLOBE**
- Our authors and readers rate the JBBA as **OUTSTANDING**
- 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**

THE JBBA
THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

Follow us on:

CEBB | Centre for Evidence-Based Blockchain®

Bridging the Blockchain Research and Practice Gap



MEMBERS

The British Blockchain Association
Advocating Evidence Based Blockchain

RMIT Blockchain Innovation Hub

cryptecon
center for cryptoeconomics

Blockchain 121

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Edinburgh Napier UNIVERSITY

The Open University

Ulster University

UNIVERSITY OF ARKANSAS

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

CEBB | Centre for Evidence-Based Blockchain®

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!

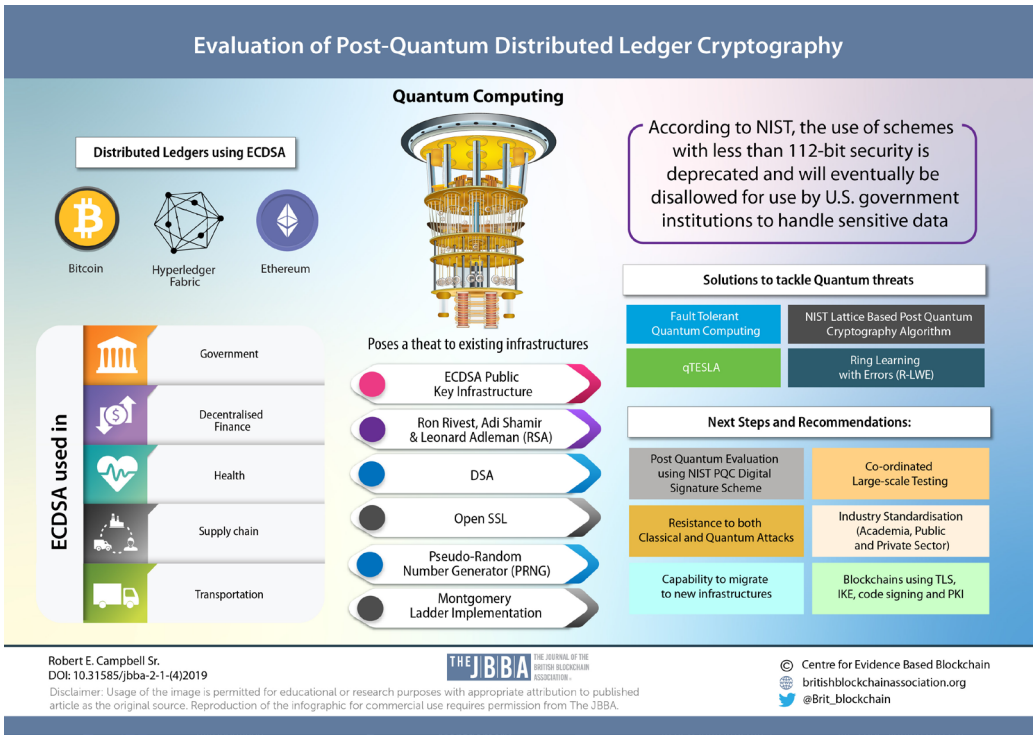
JBBA has become the World's First Blockchain Research Journal to create Video Abstracts for its Authors!

- 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

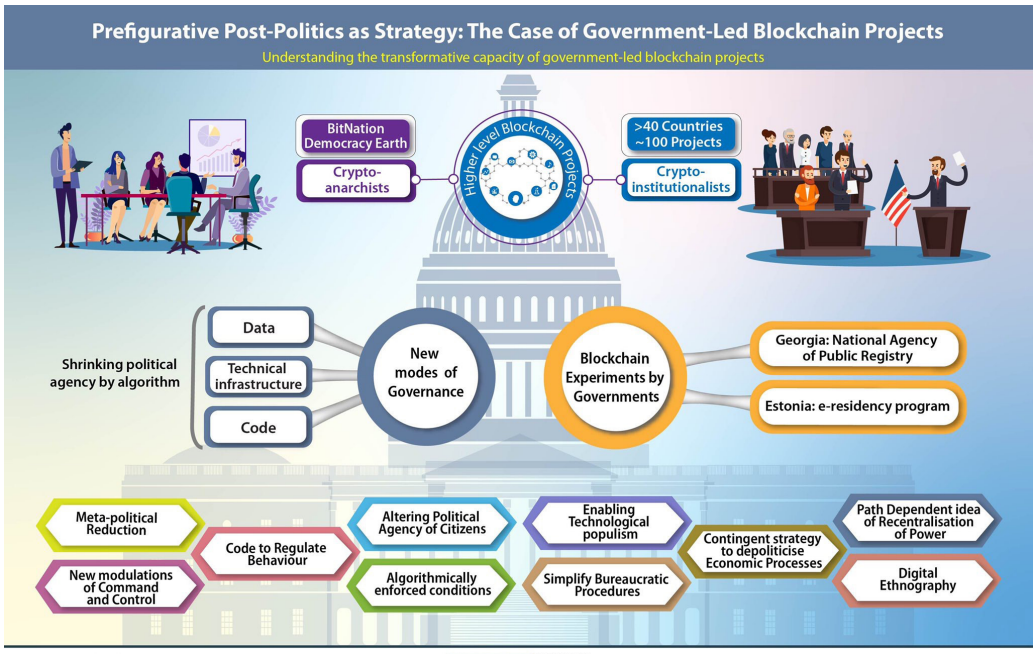
For more info, visit https://www.youtube.com/c/TheJBBA

JBBA INFOGRAPHICS

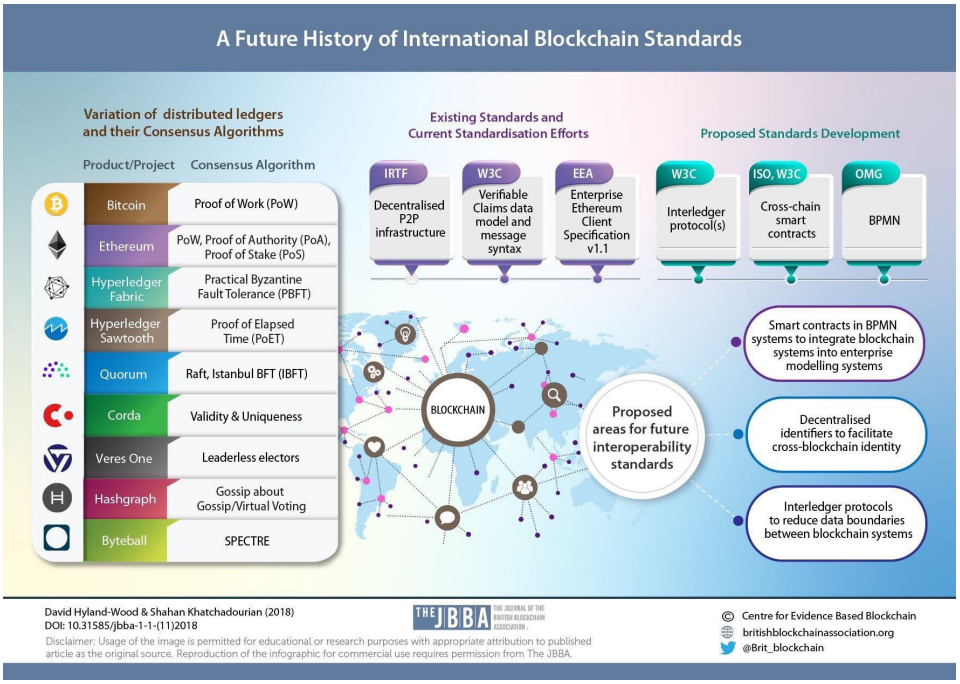
PRODUCED BY
CENTRE FOR EVIDENCE BASED BLOCKCHAIN (CEBB)



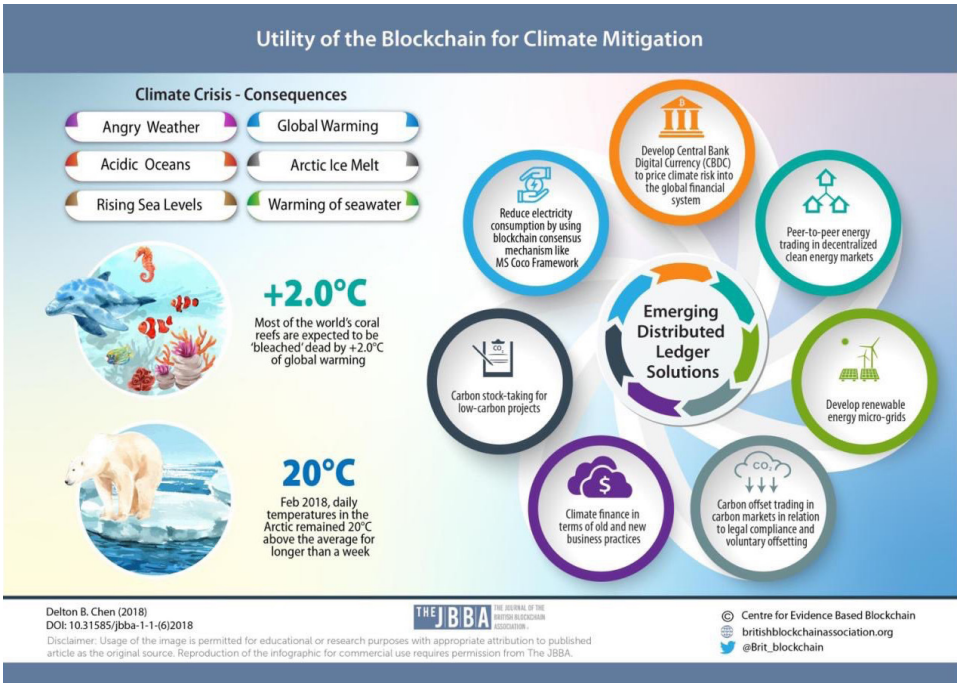
Robert E. Campbell Sr.
DOI: 10.31585/jbba-2-1-(4)2019



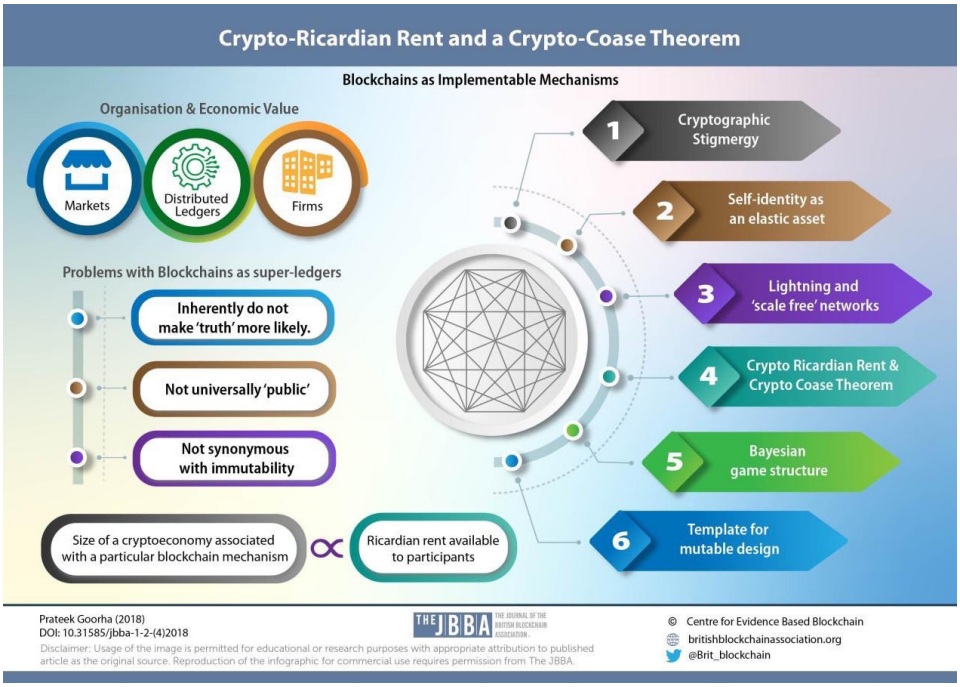
S Omer Hussain, et al. (2019)
DOI: 10.31585/jbba-3-1-(2)2020



David Hyland-Wood & Shahan Khatchadourian (2018)
DOI: 10.31585/jbba-1-1-(11)2018



Delton B. Chen (2018)
DOI: 10.31585/jbba-1-1-(6)2018



Prateek Goorha (2018)
DOI: 10.31585/jbba-1-2-(4)2018

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

EDITORIAL BOARD

EDITORIAL

It is with delight that I present this – the sixth – issue of the Journal of the British Blockchain Association. Now into its third volume, the Journal continues to publish important path-breaking research.

The contributions in this issue are truly international with authors coming from, at least, seven different countries across four continents. This highlights the valuable role the Journal has come to play in publishing leading world-class research into this new disruptive and revolutionary technology.

In such a fast moving field the Journal has quickly established a reputation as an outlet for timely, thoughtful, and important research that is of interest to both academics and practitioners. The Journal publishes impact-led and industry relevant research. Importantly, Journal articles are readable, and accessible for a broad audience. Blockchain scholarship is a multidisciplinary endeavour and that diversity is reflected in the broad range of papers that have been published over the past three years.

The papers included in this issue are:

- Who is the Blockchain Employee? Exploring Skills in Demand using Observations from the Australian Labour Market and Behavioural Institutional Cryptoeconomics
- Browser-based Crypto Mining and EU Data Protection and Privacy Law: A Critical Assessment and Possible Opportunities for the Monetisation of Web Services
- Are Blockchain-based Systems the Future of Project Management? A Preliminary exploration
- Academic Certification using Blockchain: Permissioned versus Permissionless Solutions
- Self-executing Contracts from the perspective of the selected Polish regulations and the future potential prevalence of 'Smarter' Contracts
- Blockchain - A Panacea For Trust Challenges In Public Services? A Socio-technical Perspective
- Privacy Laws, Genomic Data and Non-Fungible Tokens
- Evidence-Based Blockchain: Findings from a Global Study of Blockchain Projects and Start-up Companies

At first glance, it may appear that the papers cover a broad range of issues in the blockchain space. At the broadest level the papers all consider issues of scaling the blockchain. What are the use cases? What are the challenges? How will it actually work? Who will do the work? What qualifications will they need? What is it precisely that need be scaled?

Blockchain was first developed to provide a native internet money – yet the use cases for the technology go far beyond a payments system. It may be something of an overstatement; trust is the raison d'être of the blockchain. It is the industrialisation of trust that makes blockchain such a valuable and important institutional technology. The ability to deploy trust at scale will drive many use cases in future.

Some of those use cases are discussed in this issue of the Journal. Academic credentialing and project management are obvious use cases. But are these use cases being adopted? What impediments are there to adoption? Are managers using the technology? Does it add value? Then there are issues of interaction with outside world institutions. How do smart contracts interact with external legal systems? These are important practical questions that articles in this issue address. What of privacy concerns and data protection? Privacy by design will be embedded into all future digital business models. But how exactly can competing demands for privacy, legality and ethical behaviour be incorporated into best practice? And what of the infamous practice of browser mining? Is there a viable, legitimate place for it in the cryptoeconomy? Readers will find thoughtful arguments addressing these very questions.

The challenges facing any new technology or business process is hype. How can we know that any new technology or process is living up to its promise? It is not enough to ask tough questions, it is important to have a tough framework that informs those questions. Readers should find the paper on evidence based blockchain particularly valuable when evaluating blockchain use cases.

Then who will do all this work? Blockchain is destined to be the economic infrastructure underpinning the future digital economy. Who is going to build it? What skills will they need? Economising on the cost of trust is what makes the blockchain so valuable. Industrialising energy and power gave rise to the industrial revolution; Similarly, industrialising trust will drive the next revolution in economic activity. To better understand that process, and to allay fears that this is all hype, there is a huge need for careful and thoughtful analysis of existing use cases and industry needs. That type of analysis can be found in these pages.

My congratulations to all the authors of the papers in the issue. Thank you for your hard work and for thinking of the Journal as an outlet. Without your research and thought leadership, the blockchain space would be intellectually poorer. Then to the referees who provided insight and guidance to the authors – thank you for your voluntary contributions. Finally to the editors and production staff at the Journal itself – running a journal can often seem to be a frustrating and thankless task – so, thank you!

Sinclair Davidson PhD
Senior Editor, The JBBA
Professor of Institutional Economics, RMIT University

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 Goorha 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 Renwick PhD , University college Cork, Ireland*

> The JBBA is an exciting peer-reviewed journal of a growing, global, scientific community around Blockchain and Distributed Ledger technologies. As an author, publishing in the JBBA was an honour and I hope to continue contributing to in in the future
>
> *Evandro Pioli Moro, Blockchain Researcher, British Telecommunication (BT) Applied Research*

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(4)2020

Who is the Blockchain Employee? Exploring Skills in Demand using Observations from the Australian Labour Market and Behavioural Institutional Cryptoeconomics

[1]Jessica Atherton, [2]Alexandra Bratanova, [3]Brendan Markey-Towler
[1,2]Commonwealth Scientific and Industrial Research Organisation's Data61, Australia
[3]Independent researcher, Australia
Correspondence: jessica.atherton@data61.csiro.au
Received: 26 March 2020 **Accepted:** 13 May 2020 **Published:** 19 June 2020

Abstract

LinkedIn recently predicted that blockchain skills will be the most in-demand skill in 2020, and in 2018 blockchain led the list of the fastest growing skills in demand according to Upwork. But what exactly constitutes the skill set of a blockchain employee? We use Australian labour market data to explore what skills are in demand among the blockchain workforce. We also take a deeper dive and explore what educational qualifications and experiences are required of blockchain employees, and how blockchain-related jobs perform on salary scales. We discover that alongside 'hard' software engineering skills such as programming languages or computer science, blockchain-related jobs require candidates to have 'soft' skills such as creativity, communication and leadership. To explain this, we use institutional cryptoeconomics, applied game theory and applied behavioural science to suggest that the demand for skills may be understood as a function of challenges to blockchain adoption. We suggest that for blockchain to enter a mass adoption phase, the industry will need employees with an integrated skill set of both hard software engineering skills and soft behavioural or enterprise skills. Furthermore, blockchain leaders, community leaders and end users will need to gain 'blockchain literacy' to overcome the challenge of coordinating expectations by developers and users, who will create network externalities and facilitate rapid, coordinated adoption. We contribute to the evidence-based blockchain literature by using Australian labour market data to derive insight into the challenges posed to the adoption of blockchain as (and if) it climbs out of the current 'trough of disillusionment'.

Keywords: *blockchain; skill set; technology adoption; labour market; cryptoeconomics*

JEL Classifications: *O10, O40, J01, H30, A1*

1. Introduction

Blockchain[1] can potentially transform the Australian and global economy by offering greater data transparency, improved traceability, enhanced security and reduced costs across a variety of industries [2-4]. Blockchain allows users to transfer value efficiently in the absence of trusted intermediaries, and it has the potential to form a basis for an 'Internet of Value' by overcoming issues of trust in an online environment [5]. It has the potential to serve as a new type of inter-institutional infrastructure transforming the roles of traditional institutions including governments, firms, clubs, commons and indeed markets themselves [6]. Whether these changes can be realised is a question predicated on the level of adoption of blockchain as a technology for economic interaction [7].

This article investigates which skills are in demand for blockchain employees as the technology progresses beyond the initial hype that typically follows the introduction of a new technology, through the notorious 'trough of disillusionment' and finally into a 'plateau of productivity'—where most of the substantial economic gains can be produced [8]. To do this, we explore two data sets from the Australian labour market in 2015–2019. We then seek a theoretical explanation for our observations. This approach can be seen as phenomenological [9], and we indeed want the readers to experience and explore the data and hence observe phenomena before we position the theory to explain them. We provide the theoretical explanation by drawing on institutional cryptoeconomics, applied game theory and applied behavioural science to explain our observations as a function of the challenges to blockchain adoption. We also discuss the future challenges that Australia might face in meeting the fast-growing demand for blockchain employees seeking to solve the broader problem of securing blockchain adoption.

We first consider the emergence of blockchain jobs globally and in Australia in line with the 'hype cycle'. We then explore data sets on blockchain-related job ads and required skills. Next, we explain our observations drawing on the perspective of behavioural institutional cryptoeconomics. Finally, we discuss the broader significance of our results.

2. Blockchain hype and skills demand: a historical review

There is no industry in the world today that has not investigated the opportunities of blockchain. In just a decade the technology has facilitated the creation of new products and services in Australia and internationally. Between 2014 and 2018, worldwide venture capital funding of blockchain grew by a factor of 11 to US$5.6 billion [10]. Australia is one of the nations at the forefront of blockchain innovation with world-leading public and private sector projects such as the Australian Securities Exchange's CHESS replacement [11], Commonwealth Bank's Bond-i [12], IP Australia's IP Rights Exchange and Smart Trade Mark [13, 14] and Power Ledger's energy trading platform [15]. Australia also leads the secretariat to the technical committee developing international blockchain standards [16, 17].

Along with the emergence of blockchain technology, the demand for blockchain-related skills has been growing. The Bitcoin hype of 2017 sparked a boom in demand for blockchain-related skills, resulting in a competitive global hunt for blockchain employees [18]. For two quarters in a row (Q1–2 2018) blockchain led the list of the fastest growing skills

in demand on the freelancing platform Upwork [19]. Blockchain first drew attention on the Upwork skills index in Q3 2017 as the second fastest growing skill followed by Bitcoin as the third. In Q4 2017, Bitcoin took the lead as the top skill [19] before losing its place to blockchain for Q1 and Q2 of 2018. Since then both Bitcoin and blockchain have slipped off the Upwork skills index list.

Similarly, job analytics firm Burning Glass Technologies (BGT) revealed a steady increase in the number of blockchain job postings between 2010 and 2014 in the United States of America (USA). The figure thereafter drastically increased, from 500 jobs in 2014 to almost 1,500 in 2015, before later spiking to 3,958 in 2017 [20].

In line with global trends, labour demand in Australia also experienced fast growth in blockchain-related jobs since 2014/2015 (see Figure 1). The number of job ads in 2015/2016 was 19 and grew almost by 215% in 2017/2018 to 408. The Australian market, being smaller and less developed than that of the USA, saw explosive growth two years later than the USA did and the number of blockchain job ads in the USA was almost 10 times higher than those in Australia (see Figure 1).

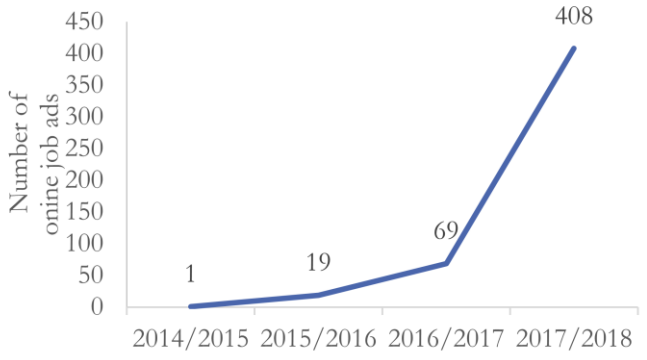


Figure 1. *Blockchain-related online jobs ads in Australia, 2014/15–2017/18.*
Source: BGT [20]

The end of 2017 marked the peak of global hype and inflated expectations for blockchain technology. The following year saw a deepening disillusionment heading into the infamous 'cryptowinter' (see Figure 2). In this period, blockchain began to be thought of as the most over-hyped technology since the beginning of the century. Voices questioning the applicability of blockchain, its maturity and effectiveness became increasingly prominent among business and government experts [21]. Media messages moved from 'blockchain can solve any problem' and 'all industries have use cases for blockchain' [22, 23] in 2017 to more sober accounts of non-blockchain use cases [21, 24] with an occasional smattering of 'there are no good uses for blockchain' [25]. Additionally, a global survey of public and private sector leaders showed that early investments in blockchain did not realise their anticipated returns [26]. On average, the respondents expected a 24% return but only realised 10%.

In Australia, crypto hype grew from 2015 until it peaked in 2018, as reflected in our observation of job ads posted monthly on the Adzuna Australia labour market platform (see Figure 3). Since then the demand for blockchain employees in Australia has decreased but remains relatively high. Globally, in January 2020 LinkedIn predicted blockchain will be the most in-demand hard skill in 2020 on the platform [28]. This may signal a recovery of blockchain-related project investment and that the sector in general might be plateauing in the trough of disillusionment, and potentially recovering from it.

This is interesting in and of itself. But job openings contain more information that allows us to ask the still more interesting question: what does it mean to be a blockchain employee? We will now use the Australian labour market data to consider which skills are required for blockchain employees. We will explore blockchain-related job ads in two data sets on the Australian labour market (BGT's Labor Insight™ data set [7] and the Data61 Australian Skills Dashboard [27]). This article extends on previous research by Data61 [7].

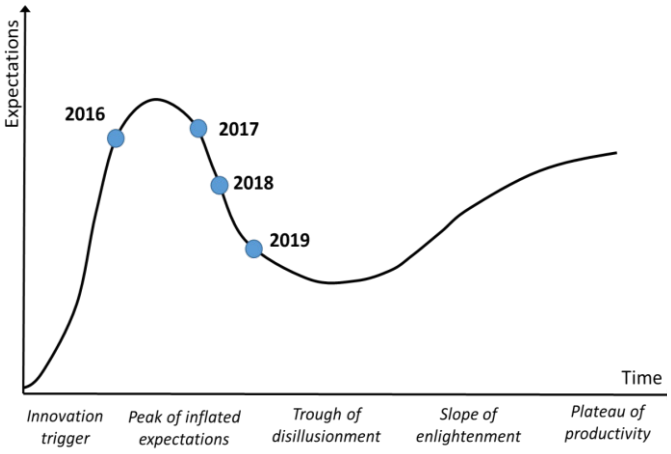


Figure 2. Approximate positions for blockchain technology along the Gartner Hype Cycle for emerging technologies, 2016–2019.

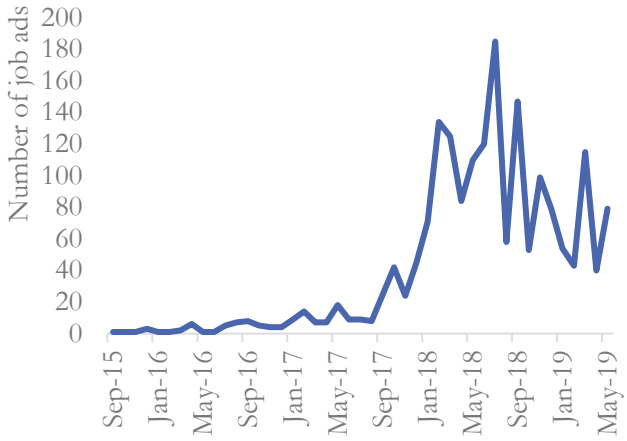


Figure 3. Blockchain-related online jobs ads in Australia by month, 2015–2019.
Source: Data61 Australian Skills Dashboard [27]

3. Data exploration

Burning Glass Technologies data set

One data set was sourced from job analytics firm BGT [29]. BGT data have been used by government and private organisations in Australia and internationally to investigate skills transformation [30], job transitions [31, 32], supply and demand [33, 34], education and credentials [35] among other topics. BGT's Labor Insight™ data set includes job vacancy data from company websites, online job boards and other online resources

available for web crawling. As of August 2018, BGT covered over 44,000 web page sources across Australia, New Zealand, the United Kingdom, USA, Singapore and Canada. Once the data are collected, BGT applies natural language processing to remove duplicate job ads and classify job skills. BGT acknowledges their data may include duplicate or miscoded job ads. See [36] for a detailed method and skills taxonomy.
We filtered the Labor Insight™ data by searching for ads that included 'blockchain' as a keyword. The final data set included 497 job ads posted between July 2014 and June 2018.

Data61 Australian Skills Dashboard data set

The Data61 Australian Skills Dashboard data set provides a snapshot of the labour market [27]. This dashboard analyses job ad data provided by the labour market platform Adzuna Australia. The data set includes job ads listed directly on the Adzuna Australia platform, ads listed in Australia's major newspapers and ads 'scraped' from other available online resources. Scraped ads must pass a screening process before entering the Adzuna platform, to minimise the number of expired, duplicate or incomplete job ads. The Data61 Australian Skills Dashboard data set is further cleansed through natural language processing and human coding to remove any remaining job ads that are duplicate or are from unreliable sources [37, 38]. Skills required by job ads are categorised using the European Skills, Competences, Qualifications and Occupations skills taxonomy. The dashboard represents the Australian labour market in terms of occupational categories and geographic locations at the state and capital city level [38]. However, job ads in the state of Western Australia as well as 'blue collar' jobs may be underrepresented [38].

For the purposes of this article, the Adzuna data set was filtered with 'blockchain' as a keyword. The search returned 1,863 job ads posted between September 2015 and May 2019. We also qualitatively classified the job ad skills into 'soft' skills and 'hard' skills to determine the demanded skills mix in advertised positions.

Observations from the Australian labour market for blockchain employees

Skills demand

Examination of the Data61 Australian Skills Dashboard data set demonstrates that employers are looking for a combination of soft and hard skills in the blockchain workforce. The hard skills frequently mentioned in the blockchain-related job ads include computer technologies and more specifically knowledge of JavaScript and Internet of Things. Around half of the skills most frequently mentioned in the job ads, alongside blockchain, are soft skills including creative thinking, customer service, communication, as well as project management and leadership (see Figure 4). Moreover, 84.3% of the job ads required a mix of both soft and hard skills (see Figure 5).

For a more detailed exploration of the required hard and soft skills, we looked at BGT job ads posted in 2017–2018. The data reveal the top technical skills desired from prospective blockchain employees (see Figure 6). The listed skills require a background in programming and/or mathematics.

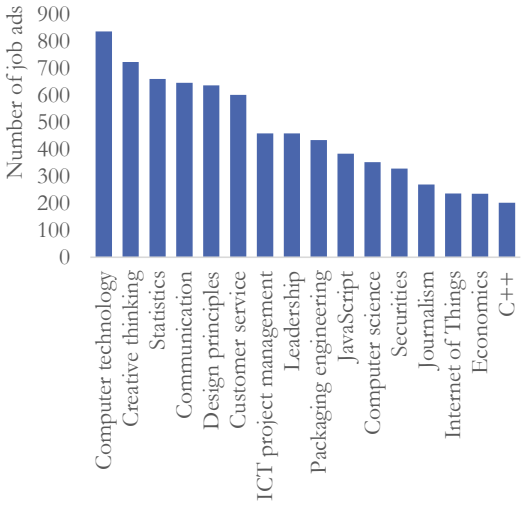


Figure 4. Top skills mentioned in Australian blockchain-related job ads between September 2015 and May 2019.
Source: Data61 Australian Skills Dashboard [27]

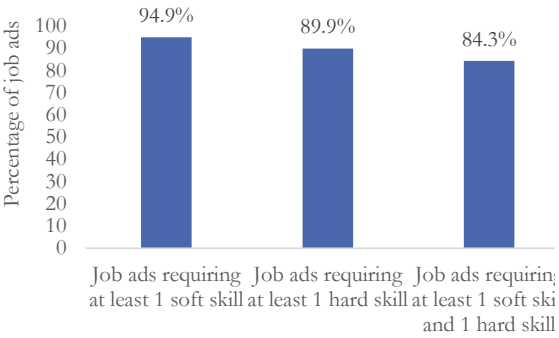


Figure 5. Soft and hard skills mix of Australian blockchain-related job ads between September 2015 and May 2019.
Source: Data61 Australian Skills Dashboard [27]
Note: 1.4% of the total job ads listed no skills and were excluded from this graph.

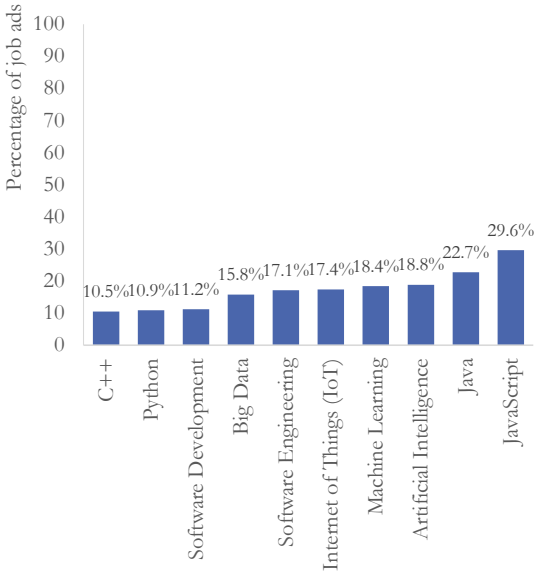


Figure 6. Top hard skills required in Australian blockchain-related job ads between August 2017 and August 2018.
Source: BGT data [7]

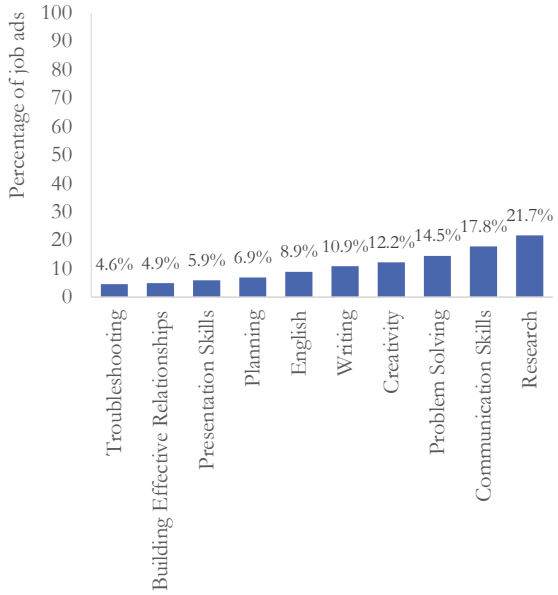


Figure 7. Top soft skills required in Australian blockchain-related job ads between August 2017 and August 2018.
Source: BGT data [7]

The BGT data also show that there is demand for soft skills among blockchain employees (see Figure 7).

Required educational qualifications

The observed demand for skills was reflected in the desired level of educational qualifications for blockchain employees (see Figure 8). Over 9 in 10 blockchain jobs required either a bachelor's degree or an even higher level of education according to the BGT data.

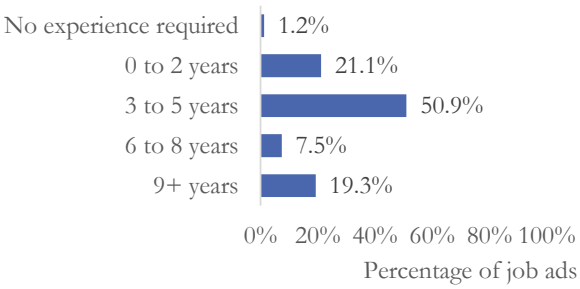


Figure 8. Level of experience required in Australian blockchain-related job ads between August 2017 and August 2018.
Source: BGT data [7] Note: 68% of records have been excluded because they did not mention required experience. Therefore, this chart may not be representative of the full sample.

In the BGT data set, 107 blockchain-related job postings referenced a preferred field of study. The top majors that blockchain job ads required are listed in Figure 9.

Experience required

In the BGT data, 161 job ads mentioned required experience (see Figure 10), with over half of the jobs requiring between three to five years of experience.

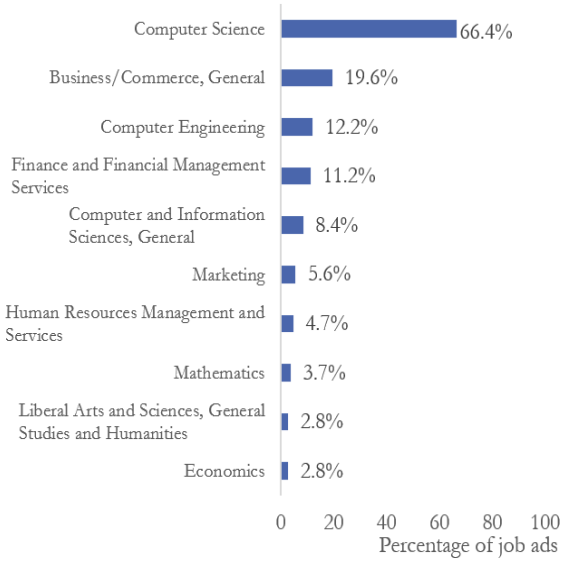


Figure 9. Top degrees required in Australian blockchain-related job ads between August 2017 and August 2018. Source: BGT data [7]
Note: 77% of records have been excluded because they did not include a major. Therefore, this chart may not be representative of the full sample.

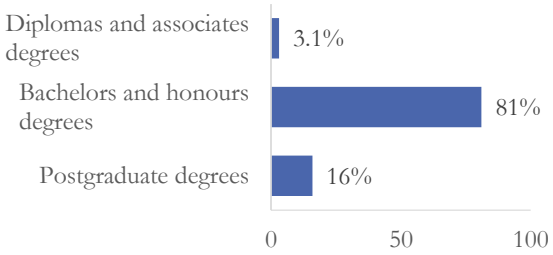


Figure 10. Qualifications required in Australian blockchain-related job ads between August 2017 and August 2018.
Source: BGT data [7]

Salary distribution of jobs

Almost 60% of the jobs offered to pay blockchain employees above AU$100,000 per year (see Figure 11). This is a higher wage level than most Professional job offers. Only around 45% of Professional jobs offered the same salary bracket. However, the data showed no difference in wage level between blockchain employees and Data Scientists and Software Engineers who have a relatively similar skill set to blockchain developers.

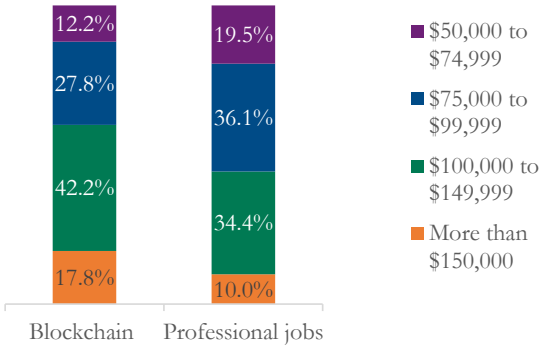


Figure 11. Salary distribution of jobs in blockchain and other Professional jobs between August 2017 and August 2018 (in Australian dollars).
Source: BGT data [7]
Note: Professional jobs are defined as the jobs requiring at least a bachelor degree.

The picture of the in-demand blockchain workforce is therefore a somewhat interesting one for a technology-heavy sector building something akin to a digital utility. The typical blockchain employee at least in Australia is one who integrates hard technical skills and soft personal and enterprise skills. They are highly educated, typically with a formal higher degree in-hand.

4. Explaining skills demand as a function of blockchain adoption challenges: behavioural institutional cryptoeconomics

We can understand the observed skills demand for blockchain-related jobs in Australia as a response to the challenge of securing blockchain adoption. Blockchain is a different technology to traditional technologies studied by economic theory as it is an institutional technology [6, 39]. Industrial, inter-firm productivity-enhancing technologies have tended to evolve at a relatively rapid rate compared to institutional technologies such as firms, markets, clubs, commons and governments that take decades and centuries to develop. However, blockchain as an institutional technology will be characterised by rapid, coordinated adoption.

To understand challenges being posed to blockchain adoption, we apply some game theory and behavioural science to round out the insights of institutional cryptoeconomics. We call this mix 'behavioural institutional cryptoeconomics'. It shows us that the key challenge to blockchain adoption is building capacity for adoption and then coordinating expectations across that population to facilitate rapid, coordinated adoption. It is the solution to this challenge—a similar challenge to that faced by Facebook, Uber, Airbnb, Amazon, PayPal and YouTube in their early years—that reveals to us what the Australian labour market for blockchain employees may be responding to.

Institutional cryptoeconomics: platforms and network externalities

Institutional cryptoeconomics identifies that the defining characteristic of blockchain is not that it is a distributed ledger technology (DLT)[2] per se, but rather that it is an institutional technology [6, 39]. It introduces a sixth archetype to the traditional five: markets, firms, governments, commons and clubs [40-43]. Such technologies require different kinds of governance, delimiting and enforcing the bounds of acceptable behaviour in society. The contention of institutional cryptoeconomics is that blockchain presents a sixth institutional technology because it is differentiated by the nature of its emergence and operation [6, 44]. Blockchain protocols (such as Bitcoin, Ethereum and Monero) delimit a range of interactions on internet platforms that can be considered legitimate and integrated by a consensus algorithm into a record held by a network. The writing and actioning of blockchain protocols to support institutional governance of internet platforms, therefore almost by definition, emerges from a decentralised network and is actioned by that network. It does not require legitimation by government or some other centralised enforcement authority. It can be entirely supported by private entities. Blockchain is thus an institutional technology that allows for privatised emergent governance of internet-based platforms.

The defining problem in blockchain adoption, that makes it different from industrial technology adoption, is that, as a technology that enables institutional governance of internet platforms, it must, as with any platform technology, harness network externalities to achieve rapid, coordinated adoption [45-47]. This is not necessarily the case with industrial technologies [48-52]. But because platform technologies exist to enable and support interactions that would not otherwise be possible, they derive their value from the interactions that are possible within them. Therefore, the value of adopting a platform for interacting with others by any one individual or organisation is contingent upon its adoption by other individuals and organisations they might like to interact with. In economic theory we call this a network externality [53-56]—the collective adoption of a particular technology affects the value an individual could realise from it.

Applied game theory, network externalities and Schelling-point coordination

Applied game theory allows us to identify why blockchain adoption needs to be rapid and coordinated. Achieving adoption of a platform governed by institutional technology is a special case of Schelling-point coordination [57]. Originally, Schelling-point coordination illustrated why the problem of disarmament is difficult to solve, because unilateral disarmament could be disastrous, and so all nuclear powers must simultaneously disarm (and maintain their disarmament). To obtain such an equilibrium, the various nuclear powers must therefore believe that all other nuclear powers will disarm simultaneously with them. Thus Schelling-point coordination becomes a problem of coordinating expectations between various nuclear powers to ensure simultaneous disarmament.

A similar problem is created by network externalities in the context of platform technology adoption and therefore the adoption of blockchains. The value of adopting a given internet-based platform for interaction subject to blockchain-based institutional governance is completely contingent on its adoption by others. Obtaining an equilibrium where a given platform and its blockchain are adopted therefore requires that there be a belief across the population that the population at large will adopt it. Hence, the adoption of blockchain as an institutional technology for platform governance depends on the coordination of *expectations* across the population of potential users that sufficiently many *others* in the population will adopt the platform and its blockchain. Lest those expectations be 'dashed' and the adoption 'fizzle', that coordination of expectations must support rapid, coordinated adoption of the internet-based platform for interaction subject to blockchain-based institutional governance under consideration.

Applied behavioural science and restraining forces in blockchain adoption

The problem of coordinating expectations is fundamentally predicated on human behaviour in a systemic context. Blockchain will not be adopted unless there is rapid, coordinated adoption at the systemic level.

Arguably the simplest formulation of psychological theory that is directly applicable to understanding the solution to this problem is that provided by Kurt Lewin [58]. Lewin sees behaviour as an equilibrium between driving and restraining forces that emerge from the interaction between motivation [59], cognition [60] and environment [61]. The challenge, Lewin suggests, when we approach problems of behaviour change, such as securing adoption of blockchain, is not to increase the driving forces towards that behaviour. The challenge is to reduce the restraining forces emerging from the interaction between motivation, cognition and environment that urge the individual away from that behaviour.

For restraining forces in blockchain adoption, there are two broad categories. For an individual or an organisation to adopt a platform subject to blockchain governance, they must be (1) able to adopt the platform as a system for interaction with others and (2) be willing to adopt the platform (see Figure 12).

In terms of the ability to adopt a platform subject to blockchain governance, the first restraining force is the actual creation and functionality of the code itself.

Building the initial system can be difficult since it often requires collaboration from various users across networks, business units, jurisdictions and systems. The networked nature of blockchain also means that it will, typically, exist within a 'winner takes all' system—with dominance in systems and protocols often being gained by those able to grow rapidly in the initial phases and obtain first mover advantage [62]. The 'winner takes all' dynamic makes the collaboration delicate and challenging. As such,

gaining collaboration to build the initial system often requires strong skills in strategic management. Delivering requires good communication to the technical team, so the system meets the requirements of the collaborators.

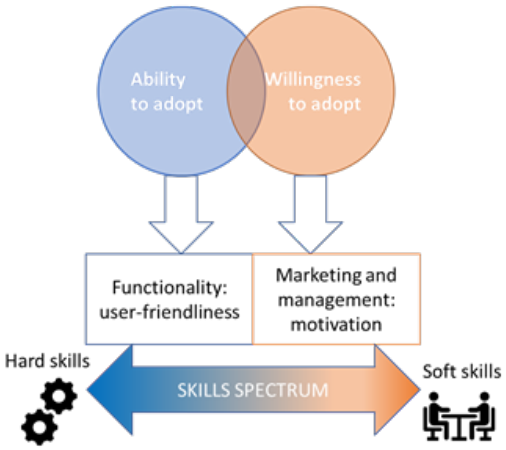


Figure 12. Overcoming restraining forces in blockchain adoption

In terms of the ability to adopt a platform subject to blockchain governance, the first restraining force is the actual creation and functionality of the code itself.

Building the initial system can be difficult since it often requires collaboration from various users across networks, business units, jurisdictions and systems. The networked nature of blockchain also means that it will, typically, exist within a 'winner takes all' system—with dominance in systems and protocols often being gained by those able to grow rapidly in the initial phases and obtain first mover advantage [62]. The 'winner takes all' dynamic makes the collaboration delicate and challenging. As such, gaining collaboration to build the initial system often requires strong skills in strategic management. Delivering requires good communication to the technical team, so the system meets the requirements of the collaborators.

In the event they can achieve this, the technical team is likely to successfully build a system with basic functionality. But when human beings are involved, cognitively limited organisms, usability goes to a far deeper level than engineering alone. To maximise the likelihood of a blockchain platform's adoption, the platform itself must be designed to be user friendly enough so that any technical functioning of the platform is essentially invisible to the user experience. The more complex the platform is in terms of user experience, the greater the restraining forces against adoption, because the requisite cognitive capabilities to use the platform cannot be developed. World-class user experience design is necessary for developing capacity for blockchain adoption among a population of potential adopters.
Continuing this, one step removed again from engineering concerns, the usability of a platform subject to blockchain governance depends on the complexity of the institutional arrangements to which it is subject. The more complex the institutional arrangements that govern the platform both internally ('on-chain') and externally ('off-chain'), especially due to external regulatory structures and again uncertain regulatory structures, the greater the restraining forces against adoption. Cognitive capabilities are necessary not only for the simple ability to use the platform on a functional level, but also for the ability to use it within the bounds of acceptability delimited by institutional governance. How many laws does one break simply because they are too complex for one unindoctrinated in the law to understand? Good institutional design and negotiation with external parties is needed to ensure the blockchain governance structure is usable enough for all potential adopters.

Now as to the *willingness* to adopt a platform subject to blockchain governance, this depends on the extent to which the cognitive dissonance [63] created by ideas about breaking with traditional platforms for interaction and embracing platforms subject to blockchain governance can be overcome. This cognitive dissonance presents a significant restraining force urging against adoption of blockchain technology, as it does with any new technology. But in the case of blockchain-based institutional technologies, the existence of network externalities and the pre-existence of established platforms (such as Amazon, Uber and YouTube) is particularly acute.

This restraining force is something that must be overcome by world-class strategic management and marketing of the design of a platform subject to blockchain governance. This strategic management and marketing must integrate design across all aspects of the platform from the functionality of the code itself to the user interface laid over it, and also integrate this design with strategic marketing that builds sufficient expectations (that will be validated) about the value of adopting the platform and its governance structure. Critically for the validation of these expectations, the strategic management and marketing of the design must be oriented to facilitating rapid, coordinated adoption *en masse*.

Unless this strategic management and marketing of design is strong, it will fail to build and/or validate expectations that reduce the restraining force of cognitive dissonance about the value of adopting a new blockchain-based platform. If that is the case, we will fail to see harnessing of network externalities to leverage rapid, coordinated adoption of the platform subject to blockchain governance, and thus we will fail to see adoption at all. Hence astute strategic thinking in management and marketing of the platform and blockchain design is critical for blockchain adoption.

Behavioural institutional cryptoeconomics: labour market demand for skills as a function of the adoption problem

We are now in a position to understand what we might be observing in the Australian labour market data as reflecting the market's response to this problem. We saw that as a technology for institutional governance of internet-based platforms, the adoption of blockchain technology is subject to network externalities that must be harnessed and overcome by Schelling-point coordination. We saw how the achievement of this Schelling-point coordination required the overcoming of restraining forces against the adoption of blockchain technology by world-class user experience design, institutional design and astute strategic thinking in the management, marketing and design of platforms subject to blockchain-based governance.

To reduce restraining forces in blockchain adoption, it is therefore necessary to *integrate* software engineering with insights from user experience, negotiation, lawmaking, political theory, strategy, management, marketing and design. While different employees in a development team may differ in their skills and strengths, it will be necessary for *at least one* to have an integrated skill set across all of them to facilitate their integration across the whole team. At least one employee, in other words, will need to 'speak the language' of hard and soft skills to facilitate their integration, and this will necessarily require them to have some proficiency in both. Only if this integration of soft skills and hard skills occurs will we observe the development of capacity and the coordination of expectations necessary to support rapid, coordinated adoption of blockchain as an institutional technology for internet-based platforms.

5. Discussion

Our exploration of Australian labour market data would appear to provide hope for blockchain enthusiasts if the observations are a function of the market responding to the core problem in blockchain adoption. If we were going to observe the adoption of blockchain as an institutional technology for internet platform governance, we ought to be observing the emergence of demand for employees who are skilled in communication strategy,

management, marketing and user experience as well as those who are skilled in software engineering. Indeed, we ought to be observing a demand for employees who can integrate soft skills with hard skills. Our observations from the Australian job ad data provide some evidence that this may be occurring, revealing a demand for hard skills, soft skills and integrated skill sets from blockchain employees.

These results accord with the general findings of empirical studies in labour economics as they track the emergence of the digital economy. As digital technologies advance and more jobs are expected to be replaced or disrupted by automation, we are observing growing demand for technical skills and programming universally across the economy. However, the demand for soft skills is also growing, and in many cases outstripping the demand for technical skills [64]. Based on the data insights and theoretical frame of behavioural institutional cryptoeconomics, we suggest we are observing at least in Australia a labour market response to the challenge of securing blockchain adoption. This might suggest that the technology is poised to emerge from the trough of disillusionment as a new generation of blockchain employees enter the sector. These employees may develop a stronger integration between software design through the application of hard technical skills, and securing the platform's adoption through the application of soft skills. This may promote rapid, coordinated adoption of blockchain by the overcoming of restraining forces contributed to by network externalities and usability, and cause the technology to become more integrated into the technological base of the economy at its core, rather than as a peripheral technology.

as develop a population that can co-develop and use it.

Blockchain developers and adopters will play an essential role in further development and implementation of the new technology across the economy and will rely on blockchain knowledge and industry expertise, contributing to the building capability for adoption. Blockchain leaders, community leaders and end users would benefit from 'blockchain literacy' or a broader understanding of how the technology works. While the usability of the system should make its technical functioning invisible, the end users will need to understand blockchain's value proposition and key differences to existing systems to build expectations of coordinated adoption. Complementary soft skills will be crucial for adopting companies and industries to fit the new approaches with existing legacy systems and to ensure the technology fit for jobs, teams and industry-specific requirements.

One pressing issue for the development and uptake of blockchain technology is the supply of a qualified workforce to meet the growing demand for blockchain development. Australia might produce fewer potential blockchain employees than other countries as Australia has fewer Information and Computer Technology (ICT) graduates than countries such as Singapore, Finland and New Zealand. In these countries, more than 6% of all students graduate with ICT qualifications compared to only 3.5% in Australia [65]. The continuing expansion of blockchain outside the ICT industry, we suggest, will open large markets for educational providers in Australia and internationally. The growing demand for quality blockchain education therefore forms a market niche for accredited

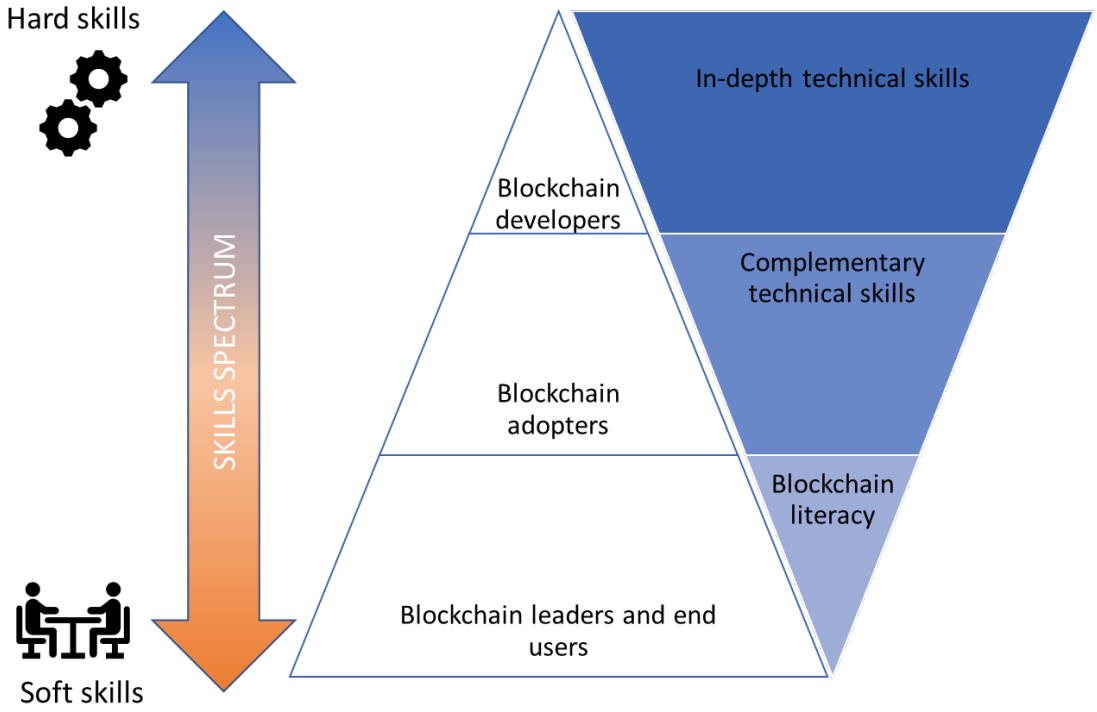


Figure 13. Hierarchy of blockchain technical skills for blockchain developers, adopters and users.

Our data insights and theoretical frame also suggests that blockchain adoption may require blockchain employees who can help build the combination of technology and complementary skills required for different groups from blockchain users to blockchain developers. A simple model of this integrated skills hierarchy that we suggest needs to be built and perhaps is being built as presented in Figure 13. Blockchain leaders will need to understand the opportunities and limitations of the technology to strategically develop, market and manage blockchains as a software as well

Australian educational providers.

Limitations and further research directions

This article explicitly focuses on blockchain as the most popular DLT. There are two reasons for this narrow focus: (1) compared to blockchain, DLT as a term (and key word) is rarely present in the online job ad data that we used, and (2) DLTs are not tracked by the Gartner Hype Cycle.

Although we suspect that our theoretical frame can be applied more broadly to DLTs, our article has not specifically investigated DLTs.
Given that blockchain technology is new and it is still early in the hype cycle, there is a lack of high-quality data to deeply understand the challenges to blockchain development and adoption. This makes it difficult to perform much more than the descriptive analyses conducted in this study.
Another limitation of the current study lays in the nature of job ad data and skills classifications. Job ads represent what skills employers demand from employees, but does not necessarily reflect the skills of those who are interviewed or hired, neither do they directly reflect the roles, tasks and responsibilities of those hired.

Lastly, in our approach, we used theories to explain what we observed in the data. The next logical step would be to validate our explanations should additional or more detailed data become available. Future research could therefore target collection of higher-quality and larger data sets and conduct inferential statistical analysis. It would also be interesting to perform a comparative analysis across international blockchain job ad data sets, especially for regions with larger labour markets such as the USA.

Another direction for future research would be a study of labour market dynamics as well as constitution and transformations of skill sets for blockchain (and broader DLTs) in comparison with other emerging technologies such as artificial intelligence or quantum computing.

6. Conclusion

This article contributed to the evidence-based blockchain literature by examining the in-demand blockchain workforce as (and if) the technology moves through the trough of disillusionment into a plateau of productivity. The exploration of Australian labour market data showed that the in-demand blockchain workforce is well compensated, experienced and highly educated, with a mix of hard software engineering skills as well as soft enterprise and personal skills. To explain the skills demand, we used behavioural institutional cryptoeconomics which theorises that coordinating expectations of blockchain adoption among developers and users is necessary to create network externalities to facilitate rapid, coordinated adoption. We explained that a mix of soft and hard skills are necessary to overcome the challenge of coordinating expectations. More specifically, we argued that hard software engineering skills, together with world-class user experience design and institutional design, are needed to create a functioning blockchain system that can be adopted by end users. Furthermore, strategic management and marketing are needed to give end users the motivation to adopt. We also argued that mass adoption also requires blockchain leaders and end users to gain blockchain literacies, as this helps them understand the platform's value proposition, thus boosting their motivation to adopt. The job market demand for both soft and hard skills showed that the blockchain industry, at least in Australia, is aware of the need for a skills mix. Gaining and maintaining this skilled workforce may be what makes or breaks blockchain—whether adoption fizzles due to a lack of strategic management, usability and marketability, or whether it overcomes these challenges and becomes the mass-adopted institutional technology that many are hopeful of.

References:

[1] P. Schueffel, N. Groeneweg, and R. Baldegger, The Crypto Encyclopedia. Bern, Switzerland: Growth Publisher, 2019.

[2] M. Staples et al., Risks and Opportunities for Systems Using Blockchain and Smart Contracts. Sydney: Commonwealth Scientific and Industrial Research Organisation, 2017.

[3] C. Catalini and J. S. Gans, Some Simple Economics of the Blockchain, Rotman School of Management Working Paper No. 2874598. MIT Sloan Research Paper No. 5191-16. Cambridge: National Bureau of Economic Research, 2016.

[4] D. W. Allen, A. Berg, and B. Markey Towler, "Blockchain and supply chains: V-form organisations, value redistributions, de-commoditisation and quality proxies," Journal of the British Blockchain Association, vol. 2, no. 1, pp. 57-65, February 2019.

[5] D. Tapscott and A. Tapscott, "How blockchain will change organizations," MIT Sloan Management Review, Dec. 7, 2016. [Online]. Available: https://sloanreview.mit.edu/. [Accessed: March 26, 2020].

[6] S. Davidson, P. De Filippi, and J. Potts, "Blockchains and the economic institutions of capitalism," Journal of Institutional Economics, vol. 14, no. 4, pp. 639-658, January 2018.

[7] A. Bratanova et al., Blockchain 2030: A look at the future of blockchain in Australia. Brisbane, Australia: Commonwealth Scientific and Industrial Research Organisation, 2019.

[8] A. Linden and J. Fenn, Understanding Gartner's Hype Cycles, Strategic Analysis Report No. R-20-1971. Stamford, CT: Gartner, 2003.

[9] R. Sokolowski, Introduction to Phenomenology. Cambridge: Cambridge University Press, 2000.

[10] T. Wilson, "Big corporates back crypto 'plumbing' despite currency caution," Reuters, Apr. 18, 2019. [Online]. Available: https://www.reuters.com/. [Accessed March 26, 2020].

[11] Australian Securities Exchange, "CHESS replacement," ASX, Sept., 2016. [Online]. Available: https://www.asx.com.au/. [Accessed: March 26, 2020].

[12] Commonwealth Bank of Australia, "Commonwealth Bank and QTC create first Government bond using blockchain," Newsroom Home, Jan. 25, 2017. [Online]. Available: https://www.commbank.com.au/. [Accessed: March 26, 2020].

[13] M. Burn, CWS/6 IP Australia's Blockchain Initiatives. Canberra, Australia: Intellectual Property Australia, 2018.

[14] M. Bacina, "Trade marks and blockchain: Technology update," Insight, July 1, 2019. [Online]. Available: https://piperalderman.com.au/. [Accessed: March 26, 2020].

[15] Power Ledger, "Energy, reimagined," Power Ledger, June 2016. [Online]. Available: https://powerledger.io/. [Accessed: March 26, 2020].

[16] Bitcoin.com.au, "How Australia is leading the world in blockchain standards," Bitcoin Australia, Aug. 9, 2018. [Online]. Available: https://bitcoin.com.au/. [Accessed: March 26, 2020].

[17] A. Coyne, "Australia to take global lead on blockchain standards," ITNews, Sept. 15, 2016. [Online]. Available: https://www.itnews.com.au/. [Accessed March 26, 2020].

[18] C. Lim, Y. Wang, J. Ren, and S.-W. Lo, "A review of fast-growing blockchain hubs in Asia," Journal of The British Blockchain Association, 9959, August 2019.

[19] Upwork, "The fastest-growing skills on Upwork: Q4 2017," Upwork, May 1, 2018. [Online]. Available: https://www.upwork.com/. [Accessed: March 26, 2020].

[20] S. Bittle, "Job postings for blockchain skills double over 2016," Burning Glass Technologies Blog, Oct. 30, 2017. [Online]. Available: https://www.burning-glass.com/. [Accessed: March 26, 2020].

[21] M. Bellmas, "Is blockchain a false idol?," ANZ Insights, March 2019. [Online]. Available: https://institutional.anz.com/. [Accessed: March 1, 2020].

[22] E. Mesropyan, "30 non-financial use cases of blockchain technology," Medici, Dec. 18, 2017. [Online]. Available: https://www.gomedici.com. [Accessed: March 26, 2020].

[23] K. Doubleday, "Blockchain for 2018 and beyond: A (growing) list of blockchain use cases," Medium, Jan. 30, 2018. [Online]. Available: https://medium.com/. [Accessed: March 26, 2020].

[24] J. Bajkowski, "ANZ rips apart blockchain, catalogues its big list of non-uses," ITNews, March 25, 2019. [Online]. Available: https://www.itnews.com.au/. [Accessed March 26, 2020].

[25] K. Stinchcombe, "BankThink: Don't believe the hype: There are no good uses for blockchain," American Banker, Jan. 2, 2018. [Online]. Available: https://www.americanbanker.com/. [Accessed March 26, 2020].

[26] World Economic Forum and Accenture, Building Value with Blockchain Technology: How to evaluate blockchain's benefits. Geneva: World Economic Forum, 2019.

[27] C. Mason, Chen, C., Wan, S., Trinh, K., Duenser, A., Sparks, R., Walker, G., Zhao, Y., Burns, S., Reeson, A., Jin B., Naughtin, C., Data61 Australian Skills Dashboard, Australia: Commonwealth Scientific and Industrial Research Organisation, 2019. [Dataset]. Available: https://dmorg.csiro.au. [Accessed: Jan. 29, 2020].

[28] B. Anderson, "The most in-demand hard and soft skills of 2020," LinkedIn Talent Blog, Jan. 9, 2020. [Online]. Available: https://business.linkedin.com/. [Accessed: March 26, 2020].

[29] Burning Glass Technologies, Labor Insight™ Real-Time Labor Market Information Tool, Boston: Burning Glass Technologies, 2018. [Dataset]. Available: https://www.burning-glass.com/. [Accessed: Aug. 30, 2018].

[30] Department of Employment, Skills, Small and Family Business, Reskilling Australia: A data-driven approach. Canberra, Australia: Department of Employment, Skills, Small and Family Business, 2019.
[31] L. Wheelahan and G. Moodie, "Vocational education qualifications' roles in pathways to work in liberal market economies," Journal of Vocational Education & Training, vol. 69, no. 1, pp. 10-27, March 2017.
[32] World Economic Forum, Towards a Reskilling Revolution: A future of jobs for all. Geneva: World Economic Forum, 2018.
[33] S. Miller and D. Hughes, The Quant Crunch: How the demand for data science skills is disrupting the job market. Boston: International Business Machines Corporation, 2017.
[34] Deloitte, The Path to Prosperity: Why the future of work is human. Melbourne, Australia: Deloitte, 2019.
[35] ExcelinEd and Burning Glass Technologies, Credentials Matter - Report 1: A national landscape of high school student credential attainment compared to workforce demand. New York: ExcelinEd and Burning Glass Technologies, 2019.
[36] Burning Glass Technologies, Mapping the Genome of Jobs: The Burning Glass skills taxonomy. Boston: Burning Glass Technologies, 2019.
[37] Y. Zhao and C. Chen, Duplicate Detection from Online Job Advertisements. Canberra, Australia: Commonwealth Scientific and Industrial Research Organisation, 2019.
[38] A. Duenser and C. Mason, Evaluating Online Job Ads as Indicators of Demand for New Workers: Characterising strengths and weaknesses. Australia: Commonwealth Scientific and Industrial Research Organisation, 2020.
[39] B. Markey-Towler, "Anarchy, blockchain and utopia: A theory of political-socioeconomic systems organised using blockchain," Journal of the British Blockchain Association, vol. 1, no. 1, pp. 1-9, March 2018.
[40] O. E. Williamson, The Economic Institutions of Capitalism. New York: Free Press, 1985.
[41] J. M. Buchanan, "An economic theory of clubs," Economica, vol. 32, no. 125, pp. 1-14, February 1965.
[42] J. M. Buchanan and G. Tullock, The Calculus of Consent, Vol. 3. Ann Arbor, MI: University of Michigan Press, 1962.
[43] E. Ostrom, Governing the Commons: The evolution of institutions for collective action. Cambridge: Cambridge University Press, 1990.
[44] D. Allen, C. Berg, B. Markey-Towler, M. Novak, and J. Potts, "Blockchain and the evolution of institutional technologies: Implications for innovation policy," Research Policy, vol. 49, no. 1, 103865, February 2020.
[45] A. McAfee and E. Brynjolfsson, Machine, Platform, Crowd: Harnessing our digital future. New York: W. W. Norton & Company, 2017.
[46] W. J. Luther, "Cryptocurrencies, network effects, and switching costs," Contemporary Economic Policy, vol. 34, no. 3, pp. 553-571, July 2016.
[47] G. G. Parker, M. W. Van Alstyne, and S. P. Choudary, Platform Revolution: How networked markets are transforming the economy and how to make them work for you. New York: W. W. Norton & Company, 2016.
[48] K. Dopfer, J. Foster, and J. Potts, "Micro-meso-macro," Journal of Evolutionary Economics, vol. 14, no. 3, pp. 263-279, July 2004.
[49] G. Dosi, "Technological paradigms and technological trajectories: A suggested interpretation of the determinants and directions of technical change," Research Policy, vol. 11, no. 3, pp. 147-162, June 1982.
[50] J. S. Metcalfe, J. Foster, and R. Ramlogan, "Adaptive economic growth," Cambridge Journal of Economics, vol. 30, no. 1, pp. 7-32, January 2005.
[51] J. S. Metcalfe, Evolutionary Economics and Creative Destruction. London: Routledge, 1998.
[52] R. R. Nelson and S. G. Winter, An Evolutionary Theory of Economic Change. Cambridge: Harvard University Press, 2009.
[53] M. Rysman, "The economics of two-sided markets," Journal of Economic Perspectives, vol. 23, no. 3, pp. 125-43, August 2009.
[54] M. L. Katz and C. Shapiro, "Network externalities, competition, and compatibility," American Economic Review, vol. 75, no. 3, pp. 424-440, June 1985.
[55] M. L. Katz and C. Shapiro, "Systems competition and network effects," Journal of Economic Perspectives, vol. 8, no. 2, pp. 93-115, May 1994.
[56] M. L. Katz and C. Shapiro, "Technology adoption in the presence of network externalities," Journal of Political Economy, vol. 94, no. 4, pp. 822-841, August 1986.
[57] T. Schelling, The Strategy of Conflict. Cambridge: Harvard University Press, 1960.
[58] K. Lewin, Field Theory in Social Science: Selected theoretical papers. Oxford: Harpers, 1951.
[59] H. A. Simon, "Motivational and emotional controls of cognition," Psychological Review, vol. 74, no. 1, pp. 29-39, January 1967.
[60] H. A. Simon, "From substantive to procedural rationality," in Method and Appraisal in Economics, S. Latsis, Ed. Cambridge: Cambridge University Press, 1976, pp. 129-148.
[61] H. A. Simon, "Rational choice and the structure of the environment," Psychological Review, vol. 63, no. 2, pp. 129-138, March 1956.
[62] D. MacDonald-Korth, V. Lehdonvirta, and E. T. Meyer, The Art Market 2.0: Blockchain and financialisation in visual arts. Oxford and London: University of Oxford and The Alan Turing Institute, 2018.
[63] L. Festinger, A Theory of Cognitive Dissonance. Stanford, CA: Stanford University Press, 1962.
[64] S. Hajkowicz, A. Reeson, L. Rudd, A. Bratanova, L. Hodgers, and C. Mason, Tomorrow's Digitally Enabled Workforce: Megatrends and scenarios for jobs and employment in Australia over the coming twenty years. Brisbane, Australia: Commonwealth Scientific and Industrial Research Organisation, 2016.
[65] United Nations Educational, Scientific and Cultural Organization Institute for Statistics, UIS.Stat (Education, full dataset), Montreal: UNESCO Institute for Statistics, 2019. [Dataset]. Available: http://data.uis.unesco.org/. [Accessed: Jan. 3, 2019].

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
JA, AB, and B M-T confirmed they prepared the manuscript in entirety.

Funding:
The Australian Computer Society funded the previous foundational research project resulted in the publication of "Blockchain 2030: A look at the future of blockchain in Australia" report. This funding allowed the researchers to access to the Burning Glass Technologies data set.

Acknowledgements:
We thank Dr Claire Mason and Dr Caron Chen from CSIRO's Data61 for their assistance in exploring the Data61 Australian Skills Dashboard, as well as Dr Kelly Trinh for her early stage observations of the BGT data set. We also thank Dr Lucy Cameron, Dr Mark Staples and Dr Claire Mason from CSIRO's Data61 for reviewing the draft manuscript.

We are grateful to the peer reviewers for reviewing the draft manuscript and providing constructive criticism and helpful comments.

The authors also acknowledge the kind contribution of Adzuna Australia's data sets to this research.

We thank Burning Glass Technologies for providing the Labor Insight™ data set.

[1] According to the Crypto Encyclopedia, a blockchain is 'a publicly accessible distributed ledger that was initially designed and implemented to enable Bitcoin transactions. It is a piece of information technology infrastructure that serves as a database which is used to keep a continuously growing list of records, so called blocks' [1].

[2] Distributed ledger technologies (DLTs) are digital infrastructure that record and store data, and consensually share and synchronise the data through a network spanning multiple sites, institutions and/or geographies [1] ibid.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(1)2020

Browser-based Crypto Mining and EU Data Protection and Privacy Law: A Critical Assessment and Possible Opportunities for the Monetisation of Web Services

Christopher F. Mondschein
European Centre on Privacy and Cybersecurity (ECPC), Maastricht University, The Netherlands
Correspondence: c.mondschein@maastrichtuniversity.nl
Received: 17 March 2020 **Accepted:** 24 March 2020 **Published:** 12 April 2020

Abstract

Recently, browser-based crypto mining (or browser mining) received attention in academic literature, mainly from the work in the field of computer science. Browser-based crypto mining describes the act of websites or other actors mining cryptocurrencies for their own gain on client-side user hardware, which mainly takes place by mining Monero through Coinhive or similar codebases. Although the practice gained infamy through the various ways in which it was illicitly deployed, browser mining has the potential to act as an alternative means for the monetization of web services and digital content. A number of studies explored browser mining for monetization purposes and highlighted its short-comings compared to the traditional advertisement-based monetisation strategies. This paper discusses the practice in light of EU data protection and privacy law, notably the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD), which is currently being overhauled and aligned with the GDPR. It adds to the discussion surrounding the feasibility of browser mining as a potential alternative for monetization by exploring the legality of browser mining in relation to EU data protection and privacy law and by identifying possible benefits regarding the protection of individuals' personal data and privacy by deploying browser mining. It is argued that employing browser mining in a transparent and legitimate manner may be an additional option to financing websites and online services due to the growing legal pressure on advertisement models such as programmatic advertisements that rely on the exploitation of large amounts of personal data and ad networks.

Keywords: *Cryptocurrency; Mining, Blockchain, GDPR, ePrivacy, Privacy and Data Protection, EU Fundamental Rights*

JEL Classifications: *K24, K42*

1. Introduction

The monetization of web services mainly relies on the advertising revenue, with a large part of the revenue stemming from programmatic advertising and behavioural targeting, with an estimated €16.8 billion market share in Europe [1]. Programmatic advertising entails the mostly automated buying, selling and matching of digital advertising spaces and advertisers over a number of platforms and aggregators, in order to display relevant ads to consumers browsing the web. The buying and selling of an ad space is automated and happens through real-time bidding (RTB) auctions within milliseconds. The ads are then displayed to users based on the users' deduced preferences that are established over the course of being tracked and profiled based on their behaviour while surfing multiple websites [2]. Online advertising, especially programmatic advertising, is criticized for its impact on individuals' privacy and the protection of their personal data for a number of reasons: these include the large quantities of personal data collected and processed, including sensitive personal data (such as sexual orientation, health data, religious belief and so on), and the general lack of awareness that the users have of these practices. Further, the practice also entails the automated sharing of personal data with many entities at high velocity, leading to the risk of data getting leaked which cannot be accounted for, thus breaching the principles of EU data protection law [3]. In this context, we also see that access to a website is often made conditional upon the acceptance of tracking and advertising (so-called tracking walls), affecting the legality of the consent collected under these practices [4].

Hence, browser-based crypto mining (or browser mining) was envisioned as an alternative to the tracking and targeting practice that is dominating online advertising [5]. Browser mining entails websites or other actors injecting mining code into client-side hardware in order to mine cryptocurrencies using those devices' computational power, thereby converting end-user devices' computational power into cryptocurrencies for the benefit of the entities deploying the mining code. Although being conceived as an alternative to online advertising, browser-based crypto mining (or browser mining) mostly garnered public attention due to scandals that revolved around its illicit use, especially during the period of 2017–2018.

Browser mining also drew the attention of academics in the field of computer science and information security studies, who mainly focused on identifying the prevalence and spread of crypto mining and its detection [6] as well as on its feasibility for monetizing web services compared to the traditional online advertising models [7]. While a large part of the the body of research touches upon browser minings' privacy and data protection implications [8], none has yet comprehensively addressed these issues. This paper discusses the practice of browser-based crypto mining in light of EU data protection and privacy law, focusing on the General Data Protection Regulation (GDPR) [9], the ePrivacy Directive (ePD) [10] and the proposal for an ePrivacy Regulation (ePR) [11]. In doing so, the paper explores the legality of browser mining in relation to EU data protection and privacy law and identifies possible benefits regarding the protection of individuals' personal data and privacy by deploying browser mining over traditional online advertisement strategies.

The paper is structured as follows: Section 1 introduces the topic and frames the discussion. Section 2 presents a short history of browser mining,

describes the practice and illustrates deployment methods of browser mining. Section 3 analyses browser mining in light of EU privacy and data protection law. Section 4 identifies possible benefits that browser mining has over online advertising practices that utilize personal data and assess what measures could be taken within the current EU privacy and data protection framework to accommodate browser mining. It further adds an outlook on where the legal framework may warrant for amendment, specifically addressing the proposal for an ePR.

1. Browser mining

a. A brief history of browser mining

The emergence of the idea of browser-based crypto mining as an alternative to finance web services dates back to 2013–2014, with an example of the MIT-based student project Tidbit. As a project, Tidbit was the product of a hackathon and was conceived with the purpose of offering an alternative to online advertising [12]. The project came under legal scrutiny soon after, leading to proceedings in New Jersey, due to Tidbit being viewed as malware and having the potential to afflict serious harm to consumers as they 'may have their computers "co-opted" or "hijacked" without their consent by unscrupulous website operators using the Tidbit code' [13]. This assessment foreshadowed the malicious applications of browser mining that would become prevalent, and the case led to the shutting down of Tidbit due to the mounting legal pressure. Yet in an interesting statement in the proceedings, the Superior Court of New Jersey acknowledged the need for openness towards innovative technological solutions, stating that:

> "this investigation, may be acting to discourage creative and 'cutting edge' new technology. (…) it appears that the Tidbit program and other similar creative endeavors serve a useful and legitimate purpose. There is nothing presented to the Court that evidences an inherently improper or malicious intent or design by Plaintiff. Rather, Tidbit appears to be an instrumentality or tool that has great potential for positive utility. The Court is mindful, however, of the State's concerns that this tool could also be subject to abuse and misuse [14]."

During the period of 2017–2018, scandals and news surrounding browser mining were abundant and saw a peak. The file-sharing website The Pirate Bay experimented with running mining code on its website in 2017 in order to monetize its service [15]. In 2018, the crypto mining code was illicitly injected into various websites, including the UK's data protection supervisory authority, the Information Commissioner's Office (ICO) [16], among many others, which mined cryptocurrencies through visitors' web browsers for the duration of their visit [17]. The US television giant CBS had mining code injected into its Showtime web-streaming service, which mined Monero in users' browsers, although it is unclear who was responsible for deploying it [18]. Crypto mining code was also deployed by a rogue employee of the E-Sports Entertainment Association (ESEA), leading to 14,000 devices being affected, which resulted in legal actions in New Jersey and California [19]. Further incidents involve the running of mining code in ad networks, Youtube ads, browser extensions, routers, Android mobile devices, fundraising campaigns by UNICEF and gaming mods, with numerous examples existing [20]. These scandals led to a negative perception of browser mining, with it being described as 'cryptojacking,' 'thieves in the browser' [21], and is widely being framed as a security issue.

With the demise of Coinhive in 2019, the browser mining landscape is in turmoil. However, security experts believe that the practice will prevail and surmise that it will also see a resurgence with the growth of (unsecured) IoT devices that could be exploited for the mining of cryptocurrencies [22].

b. A basic explanation of browser mining

'Mining' is one of the cornerstones of the functioning of blockchain-based cryptocurrencies. A number of cryptocurrencies rely on the so-called Proof-of-Work (PoW) distributed consensus algorithm in order to operate [23]. PoW requires participants in the cryptocurrency's network to solve cryptographical puzzles in order to validate transactions in the network, which is called 'mining.' Miners are rewarded, for solving cryptographical puzzles, a unit of cryptocurrency specified in the cryptocurrency's protocol [24]. The act of mining cryptocurrency was conceived as a way of sustaining a distributed network, and such a distribution functions as a means to prevent any party in the network from dominating it by owning 51% or more of the network's computational capacity, underlining the importance of a good distribution of mining power among devices and parties in the network [25].

As such, the idea of utilizing end-user devices to mine cryptocurrencies is not new and even follows the goal of a wide distribution of mining among devices in those networks. In this regard, a large number of mining services exist in the form of websites or apps that allow individuals to mine cryptocurrencies using their personal devices such as computers, laptops, smartphones and so on, without being required to run a full node of the cryptocurrency's network [26]. Similarly, the idea of individuals being able to donate or lend computational power to specific causes has already seen many applications, with numerous applications for science [27]. Both of these approaches culminate in browser mining, as the mining of cryptocurrencies takes place in the end-user's device but the benefits (that is, the cryptocurrency that is mined) are received by the entity deploying the mining code.

The most popular codebase for browser mining is Coinhive [28], which mines the cryptocurrency Monero, but numerous similar codebases exist (for example, Crypto-Loot, CoinImp, Minr, deepMiner, JSECoin and Coinhave) [29]. Mining applications such as Coinhive usually take a percentage of any mined cryptocurrencies, for instance, Coinhive took a 30% cut, whereas Crypto-Loot took 12% [30]. At the height of its operation, it is estimated that the Coinhive codebase was deployed on 0.08% of 137 million .com/.net/.org sites and the Alexa Top 1M domains were inspected, resulting in the mining of 1.18% of all blocks of the Monero cryptocurrency as of mid-2018 [31]. Coinhive ceased its operations in March 2019, due to the diminishing returns it created as a result of the drop in prices of cryptocurrencies, which also affected the value of Monero and legal concerns surrounding the practice [32].

The prevalent cryptocurrency that is mined via browser mining is Monero, as it is a cryptocurrency that focuses on ASIC (application specific integrated circuits) resistance and privacy; however, a number of other cryptocurrencies are also frequently mined through browser-based crypto mining, including Ethereum, Zcash, LiteCoin, Dash and others, with some applications utilizing third-party mining libraries that allow for the mining of multiple cryptocurrencies. The prevalence of Monero in this context is based on developments visible in a number of cryptocurrency protocols, aiming to ensure that the effectiveness of specialized mining equipment (ASIC) is diminished in order to prevent parties from controlling too large a degree of a network's computational power. Therefore, Monero is one of the cryptocurrencies that is attractive to mine in end-user devices, and it is also the cryptocurrency most often mined in browsers, whereas mining Bitcoin via non-specialized equipment has become unprofitable.

c. The deployment of browser mining

It is important to highlight some deployment methods of browser mining in order to distinguish between outright malicious deployment methods and methods that could be legitimate, in order to inform the legal discussion in Section 3. The most common form of deployment works by integrating a miner API into a website. This is the prevalent way to deploy Coinhive and several browser mining clones. These APIs offer a mining library which can easily be deployed on a website, which runs the miner via JavaScript or WebAssembly client-side. Website providers merely need to add a snippet of the code to their website and configure their

cryptocurrency wallet in order to run Coinhive or similar miners, making deployment rather easy. Once deployed, the script is loaded client-side and executes the link when the page is loaded and launches the miner in a user's browser, with the miner being loaded from a third-party website for most mining APIs (for example, Coinhive and Crypto-Loot). Some miners are self-hosted by the website provider, bypassing the reliance on third-party websites (for example, DeepMiner) [33]. Next to the deployment described above, Coinhive also offered a number of other ways to deploy its mining code:

- Shortlink service: shortens a URL for easier forwarding;
- In-game mining for games;
- CAPTCHA, which is a test to determine whether a user is a person or a bot (Figure 1) [34].

Figure 1. Coinhive CAPTCHA

Coinhive also developed an SDK for Android app developers, facilitating the mining integration for mobile applications [35].

Regarding the transparency of the deployment of crypto mining, browser-based crypto miners such as Coinhive can usually be detected – and subsequently blocked – rather easily, based on the identification of links to the mining websites that are integrated in scripts deployed by the websites running the API, with some APIs presenting the ability for obfuscation as a selling point [36]. However, the obfuscation of links has led to more sophisticated methods of detection being researched that go beyond the establishment of blocking lists of known miner links found in scripts (blacklisting) [37]. In this regard, self-hosted miners allow for stronger obfuscation. It is noted for self-hosted miners that '[u]ltimately, this is more flexible for attackers. It also helps them avoid blacklists by using their own domains (changing it whenever they need) for the client script and the websocket proxy' [38].

Next to the obfuscation of the miner scripts, the transparency and awareness of users within the user interface is also an important issue. Some miners such as Crypto-Loot advertise themselves as stealthy and promise that users will not be able to identify whether a website has deployed the miner [39]. In addition, the so-called persistent drive-by crypto mining is another technique to deploy browser mining without user awareness. It is used by deploying the same browser-based mining script found in the Coinhive API or similar APIs, but this time, the user enters a website which runs a script to open a new browser window that runs the miner. This browser window is opened as a so-called pop-under (as opposed to a pop-up), and it is placed behind the desktop's taskbar, masking its presence. Users only see that the browser is open by virtue of the desktop icon but do not see how many different windows are open. Once they close all windows, the mining also ceases [40]. Arguably, these practices contribute to the perception of the practice as illicit or dodgy and, as is argued below, are also illegal in view of EU privacy and data protection law.

On the other hand, within the Coinhive family of products, the Authedmine API was developed with the aim of facilitating the provision of information to users and the collection of consent for mining. It was developed to counter the illicit appearance of Coinhive and added an information notice and a consent option (see Figure 2). The miner is only engaged when users click the button in the pop-up. Similar configurations of Authedmine were deployed, for instance, in campaigns by UNICEF Australia and CPUforGood, in order to collect donations for good causes via browser mining [41].

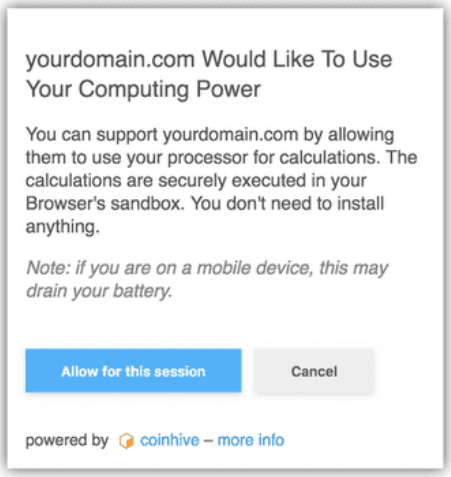


Figure 2. Authedmine notice example

d. Intermediate conclusion

Browser mining can be deployed in a number of different ways. APIs can be self-hosted or run scripts that link to third-party websites. Here, transparency and user awareness are issues with regard to the deployment of browser-based crypto miners. The mode of deployment and the intent of those entities deploying miners have to be taken into account, along with the actual deployment. Obfuscation arguably contributes to the perception of the practice as illicit or dodgy and as we will see, it also is illegal in the context of EU privacy and data protection law. The obfuscation of links in the script seems particularly questionable as this is used solely for the prevention of detection. The same holds true for persistent drive-by crypto mining. Conversely, solutions such as Authedmine strive for transparency and give the user an option to consent. These examples illustrate the broad range in which the technology can be utilized.

2. Browser mining in the light of EU privacy and data protection law

In order to establish the legality and the compatibility of browser mining in the light of EU privacy and data protection law, it is necessary to assess whether browser mining falls within the scope of the instruments in question, in particular the GDPR, the ePD and the proposal for an ePR.

Within the legal framework of the EU, a distinction is made between the fundamental right to privacy and the right of data protection. At the level of primary EU law, the former is enshrined in Article 7 of the Charter of Fundamental Rights of the EU (the Charter), whereas the right to data protection is explicated in Article 8 of the Charter and in Article 16 of the Treaty on the Functioning of the EU (TFEU). Article 16(2) TFEU provides a legal basis for the EU to adopt a secondary legislation on the protection of personal data [42]. The conceptualization of these two fundamental rights as separate rights and the relation between the rights are still subject to academic deliberation [43].

The EU is competent to adopt legislation in the field of data protection as well as in the scope of the functioning of the internal market. The EU also adopted legislation regarding the privacy of publicly available telecommunication networks and services in the form of the ePD, dating back to 2002. The ePD was updated in 2009 by the so-called Citizens' Rights Directive in order to regulate and clarify its applicability with respect to web tracking technologies such as cookies [44]. The EU adopted legislation in the field of data protection by virtue of the GDPR, which was adopted on the basis of Article 16(2) of TFEU, which replaced the Data Protection Directive (DPD) adopted in 1995. With the GDPR entering into force on 25 May 2018 [45], the EU started the reform process for the modernization of its data protection framework.

Within this reform effort, it was planned to have the revised ePR enter into force at the same time as the GDPR. One of the reasons to modernize the ePrivacy Framework was that, among Member States, the ePD was implemented in a variety of ways that undermined the protection of end-user devices due to the dilution of the provisions on tracking [46]. To remedy this, the European Commission published a proposal for the ePR in January 2017 [47]. However, the Council failed to reach a political agreement during this time, leading up to the failure of the proposal in the Council on 3 December 2019. During the Council's Telecomm Group on that day, the newly designated commissioner, Thierry Breton announced, a plan to withdraw and re-table the proposal, with the future of the ePR left unclear [48].

a. The GDPR and the ePrivacy Framework

The GDPR applies to fully or partially automated processing of personal data or processing of personal data using a filing system and applies to entities established in the territory of the EU/EEA which processes such data, as well as entities that are established outside of the EU but process data by either marketing goods or services in the EU or by tracking individuals located in the EU [49]. The scope of what constitutes personal data under the GDPR is wide and includes, for instance, dynamic IP addresses [50] and trackers and identifiers such as cookies [51].
The ePD protects individuals' privacy of telecommunication and applies 'to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices [52].' The ePD further holds specific provisions regarding the privacy of end-user devices in Article 5(3):

> "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

The provision makes the storing of information or the accessing or reading out of information stored in end-user devices conditional upon the user giving his or her consent after receiving clear and comprehensive information, with the exception of purely technical operations.
The provisions of the ePD form *lex specialis* to those of the GDPR, with a number of provisions of the Directive particularizing those of the GDPR and others complementing the provisions found in the GDPR [53]. After the GDPR replaced the 1995 DPD [54], references to provisions in the DPD found in the ePD had to be replaced with references to the GDPR [55]. This was previously established in a number of opinions of advisory bodies and was confirmed in the case law of the Court of Justice of the European Union (CJEU) [56].

b. The GDPR, the ePrivacy Framework and browser mining

1. The application of the GDPR

Regarding the applicability of the GDPR to browser mining, it is necessary to assess whether browser mining entails the processing of personal data. The operations of a website may entail a number of different processes that fall within the material scope of the GDPR as personal data is processed: these can include audience measurement, tracking of users for monetization purposes, ensuring the security of the website against cyberattacks and so on [57]. When comparing these operations to the running of a script in the end-user's device, it is difficult to establish that browser mining entails the processing of personal data. In this regard, the aforementioned processing operations have to be seen as separate operations with their own purpose, with personal data collected and processed, and require separate legal bases [58].

From a technical perspective, it therefore becomes doubtful whether the GDPR applies to browser mining, as the material scope of processing of personal data does not seem to be triggered.
Nevertheless, if this were the case and the GDPR were to apply, the full set of compliance obligations would come into effect. This would create a number of difficulties in the context of browser mining, as the GDPR does not sit well with blockchain applications [59]. One of the key issues to resolve are, on the one hand, the designation of controller(s) and processor(s) in order to attribute the obligations arising from the GDPR, and on the other hand, the designation of data subjects, who derive rights from the GDPR. A problem arises as roles can conflate in the context of blockchain applications: on the one hand, the end-user whose device is used to mine cryptocurrencies would become a data subject, whereas the end-user also mines cryptocurrencies for the benefit of the website operator, thereby potentially becoming a data processor [60].''In this situation it becomes problematic when considering whether personal data (that is, the transactional data) is processed by third parties (that is, the miners) in this situation, especially when dealing with privacy-focused cryptocurrencies such as Monero [61]. An orthodox reading of the GDPR would result in accepting the privacy-preserving measures of such cryptocurrencies merely as additional measures to secure personal data; however, the GDPR would still apply in full. This would also align with the fundamental rights logic of the GDPR that aims at securing the protection also for new technological developments. On the other hand, the development of new protocols such as CryptoNote [62] and its derivatives (such as CryptoNight, used for the Monero cryptocurrency) asserts pressure on the client-server paradigm that underlies the GDPR's regulatory structure.

In sum, it is rather doubtful whether browser mining falls within the material scope of the GDPR; however, if the GDPR applies, compliance becomes difficult.

2. The application of the ePD

Conversely, Article 5(3) ePD is applicable in the context of browser mining. Article 5(3) is one of the provisions that particularizes the GDPR [63]. The provision has a wider material scope than personal data and applies to any information, including non-personal data [64]. The rationale behind this is the guarantee of an effective protection of end-user devices' privacy in light of technological developments. Indeed, the scope of Article 5(3) ePD was clarified on numerous occasions and the provision was adapted by the Citizen's Rights Directive in 2009 in order to accommodate new technological developments [65]. These changes were guided by the legislator's and the regulators' will to ensure a technologically neutral approach that allows for the application of the provision to technological developments such as cookies, browser fingerprinting and similar technologies [66]. The extension of protection under Article 5(3) ePD, regardless of whether the processing of personal data takes place, was also affirmed by the CJEU stating that the 'provision aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data' [67]. Further, the CJEU opined 'that protection applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended, in particular, as is clear from that recital [Recital 24 ePD], to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge' [68].

The scope of protection offered by Article 5(3) ePD also extends to forms of interactions with end-user devices that differ from tracking based on cookies or device fingerprinting. It has to be questioned whether browser mining falls into the scope of this provision since the method does not intend to track users but makes use of a device's computational power for the duration of the visit to a website.

In this regard, other forms of intrusion in end-user devices have been deemed to fall within the scope of Article 5(3) ePD, as is illustrated by the Sony-MediaMax case [69]. The automatic and unobtrusive installation of content rights management software deployed when playing media stored on CDs, CD-ROMs, and USB keys was deemed an unlawful intrusion, contravening Article 5(3) ePD [70]. The use of spyware or other intrusive means to access end-user devices was brought into the scope of the ePD [71]. Further, in the guidance issued by the Dutch data protection supervisory authority, it is also stated that 'the prohibition of cookiewalls is not restricted to the setting of cookies. Not only cookies are covered by this description, but also similar technical solutions that require consent fall within the scope. These are technical solutions such as JavaScript, Flash cookies, HTML5-local storage and/or web beacons' [72]. Following these developments, the application of Article 5(3) ePD to browser mining seems logical, as running scripts in end-user devices would require valid consent.

Yet this conclusion still highlights the uneasy relation between browser mining as a new technological development and the legal framework at issue. Similar to earlier developments in tracking technologies, the legal framework is pushed to its boundaries due to these new developments, as witnessed with cookies, device fingerprinting and the Sony-MediaMax debate. With regard to browser mining, the complexities surrounding the interplay between the GDPR and the ePD are highlighted once more: the fact that this interplay largely hinges on the processing of personal data and that a form of monetization of web services devoid of any interest in the person behind the device was not envisioned by the legislator creates legal uncertainty regarding the application of the law to browser mining. However, given the telos of the provision – the protection of fundamental rights and especially the protection of individuals' sphere of privacy with regard to their devices – it is likely that browser mining falls within the scope of Article 5(3) ePD.

3. Application under proposal for the ePR

According to Article 8(1) of the proposed ePR, '[t]he use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned' is conditional either upon the end-user's consent, technical necessity in the context of electronic communications, the provision of an information society service explicitly requested by the user or for audience measurement, provided that such measurement is carried out by the provider of the information society service requested by the end-user (emphasis added). The proposed Regulation continues the wide definitional approach of its predecessor and clarifies that the use of processing and storage abilities falls within the ambit of its provisions. Hence, from the wording of Article 8(1) ePR, it can be deduced that browser mining would fall within the scope of the ePR.

c. Compliance under the ePrivacy Framework

It is unlikely that browser mining falls within the scope of the GDPR, however, it likely falls within the ambit of Article 5(3) ePD, and the wording of Article 8(1) ePR similarly applies to browser mining. This means that any operator deploying a miner must do so in a compliant manner.
Article 5(3) ePD makes the valid deployment of a miner conditional upon prior notification of the user and collection of the user's consent prior to running the mining script on their device. Even in the event of personal data being processed, the entity deploying the miner would be bound to consent as a legal basis as opposed to a choice of legal basis under Article 6 GDPR, as the provision of the Directive applies according to the l*ex specialis* rule.[73] Further, the technical exemptions envisioned in Article 5(3) ePD, second sentence have to be construed narrowly and are not applicable to browser mining.
Similarly, Articles 8 and 9 ePR would apply, mandating prior informed consent with reference to Articles 4(11) and 7 GDPR by virtue of Article 9 ePR.
In assessing these requirements, it is clear that the obfuscated deployment of a miner contravenes the provisions of both the ePD and the ePR and must therefore be deemed illegal. Regarding the various forms of deployment such as a CAPTCHA or a shortlink service, the same requirements apply as with browser-based mining, requiring the provision of information and the prior collection of user consent.

1. The provision of information

Article 5(3) ePD states that users should be provided with 'clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.' The provision contains similar requirements to former Article 10 DPD [74], which is now replaced by Article 13 GDPR. The information in that provision relates, inter alia, to the identification of relevant actors (controller(s), processor(s), third parties who receive personal data), the purposes and legal bases related to the processing, the rights of data subjects, the existence of data transfers to non-EU/EEA states and the modalities of such transfers and the existence of automated decision-making. In the context of browser mining, this information may not be relevant or might not even exist as there is arguably no processing of personal data. It therefore needs to be questioned what information should be provided. Given that the ambit of Article 5(3) ePD extends beyond the scope of personal data, even when there is no processing of personal data involved, there must be meaningful information for users [75]. The Authedmine user interface offers some general information on the use and also a warning of the potential battery drainage (see Figure 2). The website is indicated as the entity deploying the miner and the purpose is explained. Here, any third party should also be named. The legal obligation here is uncertain and it has to be questioned if such information is 'meaningful.' In sum, the exact information requirements for browser mining are not clearly laid out in the law, and the burden is put on the entity deploying the miner to ensure that the information is clear and comprehensive and that at least the purpose and the entities involved are named as the validity of consent hinges upon this. Again, the probable lack of awareness of the practice becomes apparent as it seems at odds with the regulatory mechanism in the provision.

This also holds true for the provision on the information requirements in the ePR: Article 8(1)(b) mandates the collection of consent and Article 9 links the modalities and the validity of consent to those set out in the GDPR in Articles 4(11) and 7. This means that consent must be 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4(11) GDPR). Given that the validity of the consent is tied to it being, inter alia, informed, it can be deduced that users are required to receive sufficient information. However, also in the case of the ePR, the scope of the information required, its format and its modalities are not clear in the context of browser mining. In this situation, the tension arises as the ePR would apply but the GDPR would not, something that has not been fully accounted for in the ePR and an issue that the ePR does not rectify [76].

2. Consent for browser mining

The legal uncertainty surrounding browser mining regarding the consent requirement under the ePD and ePR is even more striking: under the ePD,

consent must be collected prior to the deployment of the miner. The CJEU clarified the conditions for consent in Planet49, linking the requirements under Article 5(3) ePD with those of the DPD and GDPR, stating that consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [77].

A similar construction is found in the ePR as Article 9 clarifies that consent has to be construed within the meaning of the GDPR.
In this regard, Article 7(1) GDPR explicates: 'Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.' Hence, the logic of shifting the burden to prove compliance with the lawful collection of consent for the controller seems logical when personal data is processed and such data needs to be protected under the principle of accountability. Here, a connection between the data and the data subject exists for the duration of the existence of the data, which extends beyond the phase of collection. This begs the question of how and whether this provision applies with regard to browser mining, which arguably does not entail the processing of personal data.

Here, it can be argued that browser mining only connects a user to the entity deploying the miner during the time of mining, i.e. when the user vists the website and the script runs. Thus, the point of connection between a user and a website operator is effectively severed once the mining script stops running and the transaction of computing power for cryptocurrency has ceased and no personal data is processed for the mining. The logic behind the ongoing protection of personal data and the placing of the burden of proof on the entities handling personal data rests on the fact that the processing of personal data poses an ongoing risk to the data subject for the time the data exists, i.e. longer than the mere visiting of a website.
In applying the provision to browser mining, the creation of a consent trail would necessitate the processing of personal data in order to record the consent of the user at a specific time in connection to a notification that was provided in order to comply with Article 7(1) GDPR, which becomes applicable in this situation by reference under the ePrivacy Framework. Essentially, this means that in order to prove valid consent for browser mining – a process intended to replace the need for the processing of personal data – personal data would have to be processed so that the entity deploying the miner can prove it collected lawful consent. At face value, this seems somewhat absurd, however, the alternative would mean that no valid proof would be established whenever utilizing browser mining. Even if the user is informed and his or her consent was collected in a valid way, there would be no proof of this.
From the viewpoint of protecting the privacy and integrity of an end-user device, the lack of proof of intrusion in such a device would also require the collection of consent in a demonstrable fashion. Here, it would be beneficial for the legislator to add clarity by introducing self-standing provisions in the ePR that explicate similar principles as the GDPR, something that a number of scholars have suggested [78].

3. The benefits of browser mining

In the discussion surrounding the monetization of web services, previous research on browser mining has shown it to be largely a lacklustre replacement for programmatic advertisement from a financial perspective [79]. Further, the practice is also subject to the volatility of the cryptocurrencies mined [80]. The major question that arises when comparing browser mining as a monetization strategy with other forms of monetization is what the privacy impact on users is. In this respect, browser mining would indeed be beneficial to users in case it is deployed as an alternative to monetization strategies that rely on the processing of personal data, such as programmatic advertising. However, other forms of online advertising, such as contextual advertising, offer a similarly privacy-friendly solution [81]. The context of deployment is important in gauging the profitability of these means: contextual advertising relies on the finding of relevance to a website/the context in which advertising is shown, thereby detaching the selection of advertisement from the individual and relying on the broader context to establish the meaning for advertising. Where such a context can be deduced, contextual advertising becomes attractive, albeit it is still being questioned on how well it performs against programmatic advertisements [82]. Where such a context cannot be deduced, such as on general news sites or web services that do not offer a stream-lined contextual setting, the personalization of advertising becomes necessary. Here, browser mining poses an interesting alternative. For the profitability of browser mining, the duration of a user visiting a website is also decisive [83].
A further consideration is the use of personal data and users' perception of such practices in relation to website monetization. Research has shown that users seem to be reluctant in accepting tracking and profiling practices [84] and would prefer browser mining [85]. This information has to be taken with a grain of salt, as research on self-reporting on privacy and data protection matters shows that many users lack a basic understanding of the intricacies and the trade-offs they are engaging with [86]. Nevertheless, browser mining could be viewed as a privacy-friendly alternative. However, this is conditional on it being applied as an alternative. It would therefore be undesirable to apply browser mining as an additional source of revenue next to programmatic advertisement.

This also plays into the current debate surrounding tracking walls. Tracking walls force users to consent to tracking for monetization purposes and make such consent the condition for accessing a website or web service [87]. In essence, the practice creates a zero-sum game between users, on the one hand, and websites and third-party providers, on the other hand: either the user preserves their privacy and the website operator and the related third parties do not receive any revenue or the user loses his privacy so the operator and the related third parties can make a profit.

Throughout the existence of both the ePD and the proposed ePR, tracking walls have been a persistent point of disagreement among Member States. The 2009 Citizen's Rights Directive did not lead to a uniform interpretation of Article 5(3) ePD [88], and the disagreement among Member States in the Council led to the failure of the ePR in its current state. The validity of consent collected via tracking walls has been challenged, along with other issues surrounding non-compliance in programmatic advertisement, with data protection supervisory authorities in some EU Member States prohibiting tracking walls [89]. In its Planet49 judgement, the CJEU clarified the conditions for consent under Article 5(3) ePD, yet it availed itself from taking a stance in the dispute surrounding tracking walls [90]. Advocate General Szpunar however stated in his opinion that the 'selling' of personal data and the processing of personal data for the purpose of monetizing a service could be a condition for access to such service [91]. This hints at an acceptance of the conditionality of providing personal data for 'free' services (in that case, participation to a lottery), a view that opposes the opinions and guidance by a number of data protection supervisory authorities outlined above.

Here, browser mining might help by softening the adversarial nature that exists between users wanting to protect their personal data and privacy and website operators wishing to monetize their services by offering a means to preserve user privacy while at least creating some revenue for website operators. In this regard, the current uncertainty surrounding the status of the proposal might allow for a reconsideration.
Regarding tracking walls in the ePR, Zuiderveen Borgesius et al. illustrate a number of measures the legislator could take [92]. They note that a full or partial ban of tracking walls can take place and make a compelling argument for at least a partial ban for circumstances including 'public service media, commercial media, professions with specific confidentiality rules, and the public sector' [93]. In these circumstances, they propose a blacklist, along with a grey list:

> If a situation is on the grey list, there is a legal presumption that

> a tracking wall makes consent involuntary, and therefore invalid. Hence, the legal presumption of the grey list shifts the burden of proof. For situations on the grey list, it is up to the company employing the tracking wall to prove that people can give 'freely given' consent, even though the company installed a tracking wall [94].

If one were to accept that a total ban on tracking walls is not a realistic option, given the political disagreement and legal uncertainty, a compromise next to the one proposed above could be that tracking walls may be accepted in limited circumstances where one of the options provided as an alternative to the processing of personal data is to allow browser mining. The law would have to clarify that this would be an alternative and may not be used in conjunction with tracking. Further, the same transparency and consent modalities would need to be applied. Regarding the collection of consent, the collection of personal data for this purpose should be legitimized and the scope of the information provision should be clarified, mirroring the spirit of the GDPR but contextualized for sitatuions in which no personal data is processed. Lastly, the competence of the supervisory authorities should also be clarified with regard to the enforcement of infringements of the provisions pertaining to browser mining [95].

References:

[1] IAB Europe, 'IAB Europe European Programmatic Ad Spent Report 2018', IAB Europe (2019), https://iabeurope.eu/wp-content/uploads/2019/09/IAB-Europe_European-Programmatic-Ad-Spend-2018-Report_Sept-2019.pdf.

[2] ICO, 'Update report into adtech and real time bidding', ICO (2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf, p. 8-9 and footnote 4.

[3] See for example Lynskey, O., 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens', 36 European Law Review (2011); Zuiderveen Borgesius, F.J., Improving privacy protection in the area of behavioural advertising (PhD Thesis, UV Amsterdam, 2014); Clifford, D., 'EU Data Protection Law and Targeted Advertising – Consent and the Cookie Monster – Tracking the crumbs of online user behaviour', 5 Journal of Intellectual Property, Information Technology and E-Commerce Law (2014); Markou, C., 'Behavioural Advertising and the "New Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination', in S. Gutwirth, R. Leenes and P. de Hert (eds.), Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection (Springer, 2016). Also, Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 04/2012 of the Article 29 Working Party on Cookie Consent Exemption, 7.6.2012, WP 194; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224.

[4] See R.E. Leenes and E. Kosta, 'Taming the Cookie Monster with Dutch Law – A Tale of Regulatory Failure', 31 Computer Law and Security Review (2015); F.J. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 European Data Protection Law Review (2017).

[5] See ENISA, 'Cryptojacking – Cryptomining in the browser', ENISA (2017), https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser. The idea goes as far back as 2013/2014, with BitCoinPlus.com and the MIT-based project called 'Tidbit.' See Securitytrails, 'How much cryptocurrency can a web cryptominer actually mine?', SecurityTrails (2018), https://securitytrails.com/blog/how-much-cryptocurrency-can-a-cryptominer-actually-mine#a-little-on-the-history-of-browser-mining.

[6] S. Eskandari et al., 'A first look at browser-based Cryptojacking', IEEE Security & Privacy on the Blockchain (IEEE S&B) (2018), https://arxiv.org/abs/1803.02887; J. Rüth et al., 'Digging into Browser-based Crypto Mining', IMC '18: Internet Measurement Conference (2018), https://arxiv.org/abs/1808.00811; M. Musch et al., 'Thieves in the Browser: Web-based Cryptojacking in the Wild', Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19) (2019), https://doi.org/10.1145/3339252.3339261; M. Saad, A. Khormali and A. Mohaisen, 'End-to-End Analysis of In-Browser Cryptojacking', arVix (2018), https://arxiv.org/abs/1809.02152. R.K. Konoth, et al., 'Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense', Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018); A. Kharraz, et al., 'Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild', WWW '19: The World Wide Web Conference (2019), https://dl.acm.org/doi/10.1145/3308558.3313665.

[7] P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', arXiv (2018), https://arxiv.org/abs/1806.01994; S. Venskutonis, F. Hao and M. Collison, 'On legitimate mining of cryptocurrency in the browser – a feasibility study', arXiv (2018-2019), https://arxiv.org/abs/1812.04054.

[8] For instance, by P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', arXiv (2018), https://arxiv.org/abs/1806.01994.

[9] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive), [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (The Citizen's Rights Directive), [2009] OJ L 337/11.

[11] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

[12] Superior Court of New Jersey, Jeremy Rubin d.b.a. TIDBIT v. State of New Jersey Division of Consumer Affairs, 24 November 2014, available at https://www.eff.org › files › 2014.11.24_-_rubin_v._dca_opinion.pdf, p. 2.

[13] Ibid., p. 24.

[14] Ibid., p. 14–15.

[15] TorrentFreak, 'The Pirate Bay Website Runs a Cryptocurrency Miner (Updated)', TorrentFreak (2017), https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/; TorrentFreak, 'Pirate Bay is Mining Cryptocurrency Again But Forum Staff Aren't Worried', TorrentFreak (2018), https://torrentfreak.com/the-pirate-bay-is-mining-cryptocurrency-again-but-forum-staff-arent-worried-180702/.

[16] See, for instance, C. Williams, 'UK ICO, USCourts.gov... Thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned', The Register (2018), https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive/; C. Osborne, 'UK government websites, ICO hijacked by cryptocurrency mining malware', ZDNet (2018), https://www.zdnet.com/article/uk-government-websites-ico-hijacked-by-cryptocurrency-mining-malware/. M. Burgess, 'UK government websites were caught cryptomining. But it could have been a lot worse', Wired (2018), https://www.wired.co.uk/article/browsealoud-ico-texthelp-cryptomining-how-cryptomining-work.

[17] For a list of websites affected, see PublicWWW: https://publicwww.com/websites/browsealoud.com%2Fplus%2Fscripts%2Fba.js/.

[18] K. McCarthy, 'CBS's Showtime caught mining crypto-coins in viewers' web browsers', The Register (2017), https://www.theregister.co.uk/2017/09/25/showtime_bit_with_coinmining_script/.

[19] R. McMillan, 'Gaming Company Fined $1M for Turning Customers Into Secret Bitcoin Army', Wired (2013), https://www.wired.com/2013/11/e-sports/

[20] J. Segura, 'The state of malicious cryptomining', Malwarebyte Labs (2018), https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/; C. Cimpanu, 'Coinhive cryptojacking service to shut down in March 2019', ZDNet (2019), https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/.

[21] M. Musch et al., 'Thieves in the Browser: Web-based Cryptojacking in the Wild', Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19) (2019), https://doi.org/10.1145/3339252.3339261.

[22] S. Davidoff, 'Cryptojacking Meets IoT', LMG Security (2018), https://www.lmgsecurity.com/cryptojacking-meets-iot/.

[23] See for example A. Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Princeton University Press, 2016), ch. 2.

[24] Ibid.

[25] Ibid.

[26] See, for example, Zerocrypted, 'Honey Miner Mining Alternatives', Zerocrypted (2019), https://zerocrypted.com/honey-miner-mining-alternatives/.

[27] See, for example, D. Oberhaus, 'Seven Ways to Donate Your Computer's Unused Processing Power', Vice (2015), https://www.vice.com/en_us/article/bmj9jv/7-ways-to-donate-your-computers-unused-processing-power.

[28] For a description of Coinhive, see B. Krebs, 'Who and What Is Coinhive?', Krebs on Security (2018), https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/. At time of writing, the Coinhive website was not accessible, and Coinhive is defunct.

[29] T. Mursch, 'How to find cryptojacking malware', Bad Packets (2018), https://badpackets.net/how-to-find-cryptojacking-malware/.

[30] See the website of Crypto-loot, www.crypto-loot.org.

[31] J. Rüth et al., 'Digging into Browser-based Crypto Mining', IMC '18: Internet Measurement Conference (2018), https://arxiv.org/abs/1808.00811.

[32] C. Cimpanu, 'Coinhive cryptojacking service to shut down in March 2019', ZDNet (2019), https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/.

[33] See the GitHub repository for DeepMiner, https://github.com/deepwn/deepMiner.

[34] At time of writing, the Coinhive codebase was not available online anymore, and the Coinhive website is offline. An overview of the services can be found at https://99bitcoins.com/webmining-monetize-your-website-through-user-browsers/

[35] S. Dashevskyi et al., 'Dissecting Android Cryptocurrency Miners', arXiv (2019), arXiv:1905.02602v2.

[36] Crypto-loot, www.crypto-loot.org.

[37] R.K. Konoth, et al., 'Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense', Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018); A. Kharraz, et al., 'Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild', WWW '19: The World Wide Web Conference (2019), https://dl.acm.org/doi/10.1145/3308558.3313665.

[38] D. Sinegubko, 'Malicious Website Cryptominers from GitHub. Part 2.', Sucuri (2018), https://blog.sucuri.net/2018/01/malicious-cryptominers-from-github-part-2.html.

[39] See the website of Crypto-loot, www.crypto-loot.org.

[40] J. Segura, 'Persistent drive-by cryptomining coming to a browser near you', Malwarebyte Labs (2018), https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/.

[41] See Cryptojaxx, 'Does UNICEF Australia's use of web mining legitimise the activity?', Steemit (2018), https://steemit.com/cryptocurrency/@cryptojaxx/does-unicef-australia-s-use-of-web-mining-legitimises-the-activity; D. Roua, 'CPUforGood Wants To Free Slaves With Browser Mining', Steemit (2018), https://steemit.com/mining/@dragosroua/cpuforgood-wants-to-free-slaves-with-browser-mining.

[42] See Hijmans, H., The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU (University of Amsterdam and Vrije Universiteit Brussel, 2016).

[43] Lynskey, O., The Foundations of EU Data Protection Law (OUP, 2015), ch. 4.

[44] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (The Citizen's Rights Directive), [2009] OJ L 337/11. See also, E. Kosta, Consent in European Data Protection Law (Nijhoff, 2014), p. 293 et seq.

[45] Article 99 GDPR.

[46] Article 5(3) ePrivacy Directive. See E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Study for the European Commission DG Communications Networks, Content (2015) and the annexed tables to the study for a detailed analysis of the national divergence.

[47] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

[48] S. Stolton, 'Commission to present revamped ePrivacy proposal', EurActiv (2019), https://www.euractiv.com/section/data-protection/news/commission-to-present-revamped-eprivacy-proposal/.

[49] Article 2 GDPR sets out the material scope and Article 3 GDPR sets out the territorial scope.

[50] Case C-582/14 Partick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779.

[51] Recital 30 GDPR.

[52] Article 3 ePrivacy Directive. See for a detailed explanation E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Study for the European Commission DG Communications Networks, Content (2015), p. 24 et seq.

[53] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted 12 March 2019.

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

[55] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted 12 March 2019, para. 37 et seq.

[56] Ibid. See also C. Etteldorf, 'EDPB on the Interplay between the ePrivacy Directive and the GDPR', 2 European Data Protection Law Review (2019), p. 226–227 and the guidelines, opinions and judgements mentioned therein. Especially, Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:801.

[57] See Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224; Zuiderveen-Borgesius, F.J., 'Personal data processing for behavioural targeting: which legal basis?', 5 IDPL (2015); Case C-582/14 Partick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779.

[58] Article 5(b) GDPR read in conjunction with Article 6 GDPR.

[59] See among others, Berberich, M., & Steiner, M., 'Practitioner's Corner: Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?', 2 European Data Protection Law 3 (2016); Finck, M., 'Blockchains and Data Protection in the European Union', 4 European Data Protection Law Review 1 (2018); Finck, M., 'Blockchains and Data Protection in the European Union', MPI for Innovation and Competition Research Paper no. 18-01 (2018); Ramsay, S., 'The General Data Protection vs. The Blockchain: A legal study on the compatibility between blockchain technology and the GDPR', DiVA (2018); Schwerin, S., 'Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study', 1 The Journal of The British Blockchain Association 1 (2018); Blockchain Bundesverband, 'Blockchain, data protection, and the GDPR', Blockchain Bundesverband (2018); Kuner, C., et al., 'Blockchain versus data protection', 8 European Data Privacy Law 2 (2018). CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL (2018). EU Blockchain Observatory, 'Blockchain and the GDPR – a thematic report by the EU Blockchain Observatory', European Commission (2018), https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true.

[60] L. Edwards et al., 'Data subjects as data controllers: a Fashion(able) concept?', Internet Policy Review (2019); Finck, M., 'Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?', European Parliament Research Service, Study for the STOA Committee (2019).

[61] See CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL (2018), p. 3–4.

[62] N. van Saberhagen, 'CryptoNote v 2.0', CryptoNote (2013), https://cryptonote.org/whitepaper.pdf.
[63] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted 12 March 2019, para. 40.
[64] Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:801, para. 71.
[65] E. Kosta, Consent in European Data Protection Law (Nijhoff, 2014), p. 293 et seq.; E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Study for the European Commission DG Communications Networks, Content (2015), p. 12 et seq.
[66] Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224. E. Kosta, Consent in European Data Protection Law (Nijhoff, 2014), p. 264.
[67] Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:801, para. 69.
[68] Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:801, para. 70.
[69] E. Kosta, Consent in European Data Protection Law (Nijhoff, 2014), p. 294–296; E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Study for the European Commission DG Communications Networks, Content (2015), p. 51–51.
[70] Ibid.
[71] Ibid.
[72] Translation by author; emphasis added. Original: 'het verbod op cookiewalls ziet niet alleen op het plaatsen van cookies. Niet alleen cookies vallen onder deze beschrijving, maar ook daarmee vergelijkbare technieken waarvoor eveneens toestemming gevraagd moet worden. Dit zijn technieken zoals Javascripts, Flash cookies, HTML5-local storage en/of web beacons.' Autoriteit Persoonsgegevens, 'Cookies', Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies.
[73] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted 12 March 2019, para. 40.
[74] E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Study for the European Commission DG Communications Networks, Content (2015), p. 60.
[75] Ibid.
[76] See F. Zuiderveen Borgesius et al., 'An assessment of the Commission's Proposal on Privacy and Electronic Communications', Study for the LIBE Committee of the European Parliament (2017), p. 23-24.
[77] Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:801.
[78] F. Zuiderveen Borgesius et al., 'An assessment of the Commission's Proposal on Privacy and Electronic Communications', Study for the LIBE Committee of the European Parliament (2017), p. 25.
[79] P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', arXiv (2018), https://arxiv.org/abs/1806.01994.
[80] Ibid. S. Venskutonis, F. Hao and M. Collison, 'On legitimate mining of cryptocurrency in the browser – a feasibility study', arXiv (2018-2019), https://arxiv.org/abs/1812.04054.
[81] V. Marotta, K. Zhang and A. Acquisti, 'The Welfare Impact of Targeted Advertising', SSRN (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2951322.
[82] Ibid.
[83] P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', arXiv (2018), https://arxiv.org/abs/1806.01994.
[84] F. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 European Data Protection Law Review (2017).
[85] S. Venskutonis, F. Hao and M. Collison, 'On legitimate mining of cryptocurrency in the browser – a feasibility study', arXiv (2018-2019), https://arxiv.org/abs/1812.04054.
[85] Christopher F. Mondschein, 'Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12(1) and (7) GDPR', 2 European Data Protection Law Review (2016).
[86] R.E. Leenes and E. Kosta, 'Taming the Cookie Monster with Dutch Law – A Tale of Regulatory Failure', 31 Computer Law and Security Review (2015); F. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 European Data Protection Law Review (2017).
[87] E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Study for the European Commission DG Communications Networks, Content (2015), p. 61 et seq.
[88] M. Trevisan et al., '4 Years of EU Cookie Law: Results and Lessons Learned', Proceedings on Privacy Enhancing Technologies (2019); C. Santos, N. Bielova and C. Matte, 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', arXiv (2019), https://arxiv.org/abs/1912.07144, p. 46 et seq.
[89] Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:801; Opinion of Advocate General Szpunar in Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:246, para. 57 et seq.
[90] Opinion of Advocate General Szpunar in Case C-673/17 Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, EU:C:2019:246, para. 99.
[91] F. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 European Data Protection Law Review (2017).
[92] Ibid., p. 14.
[93] Ibid.
[94] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted 12 March 2019, para. 87–91.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
I would like to thank the anonymous reviewers.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(2)2020

Are Blockchain-based Systems the Future of Project Management? A Preliminary Exploration

Robin Renwick[1], Bryan Tierney[2]
[1]University College Cork, Ireland
[2]Boinnex Ltd., Ireland
Correspondence: rrenwick01@qub.ac.uk
Received: 13 January 2020 **Accepted:** 16 March 2020 **Published:** 13 April 2020

Abstract

Blockchain technologies have introduced a platform for a new wave of project management systems, providing managers with a range of characteristics, capabilities, and feature sets to aid their practice as they engage in increasingly complex processes and projects. This paper presents an explorative case-study in which open-ended interviews were conducted with practicing project managers. The interviews are analysed to understand currently deployed project management tools, technologies, and methods and to contextualise how blockchain-based systems may allow for improvements. Five constructs emerge: transparency, control, dynamic status updating, incentives, and trust. Feedback suggests blockchain-based alternatives could offer significantly better performance within each of these constructs, and thus should be explored as the technological backbone to the next generation of project management systems.

Keywords: *Blockchain; Distributed Ledger Technology; Project Management; Decentralised Applications; Project Management Software*

1. Introduction

The most notable instantiation of distributed ledger technology (DLT), otherwise known as blockchain technology, emerged in 2009 with the cryptocurrency Bitcoin [1]. The technology has since become a leader in innovation [2], widely recognised as defining an era using the combination of consensus mechanisms, applied cryptography, and database technology [3]. A decade since its origin, its impact is beginning to be felt across a wide range of fields: digital currency, supply chain management, digital identity, distributed computing, commodity and security tokenisation, and decentralised finance (DeFi) platforms, to name a few. Since the emergence of Bitcoin, one of the most impactful developments has been blockchain-based distributed application (Dapp) smart contract platforms, which allow the deployment of programmatically based business logic in a truthful, open, and transparent fashion [4, 5].

This paper frames concepts in the domain of project management, by understanding how it relates to key characteristics of blockchain technology. The study comprises a series of open-ended interviews with those currently engaged in the practice of project management. A mixed method of qualitative open, axial, and selective coding [6] uncovers constructs which correlate strongly with explicit characteristics of blockchain technology systems. These constructs are viewed as the rational base from which a relationship between project management and blockchain technology may evolve. The main contribution of this paper is the recognition that blockchain seems well suited to the demands of project management, positioning a proposed blockchain-based project management system as a viable solution for a series of stress points currently found within the practice.

2. Project management

Businesses are becoming more 'projectified' in the 21st century, as flexible and agile organisational structures are increasingly necessary for dynamic, technologically led markets [7]. Firms are understanding the significance of 'effective' project management, adopting rigorously structured methodologies into their operational practice in pursuit of operational efficiency and/or competitive advantage [8]. Project management combines several related domains: organisational studies, management science, psychology, governance methodology, politics, risk management, behavioural studies, information technology, and so on. Artto and Kujala [8] take a macro lens, detailing their business organisation framework (see Figure. 1) that places firms into one of four constructs, depending on the level of engagement with the project management process:

The framework provides a method of understanding how firms navigate the field. The matrix details a spectrum ranging from 'one firm > one project' organisations, to 'many firm > many project' networks. Firms are seen to be frequently adopting project-based methodologies into their daily operations.

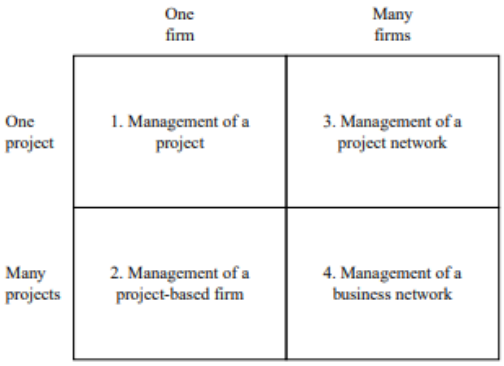


Figure 1. Framework for project business: Four distinct management areas

Unfortunately, the relationship between project management and the tools and technologies used within the practice is a somewhat neglected area of study. Many papers have discussed affordances and/or characteristics of

specific technologies in relation to project management processes [9, 10], but often in a deterministic manner – highlighting how things 'are' with respect to a predetermined set of tasks, functionalities, or characteristics.

3. Project management tools

Software, tools, technologies, and information management systems have quickly become an integral part of the project management process, either as a method for better organisation, more effective governance, to reduce risk, manage complexity, to ensure procedural compliance, and/or to increase rates of both project and project management 'success' [11, 12, 13].

Questions concerning 'success' have predominantly focussed on how to increase the rates of 'project success' or 'project management success'. Project success is a measure against the stated objectives of the project, while project management success is a measure against more traditional metrics such as resource allocation, cost, time, and quality [14]. A comprehensive study of 70 large, multi-national organisations found 12 factors crucial to project success: various elements of risk management and project length were crucial to 'on-time performance', while 'on-cost performance' was predominantly associated with the management of project scope [15].

A more recent study has highlighted various 'models' of project management success. Radujkovic et al. [16] provide an overarching framework, directing a lens towards project management tools and techniques and highlighting their importance through case-study-based analysis focussed on certain aspects of project management, seeking evidence of behaviours, functions, and characteristics. The authors conclude that it is imperative that organisations familiarise themselves with a wide range of tools and software programs, urging education and adoption in order for better 'planning, monitoring and control optimisation' [16]. The authors also urge continual learning and investment to aid the continual development and evolution of tools, technologies, software, and methodologies. Jugdev et al. [17] detail a comprehensive statistical-based study, building on prior work by Fortune et al. [18], mapping the interrelation between broad project management tools and software, and specific project management methodologies such as risk management and scheduling. The highest degree of correlation is found between project management tools and risk management methodologies, implying that benefits are found in those specifically focussed towards the management of risk [17].

Caniëls and Bakens [11] conducted surveys with 101 project managers to understand the impact tools had on 'multi-project environments'. They found that that Project Management Information Systems (PIMS) positively contribute to the ability of project managers to make effective decisions based on better organisational skills and accessibility of information – informing decisions and aiding workflows. An alternative study attempted to empirically assess the overall 'quality' of PIMS, completed through a survey-based methodology with 39 project managers. The study concluded that PIMS had a direct impact on project managers' success due to better organisation of information, project planning, scheduling, monitoring, and control [12].

Cicibas et al. [10] show a detailed comparison of 10 project management software tools, while a more recent study details project management technology specifically designed for software development projects [9]. The need for a comprehensive project management tools study is grave, especially considering the increasing complexity that project managers encounter in the modern age [19]. This requirement is detailed more specifically for small- and medium-sized enterprises (SME), viewed as resistant to adoption of specific project management software [13].

4. Blockchain-based smart contracts

Distributed application platforms have been designed, for the most part, to act as a distributed computing network onto which programmable code, otherwise known as smart contracts, may be deployed [20, 4]. While the first smart contract platform, Ethereum, did not appear until some five years after Bitcoin – the concept originated in the late 20th century [5]. The idea was focussed onto aspects of political governance, decentralised organisation, and distributed consensus models deployed through mathematical rulesets – ultimately in the pursuit of trustless systems divorced from the failings of the politicised agent [21]. Smart contracts may be described as self-enclosed deterministic logic, written as computer code, designed for execution on a predefined distributed application platform. The platforms are predominantly forms of distributed ledgers, in which there exists no single custodian of data or sole controller of the consensus ruleset. The main affordance of any contract executed on a distributed ledger platform is that it operates independent of any trusted entity. The contracts execute in trustless environments without the need for intermediaries to ensure the code is deployed correctly on behalf of the transacting parties [22]. This trust model ensures both parties are relatively certain that a contract will be executed, as agreed, once it has been initiated and logical conditions are met. Both parties may also be sure that an indelible record of all execution steps will be stored on a ledger that no one party controls and no one party can alter. This has meaningful ramifications for contract audibility, transparency, security, veracity, and efficacy [4].

5. Existing blockchain-based project management technologies

A potential realisation of a blockchain-based project planning and management solution emerged in mid-2018, with a project titled Zoom, which is marketed as a solution for developing and maintaining 'virtual organisations' comprised of geographically disparate members. The creators state their solution is a distinct method for organising remote workers around shared project goals, with blockchain technology being integral to contractual agreement, management, execution, as well as providing a platform for transparency of work flows and payments [23].

A second solution, Alehub, positions itself as a provider of a project management framework, designed to support contract execution, contract settlement, and organisation procedures and processes amongst parties coordinating in cooperative projects. The main focus of the company seems to be moving contract definition, execution, and settlement onto a custom-built smart contract-distributed ledger platform, using a custom value exchange token (ALE Token) to coordinate exchanges between transacting parties [24]. Alehub believes that doing so will ease a number of frictions currently found in the project management space: contract negotiation, settlement, and arbitration, as well as easing processes for short-term contract workers employed through digitally interfaced peer-to-peer labour markets like UpWork [25] or TaskRabbit [26].

Colony proposes a method of function (interacted through smart contracts) for organising and managing decentralised workforces [27]. The creators envision the protocol layer as providing various functionalities, such as the creation of tokens, managing reward mechanisms, and as a tool for reputation management. He attempts to apply this functionality to aspects of human organisation, affecting rules between people to help them organise better by aligning incentives around shared goals.

In a similar manner, Autark focusses on providing tools that 'empower agency and large-scale coordination' [28]. Their product suite includes an application that attempts to incorporate specific project management functionality onto existing GitHub [29]-based open-source project code repositories. Their portfolio of applications also includes a rewards mechanism module and a voting mechanism module. The functionalities address specific issues that arise within the project management process, and especially those that arise in decentralised organisations or inside projects that comprise of a number of remote members.

6. Existing studies based on the relationship between blockchain technology and project management

The application of blockchain technology to the project management sphere is in a nascent state, with most implementations emerging within the last five years – at the most. However, initial research has been conducted based on the applicability of blockchain technology to the industry, on the premise that specific characteristics of blockchain technology and/or smart contract functionality are applicable to the complex, multi-agent, and sometimes stratified management of projects in the industry. Turk and Klinc [30] propose that blockchain-based systems provide solutions to aspects of construction information management, as well as specific general-purpose information management infrastructure that other solutions, systems, tools, and technologies may be built onto.

Mason and Escott [31] also did research on the efficacy of blockchain technology in the construction industry, specifically in relation to the proposed use of smart contracts in the creation, management, and execution of construction contracts. A survey was conducted, with 117 responses from those working within the industry. The findings reveal a general adoption hesitancy, framed by a movement away from important human interaction. Automatically executed code, code immutability, and dispute resolution were all seen as factors to consider, while a reduction in the levels of human interaction was seen to be an 'unknown' quantifier, especially in an industry that relies on humanistic elements to ensure smooth contract execution, and/or the resolution of issues and disputes mid-contract. The authors note that human interactions are key to the construction industry, providing mechanisms for building relationships, detailing the generalised fear that technology may be detrimental to the benefits that accrue from forging humanistically based business relationships.

To address the paucity of research studies explicitly concerned with the relationship between blockchain technology and project management, this paper presents an explorative case-study focussed on exploring the symmetry (if one exists) between the field of project management and blockchain technology.

7. Methodology

This paper presents a qualitative analysis of a series of semi-structured interviews conducted with project managers currently engaged in the project management field. The managers have experience in a diverse range of industries: finance, software development, construction, research institutions, pharmaceuticals, etc. (see Table 1). Participants are drawn from a demographic range representative of the field, diversity in age, gender, geographic, and jurisdictional location. All participants have at least three years of practical project management experience, and all have certified project management qualifications through bodies such as the Project Management Institute (PMI), or an equivalent one. One participant requested to remain anonymous, and this request has been respected.

Table 1. Project manager profiles

Project manager interview profiles				
Participant	**Industry**	**Years experience**	**Location**	**Current workplace**
Participant 1.	Software development	>3	Ireland	Dell
Participant 2.	Multiple	>15	United States	SmartProjex
Participant 3.	Software development	>10	Holland	SAP Holland
Participant 4.	Pharmaceuticals	>5	Ireland	Johnson & Johnson
Participant 5.	Anonymous	>5	Anonymous	Anonymous

Interviews were conducted over a period of two months, beginning in February 2019 and completed in March 2019. The research may be seen as explorative, completed through a case-study approach [32]. The case-study approach is viewed as the most suitable, as the study explores a loosely bounded environment [33, 34, 35]. The number of participants is seen as providing an initial sample set from which general themes and constructs should emerge.

The focus of the study is narrowed to a series of questions surrounding practices, behaviours, and opinions of project managers with respect to existing software management tools and technologies. This elucidates areas where potential benefits of a tool built on, or deploying elements of, blockchain technology and/or smart contract functionality may exist. The data gathering and analysis process borrowed methodologies from grounded theory (GT). GT was developed in the 1960s by two sociologists as they proposed a system for 'theoretically grounded' qualitative analysis [36]. The study presented in this paper borrows from later refinements, especially the more pragmatic open, selective, and axial coding techniques used within the analysis methodology proposed by Corbin and Strauss [6]. This allows the theory to develop in a flexible manner, while still being informed by a hypothesis formed at the origin of the study [37].

8. Findings

The open-ended nature of the interview process ensured participants were free to talk about topics of importance, without conversations being unnaturally steered towards biased frames of reference. The interviews contained a number of key questions addressing general themes, but allowed scope for change and probing of any interesting avenues. Participants were encouraged to frame questions with their personal experience and context, while being aware that the interviews sought to understand how project management tools and technologies are used in practice; framing key constructs around the development of a new system or tool, and the functions and characteristics it would offer. They were not informed that the tool would be based on blockchain technology until the final section of the interview.

Below is a summary of participant responses, organised through the frames that emerged (see Table 2). There is a loose consensus on almost all of the constructs. Transparency is the only one in which there was some divergence of opinion, due to the nuanced nature of the construct. There is also some divergence on the nature of the proposed incentive systems with apprehension communicated with respect to how such a system may actually be deployed. There were also concerns raised with how performance might be measured. The following sections will detail some of the most pertinent sections of the interviews.

Table 2. Analysis of participant views

Analysis of participant views					
Proposition	**Participant 1**	**Participant 2**	**Participant 3**	**Participant 4**	**Participant 5**
Transparency	+	-	+	+	+
Control	+	*	*	+	+
Dynamic status updating	+	-	+	*	+
Incentive system	+	*	*	+	*
Trust	+	*	+	+	+
Key: Positive (+); Negative (-); Neutral (*)					

9. Transparency

Blockchain-based systems afford a substantial degree of information transparency. Understanding whether project management would benefit from a move towards more openness and transparency in processes, procedures, and reporting is a key question. The question was posed on whether incorporating a significant level of transparency would be beneficial. Participant responses were, for the most part, congruent. Some divergence surrounding reporting bias and reporting method did emerge.

All participants agreed that one of the main frictions found within their project management experience was lack of transparency – the appearance of information asymmetry, 'locked' data silos, and the ability for certain team members and/or stakeholders to maintain control on the levels of information sharing. A view was raised regarding the impact a transparent and open system would have on information accuracy – the ability for senior management to appraise impact of 'scope change'. Reporting could, in theory, accurately convey how decisions impacted the project, or how they might impact the project in the future.

Lack of transparency was found to be mitigated, presently, by more transparent project management tools, such as Trello [38]. A participant discussed how previously information asymmetry was a problem, as no central repository existed to ensure all project members were working from the 'same page'. Another participant, Participant 2, raised a concern regarding 'blame culture', noting how corporate ideologies may not be wholly congruent with open and transparent project management systems:

> Unless you are working in a culture that has encouraged people to come forward with problems, and has taken an approach that is very team oriented and not a culture that blames people with problems, I think what you are going to find is that people don't want management to know where things really stand. (Participant2)

This blame culture perspective can be compared with the response regarding transparency, and whether or not everything needs to be known by all members of a project. It was predominantly detailed that varying degrees of opacity (taking into account access rights, information security, and information privacy) would be beneficial, especially if transparency or openness was a core trait of a system (at the technical level) and the management (at an ideological level).

10. Control

There was loose agreement amongst participants that centralised control of data repositories was not desirable, leading to issues regarding data security, audibility of actions, and information asymmetry – distinct concerns when projects started to break down, or when dealing with sensitive or valuable information. The ability to maintain a record of changes, additions, deletions, along with a day-to-day tracking of issue evolution was seen as beneficial, guarding against lack of audibility when undesirable actions occurred.

Participant 1 noted how having a mutable information store allowed for perception to be skewed if information was deleted or hidden by somebody with the required authority or access control. This potential for information asymmetry was seen as a pitfall of data stores or repositories with centralised control. The concept of data 'snapshotting' was mentioned as a method for mitigating against this type of malicious action through the 'back-up' and restore processes. An instance of 'deletion' was discussed, highlighting the determined need for retrospective audibility of actions:

> I have seen it [issue deletion] to be pretty honest. I have seen user stories just disappear. … Ideally when a scrum team identify a defect, they would log it in Jira [a project management software], but imagine if the amount of defects just keeps increasing. So then there are serious questions about the type of quality standards you are following...and I have seen defects just [disappear] … they are gone. (Participant 1)

Control of information became a contentious issue for another participant (Participant 5), as they noted a project in which manual, hand-written information, or 'handover sheets', failed to record an objective version of events. Duplicate sheets would start appearing as it was beneficial for contractors to show a subjective version of events, as opposed to one 'handover sheet' recording the actual, objective, and order:

> Whoever has the handover sheet is allowed to work in the room, and you have to keep to a certain schedule, but that obviously never happened. … These duplicate sheets would start showing up, the room being handed over to somebody, when it wasn't handed over … that created an absolute nightmare. (Participant 5)

In one particular organisation, audibility is leveraged through consistent 'timesheeting', a process where actions and deliverables are reported manually on a weekly basis. However, it was unclear whether data repositories were backed up along with the reporting procedure. It was also communicated that the burden of meeting timesheeting targets placed abnormal stresses on projects, especially if they were complex or under resourced.

The discussion regarding audibility may also be framed as a conversation regarding information control. Centralised control of information and data repositories may be seen as a limiting factor, as concepts of ownership lead to tensions across departments or teams; information used as negotiation and bargaining tools with issues arising around retrospective auditing and/or measurement of process, performance, efficiency, and effectiveness. Information control was also viewed as a security issue, with Participant 5 noting that cloud-based servers were a distinct security concern for the company he worked in, especially regarding sensitive documents that would otherwise fall under the security model of non-disclosure agreements. The relationship between information control and information security is worth noting, as there seems to be a balancing act at play. Firms must consider whether they wish to allow open access of information to project members at times they require, or maintain strict access control that they can monitor and audit as and when required.

11. Dynamic status updating

There was loose convergence that dynamic and real-time updating of information is beneficial within project management. 'Dashboards' were mentioned by a number of participants – an effective way of communicating information to various stakeholders and/or project members. However, there was also an agreement that 'dashboard technology' coupled with collating and sharing of information procedures and processes are currently far from perfect. From the perspective of a project manager, the ability to create an easily understandable overview of the whole project is viewed as beneficial. However, there was some concern with giving everybody the same overview, or allowing all stakeholders unfettered access to all information pertaining to the status of a project. Information differentials were also a problem, as information elements may pertain to varied times – one information element may be up to date (e.g. timesheets) while another may lag behind by one or more time periods (e.g. financials), ensuring that the dashboards presented were not accurate or, even worse, skewed.

One participant worked in a firm described as 'project-orientated'. The firm used 'timesheets' so that stakeholders could obtain an overview of labour and resource costs at a regular and consistent time interval. This method is seen as beneficial, as it gave a consistent overview of the cost status of the project over a given time period. Of course, there is a week-long lag, given the time frames between each 'update'. In dynamic industries, or time

limited projects, a week might be seen as an inordinate amount of time, potentially problematic if a stakeholder needs to make a crucial decision based on the most up-to-date information possible.

12. Incentive system

The question of whether or not it would be beneficial having an incentive system built as a feature of a project management tool was posed to the participants. There was a degree of perspective divergence around this issue. In theory, a value exchange token could be used as the monetary exchange mechanism to incentivise both individual performances (i.e. a token distributed when one individual completes work in an efficient or efficable manner), and also as a tool for contract compensation (i.e. when work is completed, tokens are exchanged). A smart contract platform offers the potential to deploy both mechanisms, as they may be programmed at contract initiation to serve whatever purpose is necessary for the specific work package. In this manner, parties can be confident that contract execution remains deterministic, even given external pressures.

One participant communicated how a previous firm, with which he worked, employed an incentive system – a psychological reward mechanism for completion of tasks. In the firm, a bell was used – rung after a certain stage of the project was completed successfully. The bell became a positive reinforcement tool that members began to work towards – a recognition that the project was moving forward or towards its desired end goal:

> We used to implement this … following scrum [a method within 'agile' project management]. A scrum, it's basically a two week sprint … we had this very simple thing, it was a bell. So any time someone would complete a user story assigned to them they were given that bell to actually ring. This really encouraged people to get things done on time. There was some gratification involved. The incentive became that you get to ring the bell. [It created a mood] Everything was flowing. (Participant 1)

There was also mention of a direct incentive system where project managers were given 'points', which they could distribute – rewarding project members as they see fit. These points could then later be traded in for real-value items on a specific website:

> Project managers were given 75 points per quarter, per resource. We used to call it celebrating performance points … anything interesting that happened, so for example if someone did something beyond their call of duty … we could award that … it was not transparent. There might be cases where the project manager might give it to his favourite. So to overcome that, there was an audit system. It would do these random samples – who has been given the points, how much … but this really helped a lot. It was an immediate gratification system. (Participant1)

Participant 2 made a distinction between compensation and incentivisation, detailing how a token-based system could aid in the deployment of transparent and open compensation contracts based on deliverables, that is, pay to project members once a stage is satisfactorily completed. These deliverables would be set out during contract initiation, and agreed by all parties. This distinction is crucial, as tokens may be used for both purposes. Other participants could see the theoretical value of a native incentive system, but concerns were raised regarding transparency and audibility, questioning whether such a system would remain objective once distribution is centralised, in the control of a manager who may be influenced by explicit or implicit biases.

13. Trust

A concept that repeatedly arose in all interviews was trust. Participants converged around the perspective that leveraged trust helped build better relationships between project members and stakeholders. Trust is seen as a bind that affects varying aspects of both 'project success' and 'project management success'. Participants viewed technology as potentially affording an increase in levels of trust, aiding aspects such as transparency, traceability, audibility, verifiability, robustness, and openness, while also providing the technological platform on which a community may be built – either through communication, incentive systems, or common processes and procedures amongst all members of the project team, and management.

Participant 1 mentioned trust with respect to the centralised ownership of data, detailing how changes of project scope may be mitigated against if an immutable record of initial scope was documented at project initiation, as well as any agreed changes being noted within some form of read-only, access-controlled format:

> I think that [immutable storage] would really help us … in terms of trust to be honest. … Initially you have this set of requirements … apparently it is frozen in a sense that everyone signs off and agrees … but it is not really frozen. … If you have a system that says, ok, these are the set of requirements and now it is frozen and no one can make the changes to scope unilaterally, that's pretty interesting, yeah. (Participant 1)

Participant 3 discussed ownership of data, noting how relationships may not always be trusting. A system that was conducive to more trustful engagements, especially the surrounding information, was seen as beneficial. The interviewee highlighted that mutable results such as timesheeting or documenting could become points of friction in relationships. Trusted documentation is important, so that issues in relationships can be traced to their origin, or highlighted to all parties in a common 'language' when necessary.

The link between increased transparency, openness, and trust is echoed by another participant, as they described the relationship between project management and output quality. Managing expectations and scope was discussed with a system that allowed for clear and transparent communication of some form of 'immutable project charter' which was viewed as beneficial. Anything that could help manage shifting expectations in a clear and transparent fashion is something that could aid project smoothness and help mitigate against tensions that arise in the project as it develops.

14. Discussion

The study presented attempts to ascertain if a symmetry exists between project management practices and certain characteristics of blockchain technology. A series of interviews are conducted from which five constructs emerge: transparency, control, dynamic status updating, incentives, and trust. The constructs are seen as higher-level frames through which a thorough analysis of the relationship between blockchain technology and project management software may be detailed in future studies. It is viewed that each construct is an area in which a system built on blockchain technology might improve the status quo, especially from the context of a purpose-built project management tool whose underpinnings seek to leverage specific characteristics of the technology. The article details convergence of perspective from five practicing project managers; characteristics of blockchain technology would be beneficial to their work, especially if these characteristics were built as features of a specific project management system. If certain characteristics of existing tools can be combined with some of the robust, secure, decentralised, smart contract execution aspects of blockchain-based systems, there is reason to believe that significant improvements might be made.

The core limitation of this study is that only five project managers were canvassed for opinions. This limited the sample size and affected the

veracity of the coded constructs. While this is acknowledged as being a considerable weakness, it is felt that for an explorative investigation, the insights and overarching frames remain valid – especially in the context of directing further research. Future studies might explore how existing blockchain-based systems might explicitly affect, enhance, or leverage existing project management methodologies and/or processes. This would allow evidence-based feedback to be iteratively provided to developers of such systems, informed by real-world use, providing a template for the future development of blockchain-based project management systems.

References:

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" [Online] Accessed: 3rd January, 2018. [Online] Available: https://bitcoin.org/bitcoin.pdf

[2] S. Underwood, "Blockchain beyond bitcoin". Communications of the ACM, (59:11), pp. 15-17, 2015

[3] A. Narayanan, & J.Clark, "Bitcoin's academic pedigree". Communications of the ACM, 60(12), 36-45, 2017.

[4] V. Buterin, "A next-generation smart contract and decentralized application platform". White paper [Online]. 2018. Accessed 2nd March 2018. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_ decentralized_application_platform-vitalik-buterin.pdf

[5] N, Szabo. "Smart contracts: building blocks for digital markets". EXTROPY: The Journal of Transhumanist Thought, (16), 18, 1996.

[6] J. M. Corbin & A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria", Qualitative Sociology, (13:1), pp. 3-21, 1990.

[7] R. A, Lundin, N. Arvidsson, T. Brady, E. Ekstedt and C. Midler, "Managing and working in project society". Cambridge University Press, 2015.

[8] K. Artto and J. Kujala, "Project business as a research field". International Journal of Managing Projects in Business, 1(4), 469-497, 2008.

[9] H. A, Bilal, S. Amjad and M. Ilyas, "A Comparative Study of Global Software Development Tools Supporting Project Management Activities". International Journal of Education and Management Engineering, (6) 32-39, 2017.

[10] H. Cicibas, O. Unal and K. A, Demir, "A Comparison of Project Management Software Tools (PMST)", Software Engineering Research and Practice, pp. 560-565, July, 2010.

[11] M. C. Caniëls and R. J. Bakens, "The effects of Project Management Information Systems on decision making in a multi project environment", International Journal of Project Management, 30(2), 162-175, 2012.

[12] L. Raymond and F. Bergeron, "Project management information systems: An empirical study of their impact on project managers and project success", International Journal of Project Management, 26(2), 213-220, 2008.

[13] L. Teixeira, A. R Xambre, J. Figueiredo and H. Alvelos, "Analysis and Design of a Project Management Information System: practical case in a consulting company", Procedia Computer Science, 100, 171-178, 2016.

[14] A. De Wit, "Measurement of project success", International Journal of Project Management, 6(3), 164-170, 1988.

[15] T. Cooke-Davies, "The 'real' success factors on projects", International Journal of Project Management, 20(3), 185-190, 2002.

[16] M. Radujković and M. Sjekavica, "Project Management Success Factors". Procedia Engineering, 196, 607-615, 2017

[17] K. Jugdev, D. Perkins, J. Fortune, D.White and D. Walker, "An exploratory study of project success with tools, software and methods", International Journal of Managing Projects in Business, 6(3), 534-551, 2013.

[18] J. Fortune, D. White, K. Jugdev and D. Walker, "Looking again at current practice in project management", International Journal of Managing Projects in Business, Vol. 4 No. 4, pp. 553-572, 2011.

[19] A. Jaafari and K. Manivong, "Towards a smart project management information system", International Journal of Project Management, 16(4), 249-265, 1998.

[20] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, and S. Zanella-Béguelin, "Formal verification of smart contracts". In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security (pp. 91-96). ACM. October, 2016.

[21] M. Atzori, "Blockchain Technology and Decentralised Governance: Is the State Still Necessary?", Journal of Governance and Regulation, vol. 6, no. 1, 2017.

[22] K. Christidis, and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things", IEEE Access, 4, 2292-2303, 2016.

[23] Zoom Website. Accessed on 20th January, 2019. Available: https://zoom-tech-beta.firebaseapp.com/, 2019.

[24] Alehub, Company whitepaper, [Online] Accessed on 22nd March 2019. Available at: https://alehub.io/ ALEHUB_WP_eng.pdf. [Online], 2019.

[25] UpWork Website [Online], Accessed: 3rd February 2019, Available: https://www.upwork.com/, [Online], 2019.

[26] TaskRabbit Website [Online]Accesed: 3rd February 2019, Available: https://www.taskrabbit.com/, [Online], 2019.

[27] Colony, Company whitepaper, [Online] Accessed on 27nd February 2019. Available: https://colony.io/whitepaper.pdf, [Online], 2019.

[28] Autark Website [Online]. Accessed 20th February, 2019. Available: https://www.autark.xyz/, [Online], 2019.

[29] GitHub Website [Online], Accessed on 3rd March 2019, Available: https://github.com [Online], 2019.

[30] Ž, Turk and R. Klinc, "Potentials of blockchain technology for construction management", Procedia Engineering, 196, 638-645, 2017.

[31] J. Mason and H. Escott, "Smart contracts in construction: Views and perceptions of stakeholders", Proceedings of FIG Conference, Istanbul, May 2018.

[32] K. M. Eisenhardt, "Agency theory: An assessment and review". Academy of Management Review, (14:1), pp. 57-74, 1989.

[33] J. R. Feagin, A. M Orum and G. Sjoberg G, "A case for the case study", UNC Press Books, 1991.

[34] K. B. M Noor, "Case study: A strategic research methodology", American Journal of Applied Sciences, 5(11), 1602-1604, 2008.

[35] R. K. Yin, "Case study research and applications: Design and methods", Sage publications, 2017.

[36] B. G. Glaser and A. L Strauss, "Discovery of Grounded Theory: Strategies for Qualitative Research". Routledge, 1967.

[37] R. Matavire and I. Brown, "Profiling grounded theory approaches in information systems research", European Journal of Information Systems, (22:1), pp. 119-129, 2013.

[38] Trello Website [Online]. Accessed: 3rd April 2019, Available: https://trello.com/en-GB. [Online], 2019.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Robin Renwick, is main author and was responsible for writing the manuscript, collecting data, and proof reading.

Funding:
The research was partly funded by an Innovation Voucher awarded through Enterprise Ireland (IV-2018-3068) to Boinnex Ltd. and University College Cork, Ireland.

Acknowledgements:
The authors would like to thank Enterprise Ireland, University College Cork, the JBBA, and all the participants that contributed to the study.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(7)2020

Academic Certification using Blockchain: Permissioned versus Permissionless Solutions

Carlos Castro-Iragorri[1] and Olga Giraldo[2]
[1]Universidad del Rosario, Colombia
[2]Vrije Universiteit Amsterdam, The Netherlands
Correspondence: carlos.castro@urosario.edu.co
Received: 03 June 2020 **Accepted:** 15 June 2020 **Published:** 02 July 2020

Abstract

Understanding the challenges of implementing blockchain solutions is an important step towards scaling and adopting the technology. This paper analyses the adoption of blockchain technology in the management of academic certificates. In this use case, we identify certification providers that have adopted a permissionless approach and consortiums of academic institutions that are in the process of building permissioned networks. We explore the challenges faced by both approaches, and obtain information from competing projects to provide a preliminary approach for cost-benefit analysis that could potentially be applied for similar blockchain projects. For the management of academic certificates, we find that beyond the cost of implementing the technology there are additional elements of critical importance for adoption. For example, if blockchain-enabled certificates will replace notarised documents, how does the technology complement other forms of digital credentials, the ease of integration to existing administrative records within institutions and whether they are a viable first step towards a comprehensive, efficient and reliable system to share information among institutions.

Keywords: *permissioned, permissionless, digital credentials, cost-benefit analysis Software*

Keywords: *M210, O300.*

1. Introduction

Although distributed ledger technology (DLT), in particular blockchain, has captured an important amount of attention in the last decade, it is challenging to identify the added value of the technology to some of the solutions proposed. Expectations and investment are still high in firms and governments [1]. However, there is not enough information regarding investments and outcomes on existing projects. Also, IT projects are risky endeavours with overrun cost [2].

Within the context of DLT, decentralisation provides high censorship and tamper resistance, but these features come at higher costs in terms of the use of resources, processing time and coordination efforts compared to a fully centralised system [3]. Some analyst indicates, that the high cost of managing the information contained in a public permissionless blockchain, such as Bitcoin or Ethereum, compared to hosting the same information on a centralised database, is only economically rational if users have strong preferences towards censorship resistances, and are willing to pay the premium [4].

More recently, permissioned blockchains have attracted the attention of traditional firms looking to incorporate the benefits of DLT and customise these solutions to the need of their industries [1]. As there is a more general understanding of the benefits of the technology in each industry, firms are interested in solving the permissioned versus permissionless dilemma. One simple way to understand the dilemma is to think of permissionless blockchain as an existing infrastructure of highways that a firm uses to provide goods and services. Therefore, a firm that wants to jump into this ecosystem must invest in connecting to the highway and pay the toll required to use and maintain the existing infrastructure. It must also, abide by the rules (speed limits) and possible externalities (congestion) of using the infrastructure. On the other hand, for a permissioned solution, there is no existing infrastructure; therefore, the interested firms must incur the fixed cost of building the roads that will allow them to provide their goods and services. To reduce the individual contributions and diversify the risk, firms form a consortium and create a governance structure in charge of initially building the infrastructure, and later on, managing and settling disputes. This consortium agglomerates firms with similar interest, therefore, it is possible to have a more efficient and customised infrastructure that will meet the needs of the firms to deploy their solutions.

The objective of this article is to analyse the use case for the management of academic certificates using blockchain technology. We address the added value of using blockchain technology and ascertain the similarities and challenges between providing such services using a permissioned and a permissionless approach. In addition, we provide an example of cost-benefit analysis.

The document is organised as follows: section 2 introduces the use case in the context of the education sector; section 3 explains the role of blockchain technologies in the certificate management operating processes; section 4 provides a cost-benefit analysis applied to the case and section 5 concludes.

2. Managing Academic Certificates

Certificates are a social convention that provides a medium to convey new information regarding an individual or an organisation. In education, the most common form of certificates is that which provides new information regarding accomplishments and skills. The information regarding skills is relevant for employers and to continue the acquisition of knowledge.

According to research by the European Union [6] academic certificates are one of the areas in education where we could see the implementation of blockchain technologies in the short term. Further down the road this would also include transfer credit systems and lifelong learning records [7].

As considered in [6] the ontology of a certificate can be broken down into its components and its related processes. The components are as follows: a claim, the evidence, a signature, a document, an issuer and a recipient. The processes are as follows: design, issuing, verification and sharing or socialising.

So far the traditional method to provide a certificate has been paper. Paper certificates have the following characteristics: they include physical security measures (watermarks, seals) to avoid forgery; the issuer and recipient guard independent copies; they cannot be revoked and they require a manual verification. More recently, institutions have introduced different standards for digital certificates with some form of delegated signature verification. The claim and evidence information are kept in centralised databases hosted by the institution. Since the certificates are controlled by the issuer institution they can be revoked.

What is the added value of blockchain technology? According to [6], the traceability of the issuing process and the multiple copies provide stronger security features. The verification process is independent from the issuer; therefore, the service can be performed by any institution with access to a persistent registry, allowing for vendor independence. Both the issuer and the recipient obtain different levels of control over the certificate. The issuer may revoke the claim without incurring in additional cost, for example, obsolete skills or technologies. The recipient will control, collect and socialise its verifiable skills in a more efficient manner. Avoiding the need to solicit his learning record and possibly pay additional fees to update his resume.

The benefits for the recipient are complemented by self-sovereign identity. With self-sovereign identity individuals own and control their digital identity without the intervention of third parties In this context, an academic certificate or any other type of certificate is considered as a claim, associated and owned by an individual or organisation, that represents sets of information that are relevant to establish business or personal relationships.

Today, educational attainment is largely a decentralised activity because; students and professionals obtain a wide range of skills in different periods of their working life and at different types of institutions (universities, employers, online learning platforms, among others). However, the current challenge is that each institution is an independent silo of the academic accomplishments of a student. Hence the transit of one institution to another, or between employers requires a student to provide verifiable copies of their academic achievements and new skills. These pain points and inefficiencies justify improving the existing process.[1]

To avoid the current equilibrium of independent silos, blockchain technology provides the decentralised infrastructure to safely share abstractions of the information related to the educational accomplishments of a student. Most of the current implementations, register onto a blockchain hash obtained from the information contained in the certificate; this is what we denote as an abstraction. Blockcerts extends existing digital standards in education, in particular Open Badges, to incorporate a blockchain-based verification process .

Currently, projects that have implemented a solution or advanced proof of concepts for academic certificate management can be categorised into certification vendors and university consortiums. Certification vendors are firms or start-ups that have seen the potential of blockchain technology for data management, self-sovereign identity or know your customer (KYC), creating a business model around it. Other firms have included blockchain technology as part of their existing portfolio of services. In the former, the firms act as a notary (a third party between the issuer and the recipient or a recipient and employer). Some of these vendors are Accredible[2], Xertify[3] and Gradbase[4].

Universities have not lagged; the Blockcerts standard was initially developed by the MIT Media Lab and Learning Machine[5]. As of 2018, the Digital Credential Consortium is a university lead effort to design and build an infrastructure for digital credentials of academic achievement. The consortium founders are universities in Europe, North America and Latin America. Similar consortiums have been created in Singapore[6] and Spain,[7] with an increasing number of universities joining the effort. In addition, individual universities like the Open University UK and the University of Nicosia [6] were early adopters of the technology, using permissioned blockchains and the Blockcerts standard or similar types of digital badges standards.

Universities, as the main issuer of these types of certificates, have computer science departments, in-house IT personnel and the possibility to establish partnerships or fund start-ups to develop the technology. Besides, they might be reluctant to share academic information with external vendors unless they are unable to provide the service or incorporate blockchain technologies. For this reason, the most important clients of certification vendors are online education, professional associations and companies. This attitude will be a challenge going forward: to overcome the shortcomings of the current system of academic credentials, it would be desirable to allow the integration of solutions and achieve lifelong learning records. Otherwise, we might end up with the latest technology, but we will not be able to overcome the current independent silos equilibrium.

3. Blockchain Infrastructure for Managing Academic Certificates

A system for managing academic certificates can be broken down to the processes mentioned previously: design, issuing, verification and sharing or socialising. We need to understand how these operating processes are related to the services that will be impacted by the introduction of blockchain technology.

Figure 1, represents the operating processes in stages, and identifies the processes transformed by blockchain technologies.

The academic certificates (claim and evidence) are part of the administrative records stored in databases on-premise or in the cloud by issuer institutions. With or without blockchain this information is held within the institution. Data protection requirements such as General Data Protection Regulation (GDPR) require education providers to be accountable for the information of students.

The first stage of figure 1, represents the design and storage of the information contained in the certificate. In the traditional approach, the university or education provider will also be in charge of providing a system to share and verify the information contained on the paper or digital certificate. In other words, the process is entirely integrated and managed by the issuer institution.

The second and third stages of figure 1 represent the process affected by blockchain technologies, in particular, how information is shared and verified.

The system storing the information on the accomplishments of the students needs to be able to interact with a blockchain for issuance and verification. As we mentioned before, the added value of blockchain technologies for this use case is primarily concerned with the introduction of a decentralised verification system for the academic certificates. This system must also provide enough trust to avoid any further use of notary service.

When a student satisfies the requirements regarding a skill or a degree, a certificate is issued and the abstraction of the metadata contained in the certificate is registered on the blockchain. The recipient can share any digital form of the certificate and the certification vendor or the

university consortium will provide a universal verifier that will be capable of declaring the veracity of the information contained in the certificate. In both cases, issuance and verification against the blockchain are performed using applications that interact with some distributed ledger.

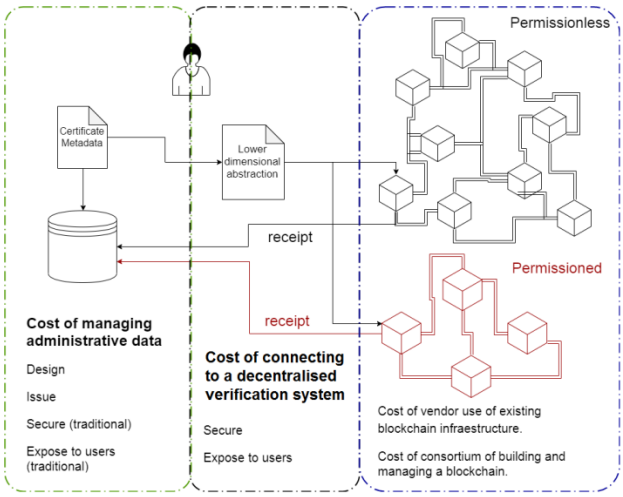


Figure 1: Management of academic certificates using Blockchain technologies.

In the third stage of figure 1, we see that the ledger can exist in a public, permissionless blockchain or a permissioned blockchain exclusively built by the consortium. To register the information contained in the certificate using a permissionless blockchain, the certification vendor is subject to the cost and rules of using this public infrastructure. For example, the use of a cryptocurrency that is a fundamental element in the incentive system that guarantees the verification and creation of new blocks. On the other hand, the consortium must build and operate the first nodes in the network, provide assistance and training for the introduction of new nodes, set up a governance structure and maintain and update the scaling infrastructure.

The cost comparisons between the permissionless and the permissioned solution are based on the high variable cost/low fixed cost of the former and high fixed cost/low variable cost of the latter. Estimates from [8] indicate that permissioned blockchain projects have fixed costs that are ten times higher than their permissionless counterparts. However, they also show that, with the current consensus mechanisms of permissionless blockchain, the average variable cost per transaction is five times higher than for permissioned blockchain. In other words, the current consensus mechanism for permissionless blockchain is well suited for a small or moderate number of transactions (less than 500k per year), but for a high transaction volume, a private blockchain is the better solution.

4. Cost-benefits Analysis for Managing Academic Certificates

Blockchain technologies provide opportunities for new business and service models or improve an existing processes. We focus on the latter and provide a first approach to cost-benefit analysis for managing academic certificates at universities. There are few documented cases of cost-benefit analysis applied to blockchain technologies, some of these look at permissionless blockchain [4], permissioned blockchain [9], compare both approaches [8] or look at specific use cases like supply-chain finance [10].

To estimate the certification needs of an institution, we use data on issued certificates and graduating student population over a school year. Universidad del Rosario is a private university in Colombia with 12,100 students. That is considered a medium-size university according to US standards[8]. Extension schools and continuing education are also important in most universities; at Universidad del Rosario this adds 15,130 participants in programmes that also receive certificates. During the school year, 3,893 students graduated from the different degree-granting programmes. Also the universities' registrar's office issued a total of 3,383 certificates of different types. This gives a rough estimate of at least 22,406 certificates issued during the school year, including graduating students, participation certificates for continuing education and various additional types of certificates.

Universities looking into blockchain technologies are mainly interested in providing a better and more secure information services regarding the skills and accomplishment of their alumni and student population. In addition, they are interested in improving the existing process and any possible cost avoidance and savings. Most universities already offer e-transcripts and digital certificates to students and alumni; the cost varies since it can be a free service or have a fee from 3 to 10 USD. Since this is a digital timestamped object, the recipient can use it as proof of his accomplishments to as many solicitors (e.g. prospective employers) as required, so there is no scaling cost. The prices of a paper certificate is usually twice that of digital certificates (15 – 25 USD), and if they are notarised documents, the price will go up to 50 USD. These costs are obtained from Stanford University[9], MIT[10] and Universidad del Rosario, Colombia[11]. Paper documents do not scale, so the cost to the recipient would increase depending on the number of solicitors.

Blockchain-enabled certificates are digital objects that provide decentralised verification, and the benefits for the recipient are that they are readily available and with the additional security measures they could be legally considered as notarised documents. They would be readily available because the information they provide would be submitted to the network at the moment of initial issuance and the recipient or solicitor could obtain that information directly at no additional effort or cost. Ideally, there would be no need to incur the cost of re-issuance or notary services.

For universities, the direct benefits are efficiency gains due to streamlined documentation and labour cost reduction for issuance, resolution of conflicting records and verification. An indirect benefit is the reduced exposure to fraud; however, it is difficult to quantify this benefit. To quantify the direct benefits, we obtain information from the registrar's office regarding expenses related to the management of academic certificates: physical and digital cost of issuance, labour cost associated with document processing, resolution of conflicting records and/or manual verification. Concerning cost, we will only consider the adoption of blockchain technologies for the decentralised verification process. As we mentioned in the previous section, individual institutions are required to maintain governance and oversight on the administrative records of their students and alumni. Our main assumption is that universities may choose to adopt a system of decentralised verification using a certification provider that uses a permissionless/public blockchain infrastructure, or by joining a consortium of institutions that are using a permissioned/private blockchain.

The current business model of certification providers is to charge the issuers for the service.[12] Certification vendors offer different packages for universities depending on the number of certificates or unique recipients per year. Naturally, the cost to issuers will decrease with the number of certificates. In table 1, we provide an estimate of the yearly cost of using a certification vendor based on a demand of 22,000 certificates per year.

It is important to note that for some of these providers blockchain technologies are only part of their portfolio of services, so it is difficult to make an exact comparison of the service provided; however, they do provide a measure of the cost faced by institutions (issuers).

Certification vendors are using the Bitcoin or the Ethereum public network as a method to notarise the certificates, so it is interesting to determine the cost of using this infrastructure. Blockcerts provide a set of applications and the documentation to implement the verification of digital certificates

using permissionless blockchains. To make an efficient use of the network, it is recommended to batch many certificates onto one transaction on the blockchain registry. Certification providers follow and convey this recommendation to their clients to reduce the cost of using the network.

Table 1: Cost per year for issuing organizations of using certification providers.

	Accredible	Xertify
# certificates / recipients		
basic	<10,000	<10,000
advanced	>10,000	unlimited
Price USD		
basic	$ 1.04	$ 0.90
advanced	$ 0.96	15% commission
Yearly cost USD	$ 21,120	$ 19,800

In the Ethereum network, the transaction fee in Ether is composed of two elements – the gas limit and the gas price. The gas limit guarantees that there are sufficient resources to process the transaction in the registry by the network and the amount necessary depends on the complexity with a recommended floor of 21,000. Gas price represents the reward for processing the transactions; therefore, lower values will require more time to get the transaction processed. Both values are affected by the network activity, meaning that when there is congestion on this public infrastructure (e.g. when there is an attractive initial coin offering, ICO) both the gas limit and price will need to increase.

Using the reference gas limit and price mentioned for the implementation of Blockcerts, we find that the yearly cost of issuing 22,000 certificates in batches of 200 certificates (that is 110 transactions per year) is around $25 USD (Table 2).[13] On the other hand, if it takes one transaction to issue each certificate the total cost of issuing the 22,000 certificates would be $5,011 USD. The price considers the average price of Ether during 2018 when the cryptocurrency was quite volatile; using data for 2019 the price is approximately $10 USD for batched certificates and $1,965 USD for the individual certificate issuance.

Table 2: Cost of using the Ethereum network for registering 22,000 academic certificates per year.

Gas Limit	25,000
Gas price in GWei	20
Transaction Fee (ETH)	0.0005
ETH-USD (avg) 2018	$ 456
ETH-USD (avg) 2019	$ 179
Transaction Fee (USD) 2018	$ 0.23
Transaction Fee (USD) 2019	$ 0.09
# transactions for 200 certificates	110
Price for batched certificates	$ 25
Price for individual certificates	$ 5,011

The estimated cost of using the Ethereum network to register groups of certificates is very small compared to the cost submitting transactions for individual certificates. The verification process is not affected by grouping the certificates and hence provides an efficient use of the network at minimal cost. Using a Merkle tree of certificate hashes provides a tractable and reliable approach to batch certificates and reduces cost. Overall, the cost associated with using the permissionless blockchain infrastructure does not seem to represent a significant factor that will affect adoption because the transactions are simple and hence the computational burden on the network is small.

For the decentralised issuance and verification of certificates, vendors must develop applications that can interact with the existing information systems within the institutions to register the abstraction of the certificate onto the blockchain and to query the metadata needed to reproduce and verify the contents of an existing certificate. Information for budgeting blockchain projects is rare; several web pages give rough estimates of blockchain development cost including the developers and infrastructure.[14] The estimates depend on the complexity of the project and are in the range of 15k – 200k USD. In the interviews conducted with the certification vendors with less than 5 years with a product in the market, the project had an overall investment of 60k, a team of two developers with an additional staff of three persons in charge of the commercial strategy and were using cloud infrastructure. Some of these providers were start-ups with several modifications on the product they offer or their commercial strategy and some are still determining whether they will focus exclusively on blockchain technologies or just have it as part of their portfolio for digital certificates.

Consortium-led projects have been created mainly by universities with the collaboration of IT companies. This is the case of Fundación Universitaria San Pablo CEU and Ibermatica in Spain. They started building a permissioned blockchain for the management of academic certificates using Hyperledger Fabric. Since it is a permissioned network, there is no existing infrastructure, so members need to assume the fixed cost to build the network, the applications, and deploy the first nodes in the network. Currently, they are working on two permissioned networks ChainTalent and Red BLUE for Spanish universities. The costs are assumed by the initial members of the consortium and a fee is charged on incoming members. ChainTalent is the more mature of the projects since it has been in development since 2018 and currently has four nodes operating in the network. The main components of the application were developed over a period of four months with a team of two developers and a project lead. The overall investment in the project up to the end of 2019 has been approximately 80k USD. The consortium has established a yearly membership fee of 5,000 EUR (5,600 USD) which provides an unlimited number of certifications to be issued by universities, their main clients. There are additional fees regarding installation of the node, integration to the institution's information systems and maintenance. An exact value for the additional fees depends on the client, but overall the additional fees do not exceed the yearly membership fee.

Similar to the services provided by the certification vendors, consortiums provide applications such as a universal verifier and the possibility for students and alumni to share the certificate information with solicitors using social media.

Using the information regarding cost avoidance and efficiency gains at Universidad del Rosario, we quantify the benefits of adopting a decentralised verification process based on blockchain and compare the cost of adopting the technology using a certification provider or joining a university consortium.

Table 3 summarizes the results of the cost-benefit analysis. In the top part, we estimate the cost of processing the certificates during a year. This cost includes both labour cost and any additional cost for physical or digital certificates. On average, the cost of producing a certificate is $1.6, but this can vary for more complex degree certificates ($5.4) to simpler certificates of continuing education ($0.1). We use very conservative estimates in terms of the reduction of cost (25%) given that the largest savings were already obtained from digitisation. This is important because the immediate benefits of blockchain projects for document processing are sometimes related to the redesign of the process and the digitisation; hence, a common criticism is that these benefits are not related to the use of decentralised verification services [9]. Also, we include the cost avoidance of dealing with conflicting records and any non-automated process related to verification. We estimate the annual benefit regarding conflicting records and automated decentralised verification of around $2,200.

Table 3: Cost-benefit analysis for universities adopting a decentralised verification system based on blockchain technologies.

	USD
Number of Records	22.000
Cost of Record Procesing	$ 35.000
Reduction in Cost per Record	25%
Savings Record Processing	$ 8.750
Conflicting records	5%
Cost of resolution of conflicting records	$ 2.200
Annual Efficiency Benefits	**$ 10.950**
Cost of integration of the technology	$ 1.980
Annual Cost of Decentralized Verification	$ 19.800
Cost of Adoption Through Vendor	**$ 21.780**
Benefit Cost Ratio	0,50
Cost of integration of the technology	$ 1.680
Annual Cost of Decentralized Verification	$ 5.600
Cost of Adoption Through Consortium	**$ 7.280**
Benefit Cost Ratio	1,50

Regarding the cost of using a decentralised verification system, we use the estimated cost from choosing a certification vendor or participating in a university consortium. Also, we estimate the cost of integrating blockchain issuance and verification to the existing technologies. These costs represent anywhere from 10 to 30% of the cost of using the service.

We find that the benefit-cost ratio is 0.48 in terms of adopting the technology using the current price structure offered by certification vendors. On the other hand, the benefit-cost ratio is 1.5 of using the technology by joining a university-sponsored consortium. These estimates are based on the interviews conducted and public information obtained on the different projects. In particular, it is fair to say that certification vendors have already gone through various iterations of the service, whereas university consortiums are in the process of developing and delivering the technology so their cost could be underestimated. Our results are meant to illustrate the dilemmas in implementing blockchain technologies and a careful comparison of the portfolio of services provided by certification vendors should be taken into consideration.

5. Conclusion

Blockchain technologies have already begun to change how we share important information, in this case, the acquisition of skills and knowledge. Although, we expect a full transformation of the knowledge management system, for the moment, the most immediate impact is to provide direct access to the certificates without the need of re-issuance and a decentralised verification system. Since digital certificates and e-transcripts are a reality at most institutions, the added security features from blockchain technology and reduced cost are especially important, if at some point they are legally accepted as notarised documents with a general acceptance across national borders.

Implementing blockchain projects has similar fixed costs for providers and challenges related to the issuance and verifications systems; this is independent from choosing a permissioned or a permissionless network. We do not find that the fees associated with using existing permissionless networks are important, nor are marginal costs for that matter. The reason is that the transactions that are registered onto the blockchain are not complex operations or time-critical and there are well-known approaches to reduce the cost substantially. So price differentials among certificate vendors are related to the quality of applications that provide a seamless interaction with the information systems of the issuer institutions and additional technologies that are part of their portfolio.
For consortium and permissioned blockchain initiatives, we do not find that the fixed cost of starting the network overwhelmingly increase the fees for newcomers. IT companies that are helping universities implement the technology are paying for some of the fixed cost and investing on building the infrastructure. The current prices for joining a permissioned network and issuing certificate are lower than using certificate vendors, but at the same time, this might also indicate that the former provides a richer portfolio of services for certificates, while consortiums are specializing in blockchain technologies.

The benefits for consortiums of tertiary education institutions are beyond the benefits of just a system for issuing and verifying academic certificates, and this is probably the first step towards systems for sharing information and knowledge management that can be built around the initial nodes that are being developed for certificate management. A similar system but using centralized databases is already a reality for most high schools, colleges and universities in the United States: The National Student Clearinghouse. The National Student Clearinghouse is a non-profit organization that exists since 1993 providing a unique database for enrolments and educational accomplishments for 97% of post-secondary students in the US. Since 2000, they provide digital verification services for degrees using DegreeVerifySM, which also provides readily available e-transcripts for students. This is a good example for a consortium-led effort between universities to share academic information. More importantly, this consortium already provides some estimates on the benefits of sharing information among institutions: first, there are costs saving in sharing academic information ($750 million USD in annual savings), and second, it provides a data-rich environment to analyse the trends in the industry.

References:

[1] Deloitte, "Deloitte's 2019 Global Blockchain Survey," 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.
[2] B. Flyvbjerg and A. Budzier, "Why your IT project may be riskier than you think," Harvard Business Review, pp. 2-4, September 2011.
[3] M. Rauchs, A. Glidden, B. Gordon, G. Pieters, M. Recanatini, F. Rostand, K. Vagneur and B. Zhang, "Distributed Ledger Technology Systems: A Conceptual Framework," 2018. [Online]. Available: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf.
[4] C. Platt, "Medium," 14 May 2018. [Online]. Available: https://medium.com/@colin_/analysing-costs-benefits-of-public-blockchains-with-data-104ec5f7d7e0.
[5] Hyperledger, «www.hyperledger.org,» 11 September 2019. [En línea]. Available: https://www.hyperledger.org/announcements/2019/09/11/consensys-joins-hyperledger-as-a-premier-member.
[6] A. Grech and A. F. Camilleri, "Blockchain in Education," 2017. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf.
[7] P. Ocheja, B. Flanagan, H. Ueda and H. Ogata, "Managing lifelong learning records through blockchain," Research and practice in technology enhanced learning, vol. 14, no. 4, pp. 2-19, 2019.
[8] Ernst & Young LLP., «Total cost of ownership for blockchain solutions,» 2019. [En línea]. Available: https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-

solutions.pdf.
[9] Forrester Research, «Emerging technology projection: The total economic impact of IBM blockchain,» 2018. [En línea]. Available: https://www.ibm.com/downloads/cas/QJ4XA0MD.
[10] P. Panuparb, "Cost-benefit analysis of a blockchain based supply chain finance solution," May 2019. [Online]. Available: https://ctl.mit.edu/pub/thesis/cost-benefit-analysis-blockchain-based-supply-chain-finance-solution. [Accessed 24 February 2020].
[11] «CollegeData,» [En línea]. Available: https://www.collegedata.com/en/explore-colleges/the-facts-on-fit/features-that-set-colleges-apart/college-size-small-medium-or-large/. [Último acceso: 11 06 2020].

Competing Interests:
Universidad del Rosario is one of the participating universities in Red Blue, one of the blockchain projects mentioned.

Ethical approval:
Not applicable.

Author's contribution:
CC-I designed and coordinated this research and prepared the manuscript in entirety. O-G has collaborated on different projects on the application of blockchain technology for academia.

Funding:
None declared.

Acknowledgements:
This paper benefited from comments received from the anonymous referees, Federico Lopez, Mauricio Tovar, Ana Maria Moreno, and seminar participants at the Hyperledger Global Forum 2018, Universidad Nacional de Colombia, Red Arca and Universidad Jorge Tadeo Lozano. CC-I would like to thank Francisco Garcia Camargo, director of de registrar's office at Universidad del Rosario, Pablo Carretero Sanchez, Blockchain lead at Ibermatica, Danny Suarez and Sebastian Farfan, co-founders of Xertify.

[1] https://www.blockcerts.org/.
[2] https://www.accredible.com/.
[3] https://xertify.co/.
[4] https://gradba.se/en/.
[5] https://www.learningmachine.com/badges-and-blockcerts/.
[6] https://opencerts.io/.
[7] https://www.chaintalent.io/; http://tic.crue.org/blue/.
[8] According to [11] in the US small universities have an enrolment of less than 5,000 students, medium size can go up to 15,000 students and larger institutions have more than 15,000. The largest institutions have 30,000 – 70,000 students.
[9] https://registrar.stanford.edu/students/certifications-and-verifications/notarized-documents
[11] https://registrar.mit.edu/transcripts-records/replacement-diplomas
[12] https://www.urosario.edu.co/registro-y-control/solicitud-de-certificados/
[11] Some vendors are transitioning to charging the recipient to manage all types of certificates, not only academic. Discussions on standards (like Verifiable Credentials and Blockcerts) are currently exploring the benefits of decentralised identifiers for the issuer and the recipient. Recipients would hold their certificates in some form of wallet and provide them to any number of solicitors. The certification providers, for a fee, would use blockchain to guarantee the validity of the information regardless of the issuer. This is similar to what a credit bureau currently does; for a monthly fee (5 – 20 USD), they collect information regarding an individual creditworthiness and provide a credit score for solicitors.
[13] https://github.com/blockchain-certificates/cert-issuer
[14] https://www.codementor.io/freelance-rates/blockchain-developers

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585//jbba-3-2-(3)2020

Self-executing Contracts from the perspective of the selected Polish regulations and the future potential prevalence of 'Smarter' Contracts

Rafał Tomasz Prabucki
University of Opole, Centre for Legal Problems of Technical Issues and New Technologies, Poland
Correspondence: rprabucki@uni.opole.pl
Received: 24 February 2020 **Accepted:** 15 April 2020 **Published:** 30 April 2020

Abstract

For some time now, blockchain technology has been used for many purposes all over the world. The question arises – how do we regulate proving facts in a dispute between agreement parties when they use self-executing contracts? The answer to this question is explored in this research in the context of civil issues. Furthermore, the Polish law has introduced a new tool in the form of a 'contract of evidence' (similar to the parol evidence rule) which may increase the popularity of smart contracts. The research methodology is based on the analysis of the two existing regulations from the Civil Procedure Code and the Commercial Code. Moreover, legal scientific studies that indicate the risks associated with using self-executing contracts in such a way will be analysed. All efforts have been taken to obtain conclusions regarding the future of this type of solution in Poland and Polish smart cities.

Keywords: *contract of evidence, Polish law, blockchain, smart contracts, evidence law*

JEL Classifications: *K10, K12, K15, K20, K24, K40*

1. Introduction and methodology

For the last few years, smart contracts have become the subject of increasing interest of political decision-makers, among others, who obviously show strong interest in this kind of novelty, but what is more important in this case is that, at the same time, they are undertaking the necessary measures to introduce legal regulations connected with it. The Polish Institute of Justice has commissioned a scientific report which, despite the fact that it does not directly address the issue of the idea of smart contracts, indicates, due to the questions related to blockchain technology, that such an element of development of this technology exists and is a subject of interest of legislators of various countries. The analysis of sources cited for the purpose of this report shows that at least four European countries have presented concrete proposals for legal definitions for this concept. In the United States, in turn, at least four states have developed new juridical categories, including smart contracts [1].

Such a keen interest of policy makers in this matter should not come as a surprise. Scientific debates, which include the word "smart contract", are not limited only to areas such as mathematics, computing and engineering but also covered the fields connected with energy and social science discussions. The countries that are at the forefront of scientific publications on smart contracts are first and foremost the ones which have officially developed or are observing and planning to develop a possible kind of regulation for the blockchain industry. Among these are countries such as the United States, China, the Russian Federation, South Korea and the United Kingdom. Poland is not listed [2].

This work aims at catching up on this issue by drawing attention to the recent amendment to the Civil Code, which introduced a contract of evidence into Polish law. In accordance with the recommendations appearing in the literature dealing with the issue of smart contracts, the work first of all assumes the approximation of the diversity of approaches in defining smart contracts.

2. Theoretical foundations of smart contracts and links to blockchain

The original source of knowledge about smart contracts are works from the 1990s. Thanks to Nick Szabo, his essays and scientific papers, the term "smart contract" has penetrated the legal world. This is not the only issue that should be brought closer to the work of a computer scientist and lawyer. Szabo also refers to the so-called "micropayments" in his works. Both phrases were supposed to help outline the predicted changes in the law of obligations, which were to appear and spread due to technological progress. The Internet, through its protocols, revolutionised the transmission of information across the globe. It has become possible to draw up a theoretical protocol for the declarations of will and knowledge that make up the agreement. N. Szabo defines smart contract as "Smart contract is a computerised transaction protocol that executes the terms of a contract". Furthermore, he added that "the general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs" [3].

The second element, which is very significant, contains micropayments. For their application, N. Szabo identified specific markets, such as the electricity market, where complicated contracts and the need for constant invoicing are major problems. In the context of micropayments, however, the researcher refers to intelligent agents [4]. Vincenzo Morabito notes that there is, in the context of their theoretical assumptions, a lot of convergence between smart agents derived from the concept of software agents and smart contracts and there is even a convertible application of both concepts. These coincidences also strongly emphasise the modern relationship of smart contracts with Distributed Ledger Technology

(DLT), which has the potential to facilitate business models based on micropayments [5]. It is necessary to mention that the dissemination of the idea of smart contracts occurred after the launch of bitcoin, the first cryptocurrency. Moreover, Vitalik Buterin added an opportunity to his idea of cryptocurrency, which is the possibility of creating smart contracts in blocks. The language in which it could be created was the programming language of Solidity. Blockchain of this type was called the "new generation", due to the implementation of the virtual machine. The Ethereum not only recorded the information about the trading of transactions of Ether (payments token) but also enabled creating computer programs which were aimed to automate this kind of trading. BT allowed to secure smart contracts accordingly. Furthermore, when smart contracts are recorded in blocks of chains, they are difficult either to sabotage or to edit the conditions they contain. G. Wood, co-founder of Ethereum, called this: "a general implementation of such a crypto-law system" [6, 7, 8, 9, 10, 11].

3. DLT and smarter contracts

However, smart contracts in the Ethereum blockchain are not free from defects and certain restrictions. Working in this environment is based on careful selection of programming code due to the fee for using a virtual machine with a token called "Gas". In consequence, the price that must be paid for purchasing Ethereum tokens can make creating certain smart contracts unprofitable. It is not only about the price of the Ether token but also about the number of Gas tokens that have to be paid to run the program [6]. Moreover, it should be emphasised that participation in an open blockchain is allowed to anyone. So it may happen that dishonest persons may appear or even smart contracts can be created to secure parties who have contracted a service which is classified as a criminal offence in a given legal system.

However, smart contracts are also possible to be carried out in closed blockchain solutions as well as blockchain-like solutions (e.g. Corda), which can be easily entered within the name range of DLT. New technological possibilities and solutions also increase the range of possible combinations in terms of operation. Rory Unsworth proposes to add the term "smarter contracts" to the scientific discussion and suggests that this term includes split and hybrid smart contract models. The author of this classification also emphasises that "smarter" is not related to the fact that these solutions are better, as the ones described by N. Szabo equally qualify for this name. In order to define smarter contracts, it is necessary to call them self-executing contracts. The hybrid model adds human factor as supervising the operation of the contract in certain situations. The split model, on the other hand, serves to combine certain expressions of language, which is understandable to people but also connects with the activities of a smart contract. These concepts expand the business application of the individual models and order the chaos in theoretical deliberations on the law and the future of self-executing contracts [12, 13, 14].

It is also important to signal that the flywheel of self-executing contracts is the incoming data, which triggers subsequent elements of the contract after the relevant facts have occurred. Collecting important information from outside the blockchain is possible due to connectors called "Oracles" [15].

It seems that it is the possibility to collect data that puts self-executing contracts high in the hierarchy of essential elements that will shape our world in the era of the Internet of Everything (IoE). The future that awaits us will surely also bring a question about where the data for self-executing contracts are drawn from and whether they can be trusted. However, before this happens, it is important to pay attention to certain possibilities and issues concerning obstacles of legal nature [15].

It should not be forgotten that a contract is still – in the traditional sense – not only a set of commitments but also a scenario designed according to certain regulations with mechanisms that are adapted to certain situations [16].

4. Contract automation in Polish legal scholarship

N. Szabo, in his theory, compares smart contracts to vending machines. In the Polish school of academic thought, this problem was raised by Ernest Till in 1900. According to these general demands, vending machines are an offer addressed to the general public. Due to the lack of words or letters, the whole state of affairs can be considered as the content. The conclusion of a contract occurs when both parties correctly demonstrate their willingness to join through appropriate behaviour. an inserted coin generates the information for the exhibitor of the vending machine of joining the offer by the other party. When it comes to smart contracts, the transfer of the relevant token(s) will be considered as silent provision of services, which the creator of the smart contract has required. This moment will be considered as a contract entry. It is worth noticing that the difference between displaying such articles as, e.g., newspapers and bread in front of the shop and a vending machine was also noticed. In the former case, E. Till emphasises that a person coming up with an offer, that is, a bidder, gives himself a certain freedom in order to secure his right to make decisions on the execution of the contract. As in the case of the hybrid model, there still remains some scope for human action [17].

It probably never occurred to E. Till that similar mechanisms would appear on the line of much more complicated contracts. That is why Robert Herian calls the vending machine theory "elegant", but he criticises it for the probability of a defect occurrence, meaning that it looks well until it works without problems [15].

A contemporary concept of smart contracts in Polish legal scholarship is presented by Dariusz Szostek. His approach is based on a list of legal definitions from other countries and their comparison. The author draws attention to three examples from Malta, Belarus and the state of Arizona. As the most advanced, mature and adequate to the technical reality, D. Szostek indicates the definition which was constructed for the needs of Maltese law. According to this definition "smart contract" means a form of innovative technology arrangement consisting of: (a) a computer protocol and/or (b) an agreement concluded entirely or partly in an electronic form, which is automatable and enforceable by the execution of computer code, although some parts may require human input and control and which may also be enforceable by ordinary legal methods or by a mixture of both [18].

In terms of the technical and theoretical elements of smart contracts cited above, the legislator's approach in such a direction as to take account of the issues of computer protocols and the electronic nature of the contract, together with a general outline of some of its features, shows a high degree of sophistication and is a sign of maturity. In both examples presented by D. Szostek – the one of the state of Arizona and another one of Belarus – references to BT and DLT terminology dominated. The use of blockchain-related concepts complicates the definition unnecessarily, making it incomprehensible to a person who does not deal with it on a daily basis. Moreover, a strong reference to the medium seems to be a significant limitation in the creation of this technology in the future [13, 18, 19].

The choice of D. Szostek expands the debate about smart contracts. The Maltese legal definition has several significant advantages:

- It emphasises the aspect of the legal act and the means of electronic communication, not the medium.
- It leaves space for the split and hybrid models.
- It proposes an additional scope of the name which does not refer to the term of the contract.

Moreover, the definition of diversity of the use of smart contracts is that it creates a technological neutrality, which can be adopted and put into long-term use without changes to this jury category. The Maltese legislator does not use the terminology which is characteristic for DLT; what is more, the

Maltese legislator proposes two concepts of smart contract, one of these is not related to the sphere of obligations. As a result, a scenario in which a smart contract can appear in the state's actions is not excluded but is taken into consideration; at the same time, a new situation is created in which smart contracts can appear in an entirely different sphere, that is, in the sphere of public authority.

In the first place, the smarter contracts and its further development will have a significant impact on the civil law sphere. It should be noted that two main points are specified within the civil law sphere according to the European Union (EU) report and these are as follows [20]:

- Smart legal contracts are smart contracts on a blockchain that represent – or that would like to represent – a legal contract, along with the issues that are involved.
- Smart contracts with legal implications are artefacts/constructs based on smart technologies that clearly have legal implications.

Therefore, it should not come as a surprise that the emergence of self-executing contracts in practice implies not only the need to create legal definitions but also changes in other legal acts. The problem is not only the legal framework of a certain relationship in which a program written in programming code may not fit but also the programming language and the way in which certain processes work, as these are the factors which the court may not understand. Moreover, it should be assumed that some changes still appear as new ones in numerous works and approach to smart contracts (jellyfish theory). It is also important to point out that not only the consequences of the regulations being created are important but also unplanned changes that are difficult to predict [9, 12, 13, 15].

5. Legislative tendencies and Polish regulations

The emergence of smart contracts is causing various reactions of law-making nature worldwide. Mainly the acts of BT regulation are introduced, but the example of the Russian Federation shows that changes are constantly made to legislative acts. Russia, like other progressive countries, has created a legal definition of smart contracts as well. The content of this definition in full wording is as follows: "an electronic contract, whose rights and obligations are executed automatically in a distributed register of digital transactions in a sequence strictly defined by such a contract and after the circumstances have occurred" [1, 21].

The introduction of this juridical concept into the Russian legal system has resulted in changes to the Civil Code. It not only did add many elements such as "Internet", "electronic" and "digital", but the section on contracts was extended with a new paragraph: "A contract may provide for the performance of an obligation under the contract after certain circumstances have occurred which were not covered by the will of the party, but were defined at the time of the conclusion of the contract by the terms of the transaction concluded in an information system (automated performance). Only the parties to the agreement may call for the performance of such an obligation". This content indicates that it was created to secure the most important element of self-executing contracts – automation. The legislator has thus introduced a new optional element of the contract – automated performance of an obligation [1, 21–23].
Another example of solution is the one called "Singapore". In this case, the legislator amended the Evidence Law Act. Although the name of the concept of smart contract is not mentioned at all, there is a definition of electronic recording. In addition, the institution of presumptions in relation to electronic records was created, and the main purpose of this kind of legal institution is to instruct the court how to evaluate evidence [24].

In Poland, despite the proposal of amendment of the Commercial Companies Code and the introduction of DLT by introducing a clause in joint-stock companies and stock companies that "the register of shareholders is maintained in an electronic form, which may take the form of a distributed and decentralized database", as it can be used in running the company, which will imply proving certain facts in the future with the need to refer to DLT elements, including what smart contracts are and what they are meant for. In the case of tokenisation, the question of a "document" also arises [25]. In general, the court will have to check whether the solution used in the DLT can be treated as a document. Additionally, the court will also be obliged to verify in which DLT solution the data was saved. This issue of legal value blockchain will need to be examined based on eIDAS regulations [20].

No simultaneous attempt has been made in Poland in order to amend the Civil Code or the Civil Procedure Code. At present, there is no separate act in Poland which would regulate the issues of the law of evidence. It is worth noticing that for the period of time that self-executing contracts started to become more and more popular, there has been a change introduced in the Polish legal system affecting the practice of using smart contracts. It is the contract of evidence that is similar to the common law parol evidence rule.

6. Contract of evidence

A new institution in Polish law, based on parol evidence law, was established, and it can be presented in the following points [26]:

- It refers to the contractual relationship.
- It is addressed to entrepreneurs.
- It excludes certain means of proof.

In the context of the consideration of a smart contract, this judicial institution does not permit any agreement that restricts the court's ability to admit evidence or any possibility that could impose its assessment. As a result, it is neither possible to create new, and especially unknown to the procedural law, means (sources) and methods of evidence nor can specific evidence, special evidentiary power or any other extraordinary procedural significance be given priority. It is also not allowed to change the function of factual and legal presumptions and other rules of taking evidence. In conclusion, the parties cannot influence the free assessment of evidence [26].

Taking other aspects into account, it should be noted that the permitted exclusion of evidence may consist in prohibiting the use of certain types of evidence (e.g. evidence from witness statements, expert opinions, documents, etc.) or specific evidence, individualised by their exact description (e.g. evidence from a specific document, from specific witnesses, from specific expert opinions, etc.). The exclusion may also depend on the ban on proving specific circumstances, as, e.g., specific facts that normally are subject to the statement of the court (subject of evidence) [26].

So there are elements that can be used in the context of this institution and smart contracts. Knowing a specific expert, who, in his opinions, is not very reliable in presenting the issues of our smart contract; nothing stands in the way of excluding him by means of a contract of evidence; it can be orally submitted before the court. It is not possible to instruct the court to use, for example, the presumption of electronic recording, as presented above, by means of this evidence contract. The very limited institution of parol evidence law under Polish law seems to be neither particularly restrictive nor particularly supportive of the development of the use of smart contracts. It is possible that further adoption of the patterns of Anglo-American solutions will result in the appearance of new models. This situation seems more than likely as the entry into the IoE era will generate the need to expand this institution.

7. Smart city in Poland and smart(er) contracts

IoE is an important element of the difficult-to-define concept of the smart

city, where in a nutshell, ubiquitous technology makes life easier for the digital society. It is worth underlining that the "smart" element of this concept, i.e. technology, may have undesirable consequences in the sphere of contracts for the legal awareness of smart city residents. The point is that people may not understand if and when they create legally binding contracts, or they may not understand their rights and obligations under their contracts. Technology saturation also depends on experts. Therefore, it seems reasonable to appeal to scientists for smart solutions, which will also be user-friendly and will take into account the dominant role of law in the sphere of contracts [23, 27].

There is also an important comment to be made in this area. Kevin Werbach and Nicolas Cornell noticed that self-executing contracts shift the focus of the remedy from execution to return [27]. However, it remains an open question whether it is a smart contract or a modern civil law turnover, with its tendency to accelerate access to, e.g., a service which implies an approach that gravity of the remedy is shifted. What really seems to change due to smarter contracts is definitely increasing formalism. The open question is how it will relate to human mess and human mistakes. Even in the most developed society functioning in a very advanced smart city, this problem will never be eliminated [27, 29].

In the context of the smart problem and technology-saturated contracts in terms of the smart city, there are also several other problems which are very significant:

- The development of smart contracts in a smart city requires a discussion about the adherent way of entering into contracts, which seems to be the natural direction in the sphere of citizen's activity in the city (entering the public transport vehicle, parking in the paid parking zone etc.)[29].
- Due to the international character of various corporations that offer smart contracts, the role of international private law, as well as establishing the proper international jurisdiction of the contract, seems to be very important [27, 30].
- The concepts of machine-to-machine contracts and the role of man who drives, for example, an autonomous electric vehicle that needs recharging batteries once in a while are also still discussed.

At the moment of writing the article in Poland, the authorities of one of the voivodeships officially admitted that they use DLT solutions. After preparing and submitting a request for access to public information to the Marshal's Office of the Warmińsko-Mazurskie voivodeships, a representative of the authorities has admitted that they use utility tokens called "CoperniCoin", which are assigned to the Waves token. The representative denied that the process of issuing took place in the framework of smart contracts and that smart contracts were used in the framework of CoperniCoins trading. Moreover, he noted that it is the designated employee who distributes the tokens as part of the region's promotional activities and that, until 18 December 2019, 101 CoperniCoin tokens were in circulation. Due to the lack of a legal definition of smart contracts, it is difficult to question or criticise such an approach, and it should be considered as correct. However, it is the irrefutable evidence that the popularity of DLT solutions will increase [31].

8. Conclusion

In conclusion, it should be noted that further dynamic development of the DLT can contribute to a greater interest of policy makers in smart contracts. It seems that it depends a lot on the significant factor which is the factor of power activity, in other words, it depends a lot on people who are in power and also on influencial persons who can contribute to increasing science's participation in the study of this novelty. It should be regarded as positive that the approval of the paper to smart contract in the Code of Commercial Companies is allowed. It seems worrying that there are no indications concerning the evidential issues connected with the introduction of this type of solution. The most visible change that can be transferred into the practice of smart contracts is the contract of evidence, but its possibilities are significantly limited.
Certainly, in the context of the digital society functioning in smart city, it should be perceived positive that the contract of evidence does not apply to the entrepreneur-consumer relationship. However, the development of the smart city concept implies many other challenges to be faced. Both in terms of smart contracts as well as in terms of law.

Taking into account the participation of Poland in the structures of the EU, it seems substantial to formulate several conclusions in the form of postulates which open the discussion on smart contract under the laws of Poland:

- Poland should be active and monitor the legislative activity of the EU in the field of DLT technology.
- The EU should regulate DLT and introduce the most sustainable technology and state a technologically neutral definition of smart contracts.
- The EU should establish an office to regulate matters relating to the competence of the experts dealing with problems concerning smart contracts, and this office should solve any potential problems within the area of smart contracts.
- The Polish legislator should, in turn, examine and propose possible amendments to the Civil Law Code and the evidence law, so that it takes into account the digital nature of digital evidence.
- The provision related to contracts of evidence should be monitored in terms of its usefulness in practice and also together with the appropriate proposals, possibly extended.

References:

[1] K. Zacharzewski and M. Kłoda, "Przegląd zastosowania technologii blockchain w wymiarze sprawiedliwości w wybranych państwach", Instytut Wymiaru Sprawiedliwości, Warsaw, 2019.
[2] E. Salmerón-Manzano and F. Manzano-Agugliaro, "The Role of Smart Contracts in Sustainability: Worldwide Research Trends", Sustainability, vol. 11, no. 11, p. 3049, 2019. Available: 10.3390/su11113049 [Accessed 13 January 2020].
[3] N. Szabo, "Formalizing and Securing Relationships on Public Networks", First Monday, vol. 2, no. 9, 1997. Available: 10.5210/fm.v2i9.548.
[4] N. Szabo, "The Mental Accounting Barrier to Micropayments", Nick Szabo's Essays and Concise Tuturials, 19.
[5] V. Morabito, Business innovation through blockchain – the b(3) perspective.
[6] V. Buterin, A next generation smart contract & decentralized platform. 2014.
[7] J. Sklaroff, "Smart Contracts and the Cost of Inflexibility", University of Pennsylvania Law Review, vol. 166, 2017. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3008899. [Accessed 13 January 2020].
[8] A. Savelyev, "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law", Information & Communications Technology Law, vol. 26, no. 2, pp. 116–134, 2017. Available: 10.1080/13600834.2017.1301036 [Accessed 13 January 2020].
[9] K. Künnapas, "From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda?", in The Future of Law and eTechnologies, T. Kerikmäe and A. Rull, Ed. Cham: Springer International Publishing Switzerland, 2016, pp. 111–129.
[10] P. Cuccuru, "Beyond bitcoin: an early overview on smart contracts", International Journal of Law and Information Technology, vol. 25, no. 3, pp. 179–195, 2017. Available: 10.1093/ijlit/eax003 [Accessed 13 January 2020].
[11] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger. EIP-150 revision", Available: http://gavwood.com/Paper.pdf [Accessed 20 March 2020].
[12] R. Unsworth, "Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for 'Self-executing' Contracts", in Legal Tech, Smart Contracts and Blockchain, M. Corrales, M. Fenwick and H. Happio, Ed. Singapore: Springer Nature Singapore Pte Ltd., 2019, pp. 17–59.

[13] K. Low and E. Mik, "Pause The Blockchain Legal Revolution", International and Comparative Law Quarterly, vol. 69, no. 1, pp. 135-175, 2019. Available: 10.1017/s0020589319000502.
[14] E. Mik, "Smart Contracts: A Requiem", SSRN Electronic Journal, 2019. Available: 10.2139/ssrn.3499998 [Accessed 13 January 2020].
[15] R. Herian, "Legal Recognition of Blockchain Registries and Smart Contracts", in Blockchains and smart contracts legal and regulatory framework, Paris, France, 2018.
[16] E. Mik, "Smart contracts: terminology, technical limitations and real world complexity", Law, Innovation and Technology, vol. 9, no. 2, pp. 269–300, 2017. Available: 10.1080/17579961.2017.1378468 [Accessed 13 January 2020].
[17] E. Till, O znaczeniu prawnem automatu. Lviv: E. Winiarz, 1900.
[18] D. Szostek, Blockchain and the Law, 1st ed. Baden-Baden: Nomos Verlagsgesellschaft Mbh & Co.
[19] E. Mik, "Smart Contracts: A Requiem", SSRN Electronic Journal, 2019. Available: 10.2139/ssrn.3499998 [Accessed 13 January 2020].
[20] The European Union Blockchain Observatory and Forum, "Legal and Regulatory Framework of Blockchains and Smart Contracts", The European Union Blockchain Observatory and Forum, 2019.
[21] G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor and X. Xu, "On legal contracts, imperative and declarative smart contracts, and blockchain systems", Artificial Intelligence and Law, vol. 26, no. 4, pp. 377–409, 2018. Available: 10.1007/s10506-018-9223-3 [Accessed 13 January 2020].
[22] Закон о внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации, no. 424632-7. Moscow: Государственная Дума Федерального Собрания Российской Федерации, 2019.
[23] T. Barton, H. Haapio, S. Passera and J. Hazard, "Successful Contracts: Integrating Design and Technology", in Legal Tech, Smart Contracts and Blockchain, M. Corrales, M. Fenwick and H. Haapio, Ed. Singapore: Springer Nature Singapore Pte Ltd., 2019.
[24] Evidence Act, vol. 97. Singapore: Singapore Government, 1983.
[25] Rządowy projekt ustawy o zmianie ustawy – Kodeks spółek handlowych oraz niektórych innych ustaw, no. 2019, 3236. Warsaw: Sejm Rzeczypospolitej Polskiej, 2019.
[26] Kodeks Postępowania Cywilnego. Warsaw: Sejm Rzeczypospolitej Polskiej, 1964.
[27] M. Kõlvart, M. Poola and A. Rull, "Smart Contracts", in The Future of Law and eTechnologies, T. Kerikmäe and A. Rull, Ed. Cham: Springer International Publishing Switzerland, 2016, pp. 133–145.
[28] K. Werbach and N. Cornell, "Contracts Ex Machina", Duke Law Journal, vol. 67, no. 2, pp. 313–381, 2017. Available: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj. [Accessed 13 January 2020].
[29] J. Sun, J. Yan and K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities", Financial Innovation, vol. 2, no. 1, 2016. Available: 10.1186/s40854-016-0040-y [Accessed 14 January 2020].
[30] M. Solarte-Vasquez, N. Järv and K. Nyman-Metcalf, "Usability Factors in Transactional Design and Smart Contracting", in The Future of Law and eTechnologies, T. Kerikmäe and A. Rull, Ed. Cham: Springer International Publishing Switzerland, 2016, pp. 149–174.
[31] M. Bułkowski, email answer for "Wniosek o dostęp do informacji publicznej dot. CoperniCoin/Request for access to public information concerning CoperniCoin" sent on 17 December 2019 to Marshal Office of the Warmia and Mazury Region.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
RTP main author responsible for writing the manuscript, collecting data, proof reading etc.

Funding:
None declared.

Acknowledgements:
Dr Janinie Grucza - for the first steps in the world of science.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585//jbba-3-2-(3)2020

Blockchain: A Panacea for Trust Challenges In Public Services? A Socio-technical Perspective

[1]Ali Shahaab, [2]Ross Maude, [1]Chaminda Hewage, [1]Imtiaz Khan
[1]Cardiff School of Technologies, Cardiff Metropolitan University, UK
[2]Companies House, Cardiff, UK
Correspondence: ashahaab@cardiffmet.ac.uk
Received: 15 May 2020 **Accepted:** 03 June 2020 **Published:** 22 July 2020

Abstract

Trust in corporations, governments and public services has been steadily declining over the last few decades. Lack of transparency and auditability has been a key driver for this decline. Blockchain technology has been commended as a solution that can help with disintermediation and filling the consistently increasing trust challenges faced by the corporate and public sectors. Public services are seeking solutions that can help establish trust and increase transparency with its citizens and businesses are undertaking extensive business analysis to determine the need and effectiveness of blockchain-like platforms as the basis for transforming their existing platforms. Due to the decisive nature, most of the analysis results thus indicate that if a trusted third party is an option, then blockchain should not be used. Here we highlight the challenges and opportunities of establishing trust and how blockchain technology can help public services bridge the trust gap with its citizens. We argue that all information technology systems rely on a suite of technologies, thus blockchain should be added to the current technology stack rather than taking an 'all or nothing' approach. We also argue that analysing the effectiveness of futuristic technology like blockchain with industrial age methodology and mindset may limit the realisation of its impact on society and economy. Therefore, we propose to take a heuristic approach, where different properties of blockchain technology need to be mapped against different aspects of current business process with a futuristic view in mind. Taking Companies House – a government organisation that holds over 4 million UK-based companies' records – as an example, we demonstrate how certain business processes in Companies House can benefit from adapting a blockchain-based solution.

Keywords: *trust, blockchain, public services, distributed ledger technology, business process*
Keywords: *K10, K12, K15, K20, K24, K40*

1. Introduction

Sir Mark Walport, the UK government's chief scientific adviser (2013–2017), states in his 2015 report that 'in distributed ledger technology we may be witnessing one of those explosions of creative potential that catalyse exceptional levels of innovation. The technology could prove to have the capacity to deliver a new kind of trust to a wide range of services'. [1]. Joseph Schumpeter coined the term 'creative destruction' to explain how the process of industry transformation revolutionises the economic structure from within, by destroying the existing one and simultaneously creating a new one [2]. Carlota Perez took the notion further to explain how technological revolutions driven by 'creative destruction' redefine not only an industry but also the infrastructures and economic institutions surrounding it [3]. Perez called the phenomenon of the diffusion of new technologies that spread and proliferate their impact across economies and eventually transform the socio-institutional structure a 'techno-economic paradigm' (TEP) [4]. As the technology evolves, the way businesses and work are organised transforms along with it. Public and private institutions frequently re-evaluate their business models to take advantage of the technological innovations. Furthermore, the technology influences the business model possibilities [5]. We have witnessed this in the shape of assembly lines during industrial revolution, office work with the introduction of computers and life as we know it since the World Wide Web (WWW).

The economies now are data driven. Organisations collect and process data at a rate never seen before. Since data has value and utility, it encourages hackers and criminals to exploit vulnerabilities in the information technology infrastructure of the organisations, leading to all sorts of hacks and breaches. Blockchain technology (BCT) has seen its utility for information security in several ways such as protecting personal data [6, 7], secure data sharing [8], access management [9], data integrity [10] and digital identities [11]. However, analogous to any other disruptive technical breakthrough, when the horizon is unclear and uncertainty is high, there is a substantial hype around BCT.

The 'Gartner Hype Cycle' illustrates the typical progression of an innovation, from the phases of inflated expectations through disillusionment to a realisation of the relevance of the innovation and its applications [12]. BCT has been one of the considerably hyped technologies and has been on the Gartner Hype Cycle for the recent few years. The world has witnessed the initial coin offer bubble, to the 'blockchain for everything' bubble and now we are seeing the exploration of serious use cases. Several industries have spent billions of dollars exploring the blockchain use cases for their business models. International Data Corporation forecasts the spending on blockchain solutions (including Distributed ledger technologies (DLTs)) in 2023 to approximately $15.9 billion, with a compound annual growth rate of 60.2% [13].

With such potential of growth, businesses seek guidance to help them decide if blockchain is a potential solution to their use case. Several different decision schemes have been proposed over the recent years to assist businesses in determining if BCT is the right solution for their use case. However, since the technology is relatively recent and quite distinct, several proposed schemes conclude differently. Koens and Poll [14] analysed 30 blockchain decision schemes and found several contradictions

between those schemes, arguing that most of them were inherently flawed [14]. Twenty out of the thirty schemes that Koens and Poll studied argued that if a trusted third party (TTP) can be used then blockchain should be avoided. However, we argue that this argument contradicts the basic ethos of Satoshi Nakamoto's design of the bitcoin blockchain and the whole principle of decentralised trust.

In his landmark paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System', S. Nakamoto writes: 'What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party' [15]. Nakamoto has noted down only one condition for transacting on the bitcoin blockchain and that is 'willingness to transact'. There is no further reasoning on only when the transacting parties should use the blockchain-based payment system (Bitcoin). If Nakamoto was to follow the same principle of 'is there a trusted third party that the transacting parties can use?' then bitcoin may not have been conceptualized, since the transacting parties can potentially 'trust' the conventional banking system. Therefore, we argue that the potential use cases of blockchain should be explored with an open mind and vision for future, so that the future potential applications and implausible solutions that the blockchain might hold are not excluded.
In this article we first establish the definition of trust in the online and offline world, followed by different forms of trust. Secondly, we compare the pros and cons of having a trusted third-party system or a blockchain-based system. Here we argue that the selection of blockchain (or blockchain-based systems) should not be an 'all or nothing' approach against current systems, but it should be aligned with business and process innovations, as it was noticed by Perez [4] and Fuller and Haefliger [5]. Thirdly and finally, we take Companies House UK (CH) as an example to demonstrate how BCT can improve or replace some of the current business processes, aiming at increasing trust, transparency, information integrity, cost reduction and efficient processing.

2. What is Trust?

Trust is paramount for the society to function. Nobel laureate Arrow called trust 'a lubricant for social systems' [16]. There is no agreed-upon definition of trust, but several definitions have emerged from multiple disciplines [17]. One of the widely cited definition of trust by Mayer, Davis and Schoorman is 'the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor and control that other party' [18]. For example, when we need purchase online, we trust the seller to send us the same product that we have purchased, without having any control over it.

Trust is often classified into broad categories [18, 21] such as calculative (based on rational choices), relational (derived from repeated interactions), organizational (based on expectations from an organisation) and institutional trust. Institutional trust refers to the confidence of individuals (trustor) in public institutions (trustee) such as military, parliament, police and other public services on a macro level [20]. While some scholars regard trust as a personal or inter-personal attribute [21, 22], others consider trust as an institutional property [23, [24, 25]. Even though the later acknowledge the importance of social trust, they argue that social controls, personal bonds or local mechanisms may work well within limited social boundaries, but formal institutions are of critical importance to establish cross-situational trust where direct personal contact is very limited [25]. However, trust is subjective and evolves with the societal shifts.

Miles and Creed [26] noted over two decades ago that the society was moving towards 'small-scale' relations where there would be a rise of independent contractors and flexible forms of organisations resulting in the breaking up of large firms. Miles and Creed [26] argued that it will result in the shift in predominant forms of trust. Furthermore, Saxenian [27] noticed a shift from institutional trust to individual and network-based trust. Neil et al have argued that social distance has an impact on the trust level [28]. The authors suggest that distributed teams with minimal physical or cultural contact operate at a limited trust level as compared to the teams functioning at the minimal social distance, which operate at the highest level of trust.

Trust is critical for businesses and individuals to transact. Since, in most cases, the transacting parties do not trust each other, a TTP is usually chosen to facilitate the transaction. The TTP acts as a gateway to establish trust. A strong assumption of trust reduces transaction cost, agency issues (entity acting on behalf of someone else to conduct a transaction) and governance expenses. It also helps to improve relationships, supports decision making when information is scarce and supports cooperation [29, 30]. The development of organizational ecology [31], institutional theory [32] and transaction cost economics [33] have all been underpinned by the assumption that organizations are the centralized source of trust and legitimacy [34].

Even though these assumptions have been historically effective, the recent emergence of distributed trust systems such as BCT has fundamentally challenged these core tenets of organizational theory [35].

3. Centralised vs Distributed Trust

In centralised trust, the trust is embedded in a central authority or institution and the transacting parties assume that the central authority will act in their best interest, following all written and unwritten rules. Examples of centralised trust are banking, public services, stockbrokers and so on. A TTP is inherently centralised. All users of such centralised system are by default required to rely on the trusted party for the provision of truth and assume that the trusted party will act selflessly in their best interest. This saturation of power leads to a single point of failure, both in technical and social terms.

The top-down coordination and hierarchical structures like governments, bureaucracy and centralised public services have been the solution to the ever-growing trust problem and facilitate mutual interactions among distant societies. Even though these centralised institutions have historically served their purpose, organizations with top-down centralized coordination and hierarchical structures tend to be inherently inefficient [36]. Furthermore, this concentration of power in the hands of few poses significant threats, such as corruption, misuse of power, lack of transparency and even regression into authoritarianism [36].

In decentralised trust, trust is disseminated to a decentralised network (DLTs, for the sake of this article), so no one entity has the sole power or monopoly over the act of transacting. By doing so, DLTs shift the trust from a central authority to a network of participants while simultaneously enabling shared information and governance. Bitcoin transactions, smart contracts and decentralised autonomous org anisations (DAO) are examples of decentralised trust. DLTs lower the uncertainty regarding the otherwise 'non-trusting' parties and allow them to transact without the need of a mutually trusted party [37]. However, this new trust enabler for exchange of information does not completely remove the need of trust but shifts the trust from intermediaries and institutions to the technology (the peer-to-peer network, cryptographic protocols, code, smart contracts, etc).
The lack of trust and need of establishing trust have always been there; however, until DLTs, centralised trust was the only dominant form of trust known to the world. The societal shift noted by Miles and Creed [26] along with a shift in trust (Saxenian) [27] enabled by the TEP [4] has led to the creation of behemoths such as Uber, Google, Amazon and Facebook which have now become the de-facto monopolies, leading to centralisation and single point of failure, among other socio-political issues.

4. The Cost of De-facto Trust

The cost of trust can be established in two ways (1) the cost of establishing the trust and (2) the repercussions when trust is breached. During the 2007–2008 economic crisis, 1.3 million people were made redundant in the United Kingdom, and 10 years later, we were still, on average, 30 pounds a week worse off than we were before the crash [38]. One of the key triggers of the 2007–2008 economic crisis was the bankruptcy of a 158-year-old business, Lehman Brothers. Only 9 months prior to declaring bankruptcy, Lehman brothers reported a record revenue and profit which was endorsed by their auditors Ernst & Young (EY) [39]. In the end, the organisations responsible for the biggest economic crisis since the great depression shrunk their responsibility to be only the agent of trust in a transaction; however, the consequences of their negligence are still felt to this day.

Furthermore, a dominant third party in any given industry poses a risk to become the 'gatekeeper' for that industry. This highly saturated centralisation, where trust is not a choice but a requirement, risks exclusion and monopoly. In the recent turmoil of events, the United States has threatened to shut down Iraq's access to the country's central bank held at the Federal Reserve Bank of New York where all funds of global oil sales are kept, depriving them from all the oil sale revenue, leading them to an economic crisis [40].

Even if the trusted central authority is honest, it poses risks to data manipulation by external parties such as hackers. A hacker may modify the vital information and cause significant losses without even being noticed. Consider, for example, if the hackers were to alter the expiry dates on the batches of milk. Valuable resource would be discarded and numerous may get sick for drinking the hazardous milk. Volkswagen's emission scandal is a recent example of data manipulation in order to pass the safety or legal requirement [34]. The same principle can be applied to medical institutions, banks and public services, leading to appalling consequences.

Breach in trust has a significant and lasting impact on the business, particularly on branding and reputation of the business. People will forget about the third party that was the main reason of the breach, but the brands will face ongoing trust issues.

5. Trust and Society

Trust in centralised entities is declining. According to a 2018 study by Ipsos Mori on a base of over 16,000 respondents, only 14% deemed government as trustworthy [41]. Similarly, media, oil and gas companies, banking and pharmaceutical companies were highly rated as untrustworthy. When the respondents were asked if 'it [bank and public sector] is open and transparent about what it does', only 26% and 23% agreed, respectively [41]. A 2015 study of Pew Research Center, USA, indicates that the public's trust in the federal government has been steadily declining since 1958 and it is at historically low levels with only 19% of Americans having reported to trust the government [42].

Not only the trust in organisations is at decline but the trust in people is declining too. The general social survey (GSS) has recorded a downward trend to the 'can people be trusted' category, over the past 32 years (Figure 1) (1972–2018, data available for 28 out of 32 years) [43]. Wilson & Rule found a prejudiced relationship between the perception of 'untrustworthiness' from facial appearance and death sentences given to convicted murderers, even for the people exonerated after originally being sentenced to death [44].

Higher level of trust has a positive casual effect on the efficiency of public services, tax compliance, anti-corruption and participation in civic activities [45]. On the contrary, lack of trust serves as a motivation for citizens to not comply with government demands and regulations. They may

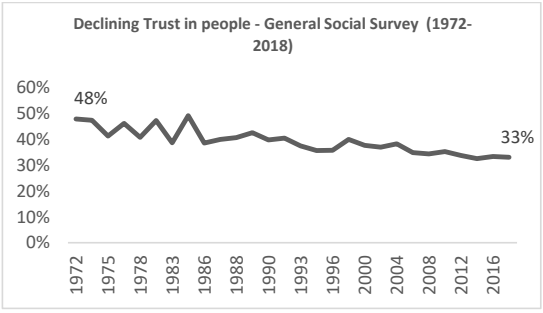


Figure 1. General social survey (GSS) 'Can people be trusted' (1972–2018 dataset). Declining trust among people with only 33% responding that they can trust other people as compared to 48% in 1972 [43].

actively resist government policies and make the government incapable of performing its tasks [46]. Tyler argues that trust helps reduce the public sector's administrative costs of control and enforcement by encouraging citizens to voluntarily comply and perform their due diligence [47].

The socio-political and technical indicators [2, 3, 4] are hauling up that BCT is ready for disruption and can flourish between the fissures between human and institutional behaviour. We call it 'digital disruption 2.0'. The first wave of online disruption saw the brick and mortar businesses being displaced by the digital intermediaries. The digital disruption 2.0 is challenging the whole notion of a 'trusted intermediary' and shifting trust from people and institutions to code and computers in impending industry 4.0 revolution.

6. When Can You Use a Blockchain?

Blockchains come with some intrinsic properties, given some degree of variation between public and private blockchains. Some of the key features of a blockchain are (1) decentralisation (transactions without a central authority), (2) persistency (very temper evident and strictly validated against the set rules), (3) anonymity (no central party keeping user's private information), (4) auditability (all transactions have a log) and (5) resiliency (no single point of failure) [48, 49] (see [49] for a literature review on the characteristics of blockchains). We must take a heuristic approach when designing systems and make use of the combination of these properties, if and as needed.

There has been a lot of debate about when a blockchain makes sense. Similar to the mid 1990s, when only a handful of people could predict the emergence of the behemoths like Google, Facebook and Amazon, we believe that it is too early to really conclude on the potential usability of the technology. The social shift, along with change in the user's perception and awareness would determine what ends up on the distributed, temper evident ledger. We believe that the 'killer apps' of the BCT are being conceived. These ideas will not be able to progress if we strictly evaluate them against the established technologies.

However, some of the key areas where most of the organisations can benefit from a blockchain-based solution are reduced verification costs, cost of exchanging value without relying on an intermediary, data integrity and reduction in frictions [50]

7. Public Service Perspective

As discussed in section 5, trust in public services and governments is decreasing. Public services can benefit from incorporating a decentralised infrastructure as a tool to gain the trust of the people. BCT can provide an infrastructure for exchanging information between public services and

significantly enhance the administrative function of the governments by reducing the complexity, cost and time in inter-governmental and public information exchange. Citizens can benefit from the increased automation, accountability, auditability and transparency of the information available on the public registries [51].

Ølnes et al suggest that BCT can be potentially used for any transaction or information exchange which involves government engagement [49]. Some of the potential use cases of BCT are secure information exchange, asset registry, both tangible assets like land and property and digital assets like reputation, health data, patents and ideas and inter/intra-governmental transactions [52]. BCT can increase government's efficiency and help in reducing corruption [53], improve digital security, privacy and enhance trust with its citizens [49]. Furthermore, BCT can improve data integrity both in terms of accuracy and consistency of the information, leading to error reductions and low infrastructure costs [54].

Table 1. Countries exploring BCT use cases worldwide with an aim of improving public services and trust with their citizens.

Government service	Country	Potential benefit
Land title registry	Georgia [55] [51], Sweden [56], United Kingdom [57], Ghana [58], South Africa [59], India [60]	Provenance, transparency
Birth certificates	India [61], Brazil [62]	Provenance, transparency
Academic/skill certificates	Malta [63] [51], Canada [64]	Provenance, efficiency
Digital identity	Switzerland [51], Luxembourg [51], Estonia [65]	Governance
Benefit management	The Netherlands [51]	Governance, transparency, efficiency
Remittance	Philippines [66]	Financial inclusion
Immigration services	Finland [67]	Governance
Voting	Sierra Leone [68]	Transparency, auditability, accountability
Business registry	Malta [69]	Governance, efficiency
E-government	Estonia [65], Dubai [70], Liberia [71]	Governance, efficiency, automation
Credit history	Sierra Leone [72]	Provenance
Bureaucratic processes/administration	China, Tanzania, Canada [73]	Transparency, auditability, reduce corruption
Clearing system for imports and exports	South Korea [74]	Efficiency, traceability
Digital currency	Tunisia, Ecuador [75]	Governance
Secure data exchange	Abu Dhabi (UAE) [70]	Digital security
Medical (organ donation and transplant)	UAE [70]	Efficiency
Taxation	China [76]	Transparency, compliance

Governments across the world acknowledge the potential of BCT to transform the public services and citizen's expectations and they have been actively exploring the BCT use cases to improve on the existing public services infrastructure. Table 1 lists some of the countries that have evaluated BCT projects to improve the services for its citizens.

We do not assume that BCT will completely eliminate the role of institutions or governments, but we believe that we will see a shift in the roles. While BCT can (to some extent) disintermediate the role of institutions in record keeping and establishing trust, we must appreciate the fact that BCT requires governance and regulatory frameworks to operate legitimately. Governments can act as trusted administrators who manage the registry and define transaction rules and regulations to ensure the functioning of the facility. Governments must remain the data stewards – accountable for running the operations and be accountable for any failures or issues [49]. BCT can act as a trust enabling technology layer, operating in conjunction with the existing technology stack.

Organisations globally are pushing for transparency and information sharing to provide better service and improved transparency. Section 35 of the recently passed Digital Economy Act (UK) encourages data sharing among public services to improve the public service delivery for the benefit of individuals or households and provide targeted public service [77]. Since the focus of this article is CH, we will only discuss the challenges that CH face to establish trust in the data that they hold, simultaneously improving transparency and accuracy in the processes of corporations and the activities of persons behind those corporations. The aim for addressing these challenges is to reduce fraud, money laundering, tax evasion and general bad behaviour.

About Companies House UK

CH is the UK's executive agency and the registrar of companies. All types of companies are incorporated and registered with CH and file-specific details, as per Companies Act 2006 [78]. The data held is of high importance to the UK's economy, and CH is aiming to improve the quality of the data that they hold, with a focus on increasing the transparency of UK corporate entities, and help combat economic crime [79]. CH recently consulted on a proposal regarding the newly proposed reforms. The reforms will require companies to disclose additional information which will be verified before acceptance and the steps to be taken to improve the exchange of intelligence between CH and UK Law Enforcement. The reforms will include knowing (1) who is incorporating, managing and controlling companies, (2) improving the usability and accuracy of data on the companies register, (3) ensuring compliance and protecting personal information on the register and (4) sharing intelligence and other measures to daunt abuse of corporate entities [79].

Here we investigate how BCT can improve the existing processes in CH and discuss three use cases that we have examined as part of our research partnership with CH. The use cases that we have chosen as part of the study are

1. Company incorporation,
2. Sharing information with law enforcement (LE) and
3. A blockchain-based legal entity identification and verification system that can add trust to the data collected and held by Companies House.

Company Incorporation

CH has a record of over 4 million limited companies registered in the United Kingdom and over 500,000 new companies are incorporated each year [80]. Each newly registered company gets an incorporation certificate as a proof that they are legally entitled to trade in the United Kingdom. The incorporation certificate is a public document and is only issued

once to a company in its lifetime. We believe that issuing a proof of the incorporation certificates on the blockchain can increase the trust in the certificate while simultaneously protecting the integrity of the certificate.

Moreover, the process can be easily integrated in the current workflow, since the only addition to the current certificate issuance process is committing a transaction with the hash of the document to the blockchain. Once the confirmation is received, the reference of the transaction is added to the metadata of the certificate and is made available for the user. For verification, the verifier can upload the certificate to the online portal. Proof of the transaction is obtained from the metadata of the document and verification is successful if a valid hash is found on the blockchain.

One could argue that the owner of the certificate should hold the private keys of the transaction to prove the ownership. However, we believe that this requires a lot more awareness and hinders the usability and acceptance of the scheme. The model discussed here is very similar to some of the current semi-automated verification processes and abstracts all caveats of the BCT from the end user.

Information Sharing With Other Public Services

A private-permissioned blockchain network can facilitate the sharing of confidential information among public services [81]. Smart contacts can be deployed for access control and data handling. We recommend not adding any confidential data to the blockchain but only adding a commitment or a proof to the network [82]. For example, consider a scenario where LE has to request data from CH regarding an ongoing investigation. LE shall submit a data protection request, requesting the data on the person. Upon successful verification, CH prepares the data, encrypts and uploads it to a safe storage such as cloud or IPFS [83]. CH will then encrypt the link to the data using LE's public key and post it on DLT along with the data hash for integrity checks. LE decrypts the link, verifies hash and accesses the data. A smart contract facilitating and governing the transaction will remove the link and data will be deleted once the requirement has been satisfied. Sharing information on a DLT provides a complete secure audit trail of the activity.

Identity System for Legal Entities

Accurately identifying legal entities on a global scale is a complex task, requiring significant amount of time, money and resources. There is no single open and up-to-date database that can provide all the required background information. This lack of information is partially responsible for the financial crisis, fraud and market abuse. Several initiatives have been taken to identify the global legal entities and their connections to each other. Established by the Financial Stability Board in June 2014, the Global Legal Entity Identifier Foundation (GLEIF) is the most renowned of all. GLEIF is tasked to support the implementation and use of the Legal Entity Identifier (LEI), with an aim of having a unique identity for every business [84]. A total of 1.4 million LEIs have been issued to the companies worldwide [85]. This number is only a small fraction of the companies registered worldwide. There are estimated 200 million registered companies globally; China alone has over 77 million registered companies. Less than 140,000 of the 4 million registered companies in the United Kingdom has an LEI [86]. The LEI is not global in a true sense since less than 1% companies globally have an LEI. Furthermore, companies and individuals will not always trust a centralised system managed by a third party. We propose a global company and individual identifier system that runs on the blockchain and benefits from the inherent security and privacy features of a cryptographically secured distributed ledger. We believe that a blockchain-based company and related person's network can be a potential solution for CH initiative on transparent and reliable data. The architecture proposed is based on the open source identity network, Sovrin [11] (Figure 2).

On an abstract level, identity is a composite of (1) identifiers that the subject has with different stakeholders, (2) self-asserted and verifiable claims and (3) proofs from others about the relation and interaction with others. We propose using self-asserted and verifiable claims [11] to establish trust among the interacting entities and the individuals controlling those entities. Blockchain network records the claims that a subject makes about themselves and their company, respectively. All relationships with stakeholders are also recorded as the public/private key pairs. The relationships can assign claims to the subject or the company. For example, Her Majesty Revenue and Customs (HMRC) can assert a claim about Bob's company that it has defaulted or CH can assert a claim about the records being up to date. These claims can then be used to make disclosures about the identity, which can be verified by the verification authority.

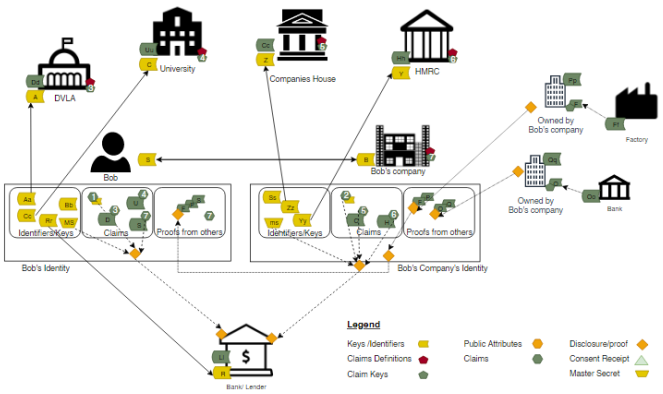


Figure 2. Different aspects of identity on the blockchain. Entities have identifiers, claims about identity attributes and proofs from others regarding their relationships. Relationships with other entities are recorded on the blockchain and entities collect verifiable claims about their identity. Solid lines represent relationships, whereas dotted lines represent a verifiable claim disclosure and the dashed line represents a delegated claim from a third party. The longer they are on the blockchain, the more verifiable claims they will collect from the relations they have on the blockchain. Entities can disclose verifiable claims to a third party, on need basis. Entities can mix and match certain aspects of their identities without revealing more than what is required. This helps in preserving privacy. Legend shows different relationships and proofs that an identity can have. Any participant in the network will have different identifiers that it uses to identify itself.

Data Sharing and Fraud Mitigation

A network of this capacity can be easily scaled to hundreds if not thousands of nodes. Data can be shared easily between governments, LE and other stakeholders such as insurance agencies. Privacy of the entity is preserved using Zero Knowledge Proofs (ZKP) and relevant data can be disclosed easily. On a blockchain identity infrastructure with verifiable claims asserting the truth about an entity's identity, fraud becomes extremely difficult. Department of Work and Pensions (DWP), CH, HMRC, banks and so on will all see Bob as the director of the company and forging Bob's identity would be nearly impossible in this trust network (Figure 2). Furthermore, we propose a relative ranking-based system that gives a score to each legal entity based on their relations and interactions on the blockchain (Figure 3). This also makes the KYC (know your customer) and on-boarding process easy. Businesses can significantly benefit from such a system that cuts their KYC and on-boarding process from weeks to minutes, not to mention the cost savings that come with it.

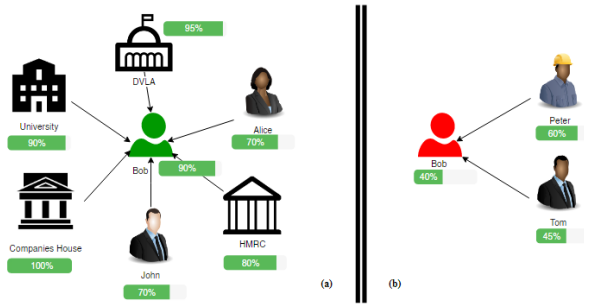


Figure 3. (a) Real Bob with several trusted verifiable claims on the left and (b) imposter Bob with few claims about his identity. If Bob is proved to be a malicious person, both Tom and Peter risk losing their score too, hence they will have to vote for the real Bob in order to preserve their own identity score.

Inter-company Trust

An infrastructure like bitcoin for intercompany settlements can be very helpful as a source of trust in today's accounting structure. It can be used to verify the integrity of records, providing a complete audit trail. Companies can write transactions directly into a joint register instead of keeping separate records based on the receipts of transactions. BCT enables the creation of an interlocking system of durable accounting records, making the destruction or falsification of information to conceal activity practically impossible [87].

BCT can be a digital equivalent of a notary. This will save significant time for the verifiers as they need not dig into piles of paper to verify the books. Transaction becomes the evidence itself.

8. Conclusion

BCT could drastically reduce the cost of trust, introduce new social constructs and pave the way to new structures of economic organisations. While we appreciate the fact that BCT has a long way to go before it can be widely adapted, we argue that different aspects of BCT should be utilised in business models where it can add value. A more appropriate question could be 'do you want to use a trusted third party?' rather than 'can you use a trusted third party?' DLTs such as BCT are paving the path of a new secure, honest and level-playing field for all and we shall see mass economies emerging from this new form of trust model.

We took three use cases from Companies House UK's business processes and mapped them to the properties of BCT, demonstrating how adding BCT to the existing Tech Stack can add an additional level of security to CH data, while also improving on the trust in the data held at CH. We believe that a solution utilizing digital identities and verifiable claims can truly transform the trust factor in companies and Companies House data and add greater value to the data acquired by the relevant authorities while simultaneously making data sharing and verification easy.

References:

[1] M. Walport, "Distributed ledger technology: Beyond block chain," 2015.
[2] J. A. Schumpeter, Capitalism, socialism and democracy. Harper & Brothers, 1942.
[3] C. Perez, Technological revolutions and financial capital. Edward Elgar Publishing, 2003.
[4] C. Perez, "Technological Revolutions and Techno-Economic Paradigms," Cambridge J. Econ., vol. 34, no. 1, pp. 185–202, 2010.
[5] C. Baden-Fuller and S. Haefliger, "Business models and technological innovation," Long Range Plann., vol. 46, no. 6, pp. 419–426, 2013.
[6] G. Zyskind and A. S. Pentland, "Decentralizing Privacy : Using Blockchain to Protect Personal Data."
[7] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A Blockchain-based Personal Data and Identity Management System," Proc. 52nd Hawaii Int. Conf. Syst. Sci., vol. 6, pp. 6855–6864, 2019.
[8] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38437–38450, 2018.
[9] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016, pp. 25–30, 2016.
[10] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," Conf. Open Innov. Assoc. Fruct, vol. 2017-April, pp. 534–539, 2017.
[11] W. Paper and S. Foundation, "Sovrin TM : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust A White Paper from the Sovrin Foundation," no. January, 2018.
[12] J. Fenn, M. Raskino, and B. Burton, "Understanding Gartner's Hype Cycles," 2013.
[13] "Worldwide Semiannual Blockchain Spending Guide." [Online]. Available: https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1842. [Accessed: 04-Dec-2019].
[14] T. Koens and E. Poll, "What Blockchain Alternative Do You Need?," pp. 113–129, 2018.
[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Www.Bitcoin.Org, p. 9, 2008.
[16] K. Arrow, The limits of organization. 1974.
[17] M. Watson and M. L. Watson, "Can There Be Just One Trust? Can There Be Just One Trust? A Cross-Disciplinary Identification Of Trust Definitions And Measurement," 2005.
[18] R. C. Mayer, J. H. Davis, and F. David Schoorman, "An Integrative Model of Organizational Trust," 1995.
[19] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," Acad. Manag. Rev., vol. 23, no. 3, pp. 393–404, 1998.
[20] L. Cerna, "Trust: What it is and why it matters for governance and education," OECD Educ. Work. Pap., no. 108, pp. 0–66, 2014.
[21] M. Granovetter, "Economic Action and Social Structure: The Problem of Embeddedness," Am. J. Sociol., vol. 91, no. 3, pp. 481–510, Nov. 1985.
[22] E. Erikson, Identity: Youth and crisis. WW Norton & Company, 1968.
[23] S. P. Shapiro, "The Social Control of Impersonal Trust," Am. J. Sociol., vol. 93, no. 3, pp. 623–658, Nov. 1987.
[24] T. Yamagishi, K. S. Cook, and M. Watabe, "Uncertainty, trust, and commitment formation in the United States and Japan," Am. J. Sociol., vol. 104, no. 1, pp. 165–194, 1998.
[25] L. Z.-R. in organizational behavior and undefined 1986, "Production of trust: Institutional sources of economic structure, 1840-1920," ci.nii.ac.jp.
[26] R. E. Miles and W. E. D. Creed, "Organizational forms and managerial philosophies-a descriptive and analytical review," Res. Organ. Behav. AN Annu. Ser. Anal. ESSAYS Crit. Rev. VOL 17, 1995, vol. 17, pp. 333–372, 1995.
[27] A. Saxenian, "Beyond boundaries: Open labor markets and learning in Silicon Valley," boundaryless career A new Employ. Princ. a new Organ. era, vol. 23, p. 39, 1996.
[28] N. Stephens, I. Khan, and R. Errington, "Analysing the role of virtualisation and visualisation on interdisciplinary knowledge exchange in stem cell research processes," Palgrave Commun., vol. 4, no. 1, Dec. 2018.
[29] B. Nooteboom, Trust: Forms, foundations, functions, failures and figures. Edward Elgar Publishing, 2002.
[30] C. Howorth and A. Moro, "Trustworthiness and the Cost of Credit: An Empirical Study of SMEs and Small Banks in Italy," Small Bus. Econ., vol. 39, no. 1, pp. 161–177, 2012.
[31] M. T. Hannan and J. Freeman, Organizational ecology. Harvard university press, 1989.
[32] J. W. Meyer and B. Rowan, "Institutionalized Organizations: Formal Structure as Myth and Ceremony," Am. J. Sociol., vol. 83, no. 2, pp. 340–363, Sep. 1977.
[33] O. E. Williamson, "Calculativeness, Trust, and Economic Organization," J. Law Econ., vol. 36, no. 1, Part 2, pp. 453–486, Apr. 1993.
[34] M.-D. Seidel, "Questioning Centralized Organizations in a Time of Distributed Trust," J. Manag. Inq., vol. 27, pp. 40–44, 2018.

[35] M.-D. L. Seidel and H. R. Greve, "Emergence: How novelty, growth, and formation shape organizations and their ecosystems," in Emergence, Emerald Publishing Limited, 2017, pp. 1–27.
[36] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," SSRN Electron. J., Jan. 2016.
[37] A. Zwitter and J. Hazenberg, "Decentralized Network Governance: Blockchain Technology and the Future of Regulation," Front. Blockchain, vol. 3, p. 12, Mar. 2020.
[38] "FactCheck: how many bankers were jailed for their part in the financial crisis? – Channel 4 News." [Online]. Available: https://www.channel4.com/news/factcheck/factcheck-how-many-bankers-were-jailed-for-their-part-in-the-financial-crisis. [Accessed: 03-Jan-2020].
[39] M. J. Casey and P. Vigna, "In blockchain we trust," Technol. Rev, vol. 121, pp. 10–16, 2018.
[40] I. Talley and I. Coles, "U.S. Warns Iraq It Risks Losing Access to Key Bank Account if Troops Told to Leave - WSJ," 2020. [Online]. Available: https://www.wsj.com/articles/u-s-warns-iraq-it-risks-losing-access-to-key-bank-account-if-troops-told-to-leave-11578759629. [Accessed: 13-Jan-2020].
[41] G. Skinner et al., "Trust: The Truth?," 2019.
[42] "1. Trust in government: 1958-2015 | Pew Research Center." [Online]. Available: https://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/. [Accessed: 02-Jan-2020].
[43] "GSS Data Explorer | NORC at the University of Chicago," 2018. [Online]. Available: https://gssdataexplorer.norc.org/variables/441/vshow. [Accessed: 08-Jan-2020].
[44] J. P. Wilson and N. O. Rule, "Facial Trustworthiness Predicts Extreme Criminal-Sentencing Outcomes.," Psychol. Sci., vol. 26, no. 8, pp. 1325–31, Aug. 2015.
[45] R. La Porta, F. Lopez-de-Silane, A. Shleifer, and R. Vishny, "Trust in Large Organizations," Cambridge, MA, Dec. 1996.
[46] J. N. Jr, … P. Z. don't, and U. 1997, "Conclusion: Reflections, conjectures, and puzzles," in Harvard University Press Cambridge …, pp. 276–277.
[47] T. T.-T. and governance and undefined 1998, "Trust and democratic governance," in Russell Sage Foundation New York, 1998, p. 290.
[48] Z. Xie, S. Dai, H.-N. Chen, and X. Wang, "Blockchain challenges and opportunities: a survey," Int. Congr. Big Data, vol. 14, no. 4, pp. 352–375, 2018.
[49] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," Gov. Inf. Q., vol. 34, no. 3, pp. 355–364, 2017.
[50] P. Michelman, "Seeing Beyond the Blockchain Hype."
[51] D. Allessie and M. Sobolewski, "Blockchain for digital government An assessment of pioneering implementations in public services."
[52] B. U. Enzo et al., "State of the art in the use of emerging technologies in the public sector," no. 3, 2019.
[53] H. Hyvärinen, M. Risius, and G. Friis, "A blockchain-based approach towards overcoming financial fraud in public sector services," Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 441–456, 2017.
[54] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," New Econ. Wind., pp. 239–278, 2016.
[55] Q. Shang and A. Price, "A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects," Innov. Technol. Governance, Glob., vol. 12, no. 3–4, pp. 72–78, Jan. 2019.
[56] G. Chavez-Dreyfuss, "Sweden tests blockchain technology for land registry," 2017.
[57] "Could blockchain be the future of the property market? - HM Land Registry." [Online]. Available: https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/. [Accessed: 12-May-2020].
[58] G. Eder, "Digital Transformation: Blockchain and Land Titles."
[59] "South Africa pilots blockchain for property registry - Ledger Insights - enterprise blockchain." [Online]. Available: https://www.ledgerinsights.com/south-africa-pilots-blockchain-property-registry/. [Accessed: 12-May-2020].
[60] V. Thakur, M. N. Doja, Y. K. Dwivedi, T. Ahmad, and G. Khadanga, "Land records on Blockchain for implementation of Land Titling in India," Int. J. Inf. Manage., vol. 52, p. 101940, Jun. 2020.
[61] "A 1st in Bengal, baby gets blockchained birth certificate | India News - Times of India." [Online]. Available: https://timesofindia.indiatimes.com/india/a-1st-in-bengal-baby-gets-blockchained-birth-certificate/articleshow/67170551.cms. [Accessed: 12-May-2020].
[62] "Parceria entre IBM, Hospital e Cartório faz registro de nascimento totalmente em blockchain." [Online]. Available: https://cointelegraph.com.br/news/brazil-birth-certificate-and-blockchain. [Accessed: 12-May-2020].
[63] "Pilot project extended: All educational certificates to be issued through blockchain - The Malta Independent." [Online]. Available: https://www.independent.com.mt/articles/2019-02-21/local-news/Pilot-project-extended-All-educational-certificates-to-be-issued-through-blockchain-6736204012. [Accessed: 04-May-2020].
[64] "Canada pilots blockchain staff records – Government & civil service news." [Online]. Available: https://www.globalgovernmentforum.com/canada-pilots-blockchain-staff-records/. [Accessed: 12-May-2020].
[65] e-estonia.com, "Frequently Asked Questions: Estonian blockchain technology," 2017.
[66] "Blockchain Payments: Project i2i Case Study." [Online]. Available: https://consensys.net/blockchain-use-cases/finance/project-i2i/. [Accessed: 12-May-2020].
[67] "How Blockchain Is Kickstarting the Financial Lives of Refugees | MIT Technology Review." [Online]. Available: https://www.technologyreview.com/2017/09/05/149330/how-blockchain-is-kickstarting-the-financial-lives-of-refugees/. [Accessed: 12-May-2020].
[68] Agora, "Swiss-based Agora powers world's first ever blockchain elections in Sierra Leone," p. 8848, 2018.
[69] "Registry of Companies to be first agency in the world run by a Blockchain-based system - The Malta Independent." [Online]. Available: https://www.independent.com.mt/articles/2019-05-08/local-news/Registry-of-Companies-to-be-first-agency-in-the-world-run-by-a-Blockchain-based-system-6736207848. [Accessed: 13-May-2020].
[70] "Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates In collaboration with the Dubai Future Foundation," 2020.
[71] "Medici Land Governance Signs MOU with Liberia's Ministry of Finance and Development Planning for Pilot Project for E-Government Processes Nasdaq:OSTK." [Online]. Available: https://www.globenewswire.com/news-release/2019/06/10/1866326/0/en/Medici-Land-Governance-Signs-MOU-with-Liberia-s-Ministry-of-Finance-and-Development-Planning-for-Pilot-Project-for-E-Government-Processes.html. [Accessed: 13-May-2020].
[72] "San Francisco crowdfunder Kiva sets up Sierra Leone credit database - Reuters." [Online]. Available: https://www.reuters.com/article/us-leone-kiva/san-francisco-crowdfunder-kiva-sets-up-sierra-leone-credit-database-idUSKCN1VB262. [Accessed: 13-May-2020].
[73] "Government of Canada exploring the potential of Blockchain technology - Bitaccess." [Online]. Available: https://bitaccess.ca/blog/government-of-canada-exploring-the-potential-of-blockchain-technology/. [Accessed: 12-May-2020].
[74] "South Korea Customs Takes the Lead in Blockchain Technology Application---South Korea Customs Introduces Blockchain Technology in the Import and Export Shipping Management | 中国航海学会 China Institution of Navigation." [Online]. Available: http://www.cinnet.cn/en/news/3364-south-korea-customs-takes-lead-blockchain-technology-application-south-korea-customs-introduces-blockchain-technology-import-and-export-shipping-management.htm. [Accessed: 12-May-2020].
[75] "State-Issued Digital Currencies: The Countries Which Adopted, Rejected or Researched the Concept." [Online]. Available: https://cointelegraph.com/news/state-issued-digital-currencies-the-countries-which-adopted-rejected-or-researched-the-concept. [Accessed: 13-May-2020].
[76] "Beijing Administration of Taxation, State Administration of Taxation." [Online]. Available: http://beijing.chinatax.gov.cn/bjsnjwz/xxgk/tzgg/202003/t20200302_447896.html. [Accessed: 12-May-2020].
[77] Digital Economy Act 2017 - Section 35: Disclosure of information to improve public service delivery. United Kingdom: Queen's Printer of Acts of Parliament, 2017.
[78] Companies Act 2006 - CHAPTER 46. United Kingdom, 2006.
[79] "Corporate transparency and register reform - GOV.UK," 2019. [Online]. Available: https://www.gov.uk/government/consultations/corporate-transparency-and-register-reform. [Accessed: 28-Jun-2019].
[80] "About Companies House - Companies House." [Online]. Available: https://companieshouse.blog.gov.uk/about-companies-house/. [Accessed: 20-Jan-2020].
[81] A. Shahaab, B. Lidgey, C. Hewage, and I. Khan, "Applicability and

Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review," IEEE Access, vol. 7, pp. 43622–43636, 2019.
[82] A. Shahaab, R. Maude, C. Hewage, and I. Khan, "Managing Gender Change Information on Immutable Blockchain in Context of GDPR," vol. 3, no. 1, 2020.
[83] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXiv Prepr. arXiv1407.3561, 2014.
[84] "This is GLEIF – About GLEIF – GLEIF." [Online]. Available: https://www.gleif.org/en/about/this-is-gleif. [Accessed: 28-Jun-2019].
[85] "LEI Statistics – Global LEI Index – LEI Data – GLEIF." [Online]. Available: https://www.gleif.org/en/lei-data/global-lei-index/lei-statistics. [Accessed: 28-Jun-2019].
[86] "UK Companies with LEI– GLEIF." [Online]. Available: https://www.gleif.org/en/lei/search/#filters%5B0%5D%5Bfield%5D=Entity.LegalAddress.Country&filters%5B0%5D%5Boperator%5D=%3D%3D&filters%5B0%5D%5Bvalue%5D=GB. [Accessed: 28-Jun-2019].
[87] "Blockchain Technology A game-changer in accounting?" https://www.finyear.com/Blockchain-Technology-A-game-changer-in-accounting_a35816.html

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Author's contribution (confirm you are the main author responsible for writing the manuscript, collecting data, proof reading etc)
AS designed and coordinated this research and prepared the manuscript in its entirety under the supervision and guidance of RM, CH and IK.

Funding:
"This research has been supported by Knowledge Economy Skills Scholarships (Scholarship # CMK219) a major pan-Wales operation supported by the European Social Funds through the Welsh Government. The scholarship was also partly funded by Companies House, UK."

Acknowledgements:
None declared.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(5)2020

Privacy Laws, Genomic Data and Non-Fungible Tokens

[1]Daniel Uribe and [2]Gisele Waters
[1]Genobank.io, USA
[2]Engineering Hearts™, USA
Correspondence: daniel@genobank.io
Received: 19 April 2020 **Accepted:** 15 May 2020 **Published:** 30 May 2020

Abstract

This article analyses the main legal requirements in the California Consumer Protection Act (CCPA), general data protection regulation (GDPR) and the intersections between privacy laws, genomic data and smart contracts (such as fungible and non-fungible tokens [NFTs]). The CCPA and GDPR laws impose several restrictions on the storing, accessing, processing and transferring of personal data. This has generated some challenges for lawyers, data processors and business enterprises engaged in blockchain offerings, especially as they pertain to high-risk data sets such as genomic data. The technical features of NFT, distributed storage and wallets to trace and govern genomic (DNA) data sets will allow data donors to establish digital ownership and control in line with privacy laws using 'programmable privacy smart contracts'. To be legally compliant, the design of blockchain value propositions should include privacy-by-design capabilities in the smart contract coding language itself. This article describes three domains (privacy laws, genomics and NFTs) and begins to explore how data engineers can address the challenges of coding privacy laws, the legal requirements into smart contracts. This current approach focuses on NFTs and genomic data requirements which include the selection of genetic metadata borrowing from developing ERC specifications and their programming logic. Programmable privacy is a unique way to write and design computer code, which can automatically check the legal compliance of the smart contract in a trust-less and decentralised way. We exemplify the approach by describing the conceptual value proposition of Genobank.io, a privacy-preserving genomic data platform.

Keywords: *Blockchain, biobanking, biometric, smart contracts, California Consumer Protection Act, privacy, programmable, distributed storage, IPFS, genomics, DNA, data processor, privacy law, GDPR, CCPA, non-fungible tokens (NFTs), fungible tokens, ERC998, ERC1155, ERC721, data sovereignty, Ethereum*

1. Introduction

The battle of legitimate authority and control over genomics [1] data introduces a substantial legal and computational burden on data privacy. Consumers are already suing doctors [2], hospitals and data processors to hold them liable for how they offer, interpret and counsel patients about genetic tests. In this article, we introduce one use case, Genobank.io [3], which aims to protect consumer privacy by engaging stakeholders at the intersection of privacy law, smart contracts [4] [5] using non-fungible tokens (NFTs) [6] [7] and genomics.

There are growing challenges in this complex ecosystem that can only be solved collaboratively [8]. Subject matter experts in all three domains (law, genomics and smart contracts) will be dependent on each other to achieve success and avoid risk. Here, the concepts, interrelationships and the implications of a specific use case in genomics: the implications of the California Consumer Privacy Act [9][10] (CCPA) and the European Union's general data protection regulation [11] (GDPR) to smart contracts, specifically NFTs in the blockchain [12], are presented. The Consumer Online Privacy Act (COPRA) [13] is also briefly overviewed. Two questions are posed as a starting point for stakeholder collaboration:

1. The human challenge: How do stakeholders with conflicting interests work together to ensure privacy laws protect the most personal, private, and sensitive data[1] derived from biospecimens [14]?
2. The technology challenge: How can privacy laws be coded [15] into smart contracts to protect high-risk data with strong consent and privacy mechanisms? In other words, how do you embed laws of the physical world into machine code with privacy as the highest value?

There are about 8 billion people on the planet and more than 26 million [16] have already analysed their DNA. Approximately a million people worldwide have had their whole genome sequenced [17].

> *So many people have had their DNA sequenced that they have put other people's privacy at risk. [18]*

On the other hand, 99% [14] of the world's genetic information has *yet* to be produced. Those global statistics represent billions of dollars in marketplace opportunity [19] and probably an equally large risk [20] [21] in liability. How the opportunities and risks get defined in the next decade will be led by stakeholders working together across domains in law, genomics and technology.

Inevitable problems will arise if companies do not address the form and function of their technology solutions to face international and local data-privacy laws [22] [23], especially in the field of genomics. To create a fair and more secure marketplace for genetic information, privacy laws can be applied to the use of blockchain with NFTs (a type of smart contract). To help mitigate the gaps and challenges, stakeholders can also work together in transdisciplinary [24] ways that begin to create a common language [25] of understanding across the three domains of privacy laws, genomics and smart contracts. This article is a preliminary effort towards one of the much-needed stakeholder conversations and collaborations. This is a long-term endeavour where lawyers, data processors, genomic researchers and data subjects can define, together, what data practices and governance will be in the future.

At the intersection of the three domains, business enterprise is beginning to address this challenge by engineering various iterations of privacy-by-design offers and more specifically by engineering *privacy by blockchain*

design [26] [27]. In the latter, solutions can be GDPR compliant and also include additional legal privacy requirements with strategic smart contract terms and conditions. These new business models are helping to raise data protection levels and aim to give back data ownership to individuals. Specifically, one such enterprise, Genobank.io, has focused on bringing smart contracts such as NFTs that combine unique value-added architectures to the privacy-by-design proposition for genomic data. Details are shared later; first, we introduce the primary concepts of the three domains.

2. Three domains: collaboration required

Privacy laws

The European Union's GDPR went into effect on 25 May 2018 and a similar law in California, the world's fifth largest economy, the CCPA, went into effect on 1 January 2020. The newest privacy legislation from the U.S. Congress is COPRA, a Federal Bill aimed at protecting the privacy of consumers online at the national level. If this Bill crosses the finish line in the future, it would finally strengthen the Federal Trade Commission's ability to enforce digital privacy protections. But other similar Bills introduced in the past have never made it. Regardless, international and local privacy laws are keeping many privacy and security officers awake at night. Those concerns will not be alleviated unless stakeholders work together on how to address the requirements and specifications for policy and practice.

A few legal experts have coined the CCPA law as 'GDPR *Lite*'. But others suggest the CCPA is *not Lite* [28] at all and there is much more to do with the CCPA than previously believed. Some privacy lawyers say that companies who have already addressed the requirements of the GDPR have *a lot more* to prepare in order to address the higher requirements in the CCPA. The CCPA intends to provide California residents with the rights to:

1. know what personal data is being collected,
2. know whether it is being sold or disclosed and to whom,
3. refuse the sale of their personal data,
4. access their personal data,
5. request a business delete any personal data,
6. and not be discriminated against for exercising their privacy rights.

These six essential rights are part of the new CCPA challenges that privacy lawyers, technologists, genomic researchers and data processors are faced with today. The new law also sets penalties of $2,500–$7,500 per violation [23] and a private right of action to individuals affected by a breach caused by a lack of reasonable security measures. Due to the provision of statutory damages, the risk of litigation [29] is very significant. Under the CCPA, an entity qualifying as a 'business' must also provide seven protections. For example, business must provide disclosures regarding the sale of personal information collected from or about covered consumers (id. § 1798.110(a), an opt-in requirement before selling a minor's personal information (id. § 1798.120(c), the ability for covered consumers to access and/or delete personal information collected from or about them (id. §§ 1798.105), and must also implement measures to prevent discrimination against consumers who exercise their rights under the CCPA (id. § 1798.125) among others.

A few of the conditions required by the CCPA suggest a substantially different way of doing business and a higher threshold for data governance than has been required previously. The law also expands upon *what* personal information is and *how* it is used by businesses.

Under the CCPA, personal data (identifiers, geolocation, internet activity, education and employment information among others) also includes biometric information. Biometric information is defined as 'an individual's physiological, biological, or behavioural characteristics, including deoxyribonucleic acid (DNA), that can be used singly or in combination with other identifying data, to establish identify' [9]. Examples such as imagery of the iris, retina, fingerprint, face, hand, palm, voice recordings, keystroke patterns, exercise data, gait patterns and *even sleep* are protected by the law.

Businesses should take heed, if personal or biometric data are gathered by a company, without notice, it is still considered private personal information and subject to legal protection. These new considerations on what kind of data and under what conditions the data are protected under the law sets a higher bar for data governance.

The newest privacy law proposed at the federal level may extend consumer protections even further. It was introduced by Senators Cantwell, Schatz, Klobuchar and Markey on 26 November 2019. COPRA is written to provide consumers with foundational data-privacy rights, creating strong oversight mechanisms and establishing meaningful enforcement of the same. This new legislation, as introduced, suggests that companies must not collect more information than they 'reasonably' need to function. COPRA is tremendously ground-breaking as proposed [30] and could, *if passed*, create the need for substantial liability and risk resource allocation in the future. The basic tenets of this new law include extended data-privacy rights (Title I), augmented oversight and responsibility (Title II) including a section on digital content forgeries and some added legal traction with Title III that adds miscellaneous sections on enforcement, civil penalties, authorisation of appropriations and severability among others.

The following genomic and digital data are considered *biometric information* that is to be protected online by the COPRA:

(i) fingerprints.
(ii) voice prints.
(iii) iris or retina scans.
(iv) facial scans or templates.
(v) deoxyribonucleic acid (DNA) information; and
(vi) gait.

Similar to CCPA, gait is also included; a person's manner of walking is protected biometric information. Excluded are writing samples, written signatures, photographs, voice recordings and demographic data. Also excluded are physical characteristics such as height, weight, hair colour and eye colour, provided that such data is *not used* for the purpose of identifying an individual's unique biological, physical or physiological characteristics.

COPRA would go further than past laws, in that it defines the terms 'collect' and 'collection' to mean buying, renting, gathering, obtaining, receiving, accessing or otherwise acquiring covered data by any means, including by passively or actively observing the individual's behaviour. The CCPA and COPRA are huge shifts in regulation and data governance towards protecting the rights of consumers as opposed to allowing any collection and use of consumer data for a company's own benefits.

Implications

All laws [31] are meant to protect general safety and ensure our rights as citizens against abuses by other people, by organisations, and by the government itself. Laws do this by requiring specific behaviours and prohibiting others. The CCPA as enacted will 'nudge' [32] and require companies to act differently. If enacted, COPRA, as the next-generation regulation, will push the 'nudging' further. As privacy lawyers, data processors, genomic researchers and DNA donors consider a path forward, we suggest stakeholders collaborate on how to manage the opportunities and risks to balance public and private interests. It is inevitable that the implementation of the CCPA (enacted law) will bring about drastic challenges to companies and developers using the blockchain, especially in regard to genomics.

Genomics

Genomics [33] [34] is a domain within genetics that concerns the sequencing and analysis of an organism's genome. It is an is an interdisciplinary field of biology focusing on the structure, function, evolution, mapping and editing of genomes. Experts in genomics seek to complete DNA sequences beyond just partial analyses in order to perform genetic mapping that can help understand disease. A genome is a complete set of DNAs including all genes in one organism. Due to the highly sensitive nature in the uniqueness of genomic data, privacy requirements are complex transaction-laden systems with layers of health information that need both legal and computational privacy protection. Privacy protections are only beginning to gain solid ground in the United States and have yet to be fully realised.

Next-generation sequencing and genome editing have helped to make medicine more precise and efficient, especially regarding disease diagnostics and treatment. But the rapid development can only be realised by the *aggregation and analysis of people's genomic and health data* at scale. Efficient processing of very large-scale genomic data sets creates risk in the marketplace of biometric information. For the most part, DNA donors have been left powerless [35] [36] without any control over their own personal genetic profiles, essentially left without sovereignty. Data sovereignty is the concept that information, which has been converted and stored in binary digital form, is subject to the laws of the country in which it is located. The CCPA, Health Insurance Portability and Accountability Act (HIPAA) [37] and the Genetic Information Non-discrimination Act (GINA) [38] are the first set of laws in the United States that are beginning to provide protection and sovereignty. But the global wars over genetic information [39] [40] have only just begun and case histories, in the United States for example, reflect the struggles that the private and public sectors continue to have with gaps and challenges to the four corners of the law.

With newer and stronger privacy laws, the government is approximating prudence [41] and protection for the general safety and security of its citizens. But technology providers can go further. The lingering gaps in regulation add persuasive motivation to ethical technology leaders to move beyond the minimal requirements of the law towards *ethical best* practices [42] [43]. Working together with regulators on ethical data governance and understanding, they can provide a value proposition that both protects the consumer and provides a marketplace competitive advantage. One does not have to exclude the other. Rapid developments in the aggregation and analysis of people's genomic and health data at scale *can* benefit individuals, the public and the private sectors *simultaneously*.

The new laws imposed and the plethora of lawsuits that businesses are enduring indicate, from the individual's perspective, that the CCPA and the like may not go far enough, yet, to protect an individual's biometric data [39] [44]. From the enterprise perspective, the risk of liability from intended, unintended and even derivative attempts at aggregation of de-identified biometric data to identifiable databases should be at least one reason to borrow from the spirit of the law and its legal premise to create privacy-by-design solutions with grit. Using NFTs *for genomics data may give both the individual and the enterprise a way to work together on balancing* disparate, indeed often conflicting interests. The use of NFTs to address this challenge will be explained shortly.

Blockchain

A blockchain [45] is a time-stamped series of records (like a record in a spreadsheet but written only once) that is managed by a cluster of computers not owned by any single entity. Blocks of data (i.e. block) are secured and bound to each other like a chain using cryptographic principles such as confidentiality, authentication, integrity and non-repudiation [46]. All data stored on the blockchain have a common history available to all network participants. With this mechanism, the chances of fraudulent activity or duplications is eliminated without the need of third-party intermediaries [47].

Otherwise known as a distributed public ledger [48] [49], a blockchain tracks assets and transaction records so that each data block contains a unique hash 'tag' (digital fingerprint/signature) and time-stamped batches of recent transactions plus a hash of the previous block [50]. Each record with an encrypted digital signature proving its authenticity in the blockchain is tamper proof and cannot be changed. Blockchain and smart contracts can help counter problems such as imbalances in data control, information islands, data tampering, theft, abuse, data leaking, grey data transactions and missing records [50]. As with other technologies, blockchain has augmented [51] its bandwidth and expanded its capacity.

There are four [52] generations of current blockchains across many industries [53] worldwide [54]. The use cases expand daily in healthcare [55] [56]. On top of privacy laws nudging new business behaviour, in the healthcare space, providers are already answering strong calls to give easy access and control of personal healthcare records to the patient. But a review of the usage of blockchain technology in healthcare reveals that a patient's sovereignty, privacy and security [57] is not the most prevalent foci necessarily. The vast majority of blockchain applications in healthcare have been implemented to address interoperability and the substantial siloed data structures among diverse organisations. This is why decentralised, immutable ledgers like the blockchain provide more portable, interoperable mechanisms for the correct processing and secure sharing of data [21] [58] [59].

To share medical data, and more importantly highly sensitive genomic data securely, it is required that parties agree on the structure and semantics of data sharing [50]. Again, the human challenge to using technology optimally is represented here. Taking full advantage of the promise blockchain and smart contracts offer to computational genomics [1] [43] [60] is a fit-for-purpose that should be taken seriously by collaborating at domain intersections. Implementing privacy laws in the genomic data ecosystem is also a socio-technical challenge, not just a technical one. Furthermore, the maturity of the blockchain field is timely now in consideration of the greater need to manage vast quantities and different kinds of data (e.g. biobanking and biometric data) that require inviolable privacy parameters [59] [61]. Although many blockchain applications are still in conceptual stages testing various aspects of the technology, these more complex requirements for security demonstrate a need for the added transparency, confidentiality and programmable privacy in smart contracts [61] [62].

Self-executing computer protocols such as smart contracts execute agreements based on computer algorithms between two or more parties while creating an indisputable record of transactions associated with granting and revoking access [63] to a data (cryptocurrency) wallet. To ensure control, data transactions are signed by the owner using a private key [1] [64]. Private keys are created when users create an account (crypto data wallet) on any Web3 decentralised platform. A crypto data wallet usually has two main purposes. The first is to be able to easily share your public address through the internet and second to securely store the corresponding private key(s). Private keys can be encrypted or unencrypted as decided by the level of security offered by the blockchain platform.

The main idea behind using a crypto data wallet for genomic data is to introduce a novel alternative for users to regain data sovereignty with the support of privacy laws. Data wallets will enable data subjects to become data custodians while interacting with a genomic data processor (labs or researchers, for example) without losing any control or ownership. Unlike when companies such as 23&Me sell an ancestry and health report to a specific consumer, they claim ownership and establish control over a consumer's genomic data. In contrast, a DNA data wallet allows users to temporarily grant access to a genomic data processor so they can execute an interpretation algorithm or other analyses. These analyses are governed

by a smart contract that can be programmed to destroy or delete any digital computer instance that was created during the data processing for privacy purposes.

In other words, all instances of virtual machining can be deleted or destroyed by the terms and conditions of the smart contracts selected. This would be an equivalent to self-serving a consumer's right to be forgotten as a data subject/owner in GDPR and CCPA terms, respectively. There is no need for the data owner to keep a copy of the analytics or algorithms used for a report and there is no need for 23&Me to keep a copy of the data owner's DNA. Both parties are satisfied and protected. There is no justification or reason for the data owner to keep any IP from the data processor and no justification for the processor to keep a copy of the data owner's DNA. Then by integrating the terms and conditions of privacy laws into smart contracts with the specifications of NFTs, we suggest this combination of programmable privacy could be a novel and valuable form of next-generation privacy-preserving [65] technology.

This could dramatically change the status quo of data custodianship. Currently, the reality is data owners give away their rights, their custody and ownership to their DNA data or sell it for cents on the dollar [66] [67]. We argue crypto data wallets in combination with smart contracts, using NFTs, can disrupt the status quo of data ownership and governance.

All together, these mechanisms can facilitate a CCPA and GDPR compliant data management system by encoding in the smart contract a set of rules that ensure privacy for consumer-sensitive data. In essence, smart contracts provide better security performance than traditional contract law because they are encoded and written in such a way that they guarantee the execution of explicitly specified conditions [5] [44].

Risks

With broad opportunities come many risks. Inherent in any technology innovation is the absence of time and conditions that help stress test the boundaries of any new applications. Here, two primary risks with these smart contracts will be addressed in the limited time and space allowed. One is the potential that private keys are lost or mishandled. The second is the security and privacy risks when the data is at rest or in transit.

According to Chainalysis, 19% of cryptocurrency holders lost digital assets due to mismanaged digital wallets and keys [68]. But the market has already responded by offering new private key recovery solutions, both for custodial and non-custodial authorisations. One such service is the Squarelink platform. For now, it is the only *pure* non-custodial private key recovery platform. Others rely on custodial key-management services like Amazon Cognito, for example [69]. Another mitigation scheme for lost keys and wallet access is known as secure attribute-based signatures that support multiple authorities for expanded authorised access [70]. Attribute-based signatures are also being explored and tested still. As to how to address the issue of risk when data is at rest or in transit, the maintenance of encryption, authorisation and authentication during both data states are absolutely crucial and possible with proxy re-encryption (PRE) schemes [71]. Data transit can also be limited through distributed storage governance. As explained earlier in the 23&Me example, software analysis can be 'brought to the data' rather than software or algorithms processing data from a corporate owned machine [72].

One configuration of data storage, for example, is private IPFS nodes hosting DNA data for a single owner [56]. IPFS is the new alternative to corporate controlled data storage. In other words, IPFS is controlled by a community of developers similar to Bitcoin where the data repositories are only owned by the creators of content that also hold the private keys. Data owners can allow trusted third□ party validators and other authorised custodians [60] [61]. Using PRE layers such as Nucypher, consumers can securely share encrypted data without sharing their private key [73]. PRE serves as a means for delegating decryption rights, opening up applications that require delegated access to encrypted data (whether genomic or otherwise) [71].

By augmenting who gets access in these kinds of configurations, authorised custodians may be optionally established over time without compromising either the security or the integrity of the data and the data owner. Essentially PRE helps data owners share a secret with minimal risks to the secret or secret keeper [74]. Risks are thereby minimised more adequately within these frameworks as opposed to what is in existence in legacy healthcare and genomic data silos. The data owner can essentially rent out their data never losing control over it. Next, we explain how NFTs, specifically on top of these crypto privacy-preserving [65] offerings, create additional value for highly sensitive and scarce data like genomic data in the context of adhering to privacy laws.

Non-fungible tokens (smart contracts)

Gamers were first attracted to NFTs because they could represent the collectible creatures called CryptoKitties [75]. NFTs are now used by crypto artists, blockchain games and countless other users to ensure digital scarcity and ownership. NFTs are tokens *minted* on blockchains that are irreplaceable and individually unique [76] [77]. In contrast, fungible tokens refer to something that can easily be replaced by something identical and is interchangeable. A dollar bill is an example of a fungible item. If you were to lend a dollar, it wouldn't matter what dollar nor what fungible token representing it was returned. Non-fungible means that no other asset or representative token is exactly like it. This is both relevant and similar to the representation, form and function of genomic data. The NFT design is especially advantageous for managing the rights and ownership of highly scarce and unique assets, both on and off the blockchain.

In this same way, we believe using NFTs will assist in making genomics data portable beyond the specified solution across multiple environments, while still allowing for strong governance and control by the genomic data owner or authorised custodian. Thus, we identify the use of NFTs to represent individual user genomes. Unlike traditional cryptocurrency or ledger-based tokens, NFTs are not interchangeable – carrying their own information or other attributes that make them irreplaceable. NFTs on the Ethereum Blockchain are governed by two specifications known as ERC-721 and ERC-1155 [7] [78]. Additional Ethereum Request for Comments (ERCs) show developmental growth that may represent more robust specifications in genomics data use cases. See Table 1.

Table 1

Privacy law, genomic data, NFT/ERC developmental stages					
	ERC721	ERC998	ERC1155	ERC994	ERCXXXX (IDEAL)
Locked ownership (ownership loss prevented)	Yes	Yes	Yes	Yes	Yes
Non-fungible token collective ownership (parent, child, family tokens possible)	No	Yes	Yes	No	Yes
Semi-fungible (Can hold both non-fungible and fungible tokens)	No	No	Yes	No	Yes
Delegated to authorised custodians (suitable for "rent")	No	No	Yes	Yes	Yes
Metadata included for location of cytogenic data (e.g. (whole genome, chromosome, genes, SNPs)	No	No	No	No	Yes
Data maintenance and programmable privacy code schemas (GDPR, CCPA, COPRA, etc.)	No	No	No	No	Yes

ERC-721 defines a minimum interface written in Solidity [79] that allows unique tokens to be managed, owned and traded [78]. It does not mandate a standard for token metadata or restrict adding supplemental functions for genomics payloads. In the proposed solution, ERC-721 are used to store references to genomic material and searchable metadata attributes. Whereas ERC-721 mandates a unique token contract for each token created, ERC-1155 may be more efficient to create and bundle token transactions. ERC-1155 can be used to meter requests for genomic data and ensure that no user has more than their share of resources commuted to perform work in the data processors environment.

ERC-1155 provides additional flexibility over ERC-721 by creating flexible, re-configurable or exhaustible tokens. Alternatively, the ERC-998 extension to ERC-721 is still in draft but offers the idea of NFT collections such as parent, child and family DNA collections. The ERC-998 and future ERCs are developmentally better iterations on past ERCs with other limitations such as inefficient transfer capability, array length and inability to get token IDs [79]. But as illustrated in Table 1, in ERCXXX, Genobank is targeting the development of a future more robust solution specification to the challenges at the intersection of privacy laws, genomics and smart contracts.

Use case

Genobank is the first privacy-preserving personal DNA Kit (patented) that guarantees consumers' complete ownership and control over their DNA. It was founded so that patients can benefit from finding DNA-based clinical trials without risking their identities or control over their data. Genobank.io is built on an Oasis Lab decentralised cloud infrastructure [80] that allows developers to create Web 3.0 applications where users can own and control their genomic data in a peer-to-peer transaction mode. This offers a high-performing (1000s of transactions per second) confidential and privacy-preserving NFT [6] execution. Its purposeful design supports rigorous analysis using various security properties [63] [81]. The DNA crypto wallet allows users to purchase biospecimen extraction kits. Biospecimens include biomaterial such as saliva that render DNA and RNA genomic information. After the biospecimen is collected for the specific extraction kit, the user can choose to send the kit to their preferred CLIA Certified Laboratories Sequencing Service [82] for analyses. The biospecimen itself will remain at the CLIA Lab, but the digital data, analyses and any 'reporting' will be stored in a data wallet repository. The wallet repository is the 'place' where genetic data is 'banked'. The Genobank approach is still developing and refining itself as a value proposition. But unlike many existing options (e.g. LunaDNA, Nebula Genomics, EncrypGen [62] [66]), Genobank offers the DNA donor and data processor a secure platform where they can both ethically and efficiently process genetic data without DNA owners losing custody or control over their DNA.

3. Discussion

Over the last 10 years, laws, medicine and technology together with policy makers and regulators (including the United States Food and Drug Administration, FDA) have struggled to establish timely regulation [44] [60] and oversight over the direct to consumer genetic testing (DTC-GT) health market.

The DTC-GT market has pushed the boundaries of how society and the law will manage the value of privacy over profit and what that will look like in data governance practices. To date, companies such as 23andMe and Ancestry, among others [83], have shown an inexhaustible ability and willingness to exchange consumer information (e.g. statistics about raw genetic health risk and ancestry/genealogical data, and genetic data) with third parties [84] [35]. But now, even their third-party collaborators are at risk for liability issues because privacy laws like the CCPA are requiring different business behaviour than in the past.

Sharing, selling and reselling DNA data is not unique to companies like 23andMe, Ancestry and GSK [35]. History and the law provide an endless record of people and entities that find highly sensitive information like health and genetics data valuable [8] [83] [85]. Analysing millions of people's genetics alongside their health issues gives big pharma and data processors immense power and innumerable clues on the interplay between genetics and the conditions leading to untold future profits. Ensuring both the ethical and legal underpinnings of this marketplace may not be the norm now, but it could be in the future.

Platforms such as Genobank.io can help re-balance the power [86] between stakeholders where privacy laws are trying to redress negative outcomes on the public with NFTs and programmable privacy.

4. Conclusion

At the intersection of privacy law, genomics and smart contracts, stakeholders can either help drive or hinder progress to address the balance between public and private interests more fairly. Stricter privacy laws are not the only changes coming. Professional engineering and computer software standards are also changing the design and development landscape for technological innovations.

Various professional standards such as the IEEE P7000 series [42] and the new IEEE P2089 [87] standard for age appropriate digital services for children and P2418.6 [43] – the standard for the framework of distributed ledger technology (DLT) use in healthcare – are all being developed to help address obstacles, gaps and challenges in the digital data marketplace.

In the future, these professional standards exploring the ethical considerations of software engineering could be used in the courts, in conjunction with privacy law to protect consumers and data owners. Standards often add teeth [88] to professional practices that add illustrative strength to law. These particular standards aim to integrate ethical guides that are meant to protect consumers from the wild West [89] markets of the past. In sum, the public can look forward to future benefits in regulation and standards that will challenge decades of laissez faire interests in the private sector.

The blockchain and smart contracts can be the language that frames new relationships between law, genomic data and technology. We ask you to collaborate with us and work together to address both the human and the technological challenges in this complex DNA data marketplace. Together, we can develop a better future between stakeholders to reduce litigation risk while making genomic data analysis safer and more private. Blockchain companies with ethical [67] [90] [91] foundations, like Genobank.io, will be setting themselves apart from others in the market. By offering programmable privacy with NFTs derived from privacy laws' terms and conditions [92], Genobank.io and stakeholders can help provide at least one novel approach to adding transparency and data owner sovereignty to the genomic data marketplace.

References:

[1] H. I. Ozercan, A. M. Ileri, E. Ayday, and C. Alkan, "Realizing the potential of blockchain technologies in genomics," Genome Research, vol. 28, no. 9. Cold Spring Harbor Laboratory Press, pp. 1255–1263, 01-Sep-2018.

[2] L. Goldman and J. Lewis, "See you in court," Occupational Health, 2001. [Online]. Available: https://www.genomeweb.com/scan/see-you-court#.Xb4wLUdKiUk. [Accessed: 14-Jan-2020].

[3] "GenoBank – Power of DNA." [Online]. Available: https://genobank.io/#product. [Accessed: 14-Jan-2020].

[4] M. Corrales, P. Jurˇ, and G. Kousiouris, Legal Tech, Smart Contracts and Blockchain. 2019.

[5] M. Corrales, P. Jurčys, and G. Kousiouris, "Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework," in Legal Tech, Smart Contracts and Blockchain, M. Corrales, M. Fenwick, and H. Haapio, Eds. Singapore: Springer Singapore, 2019, pp. 189–220.

[6] C. Blenkinsop, "Non-Fungible Tokens, Explained | Cointelegraph," 2018. [Online].

Available: https:// cointelegraph.com/explained/non-fungible-tokens-explained. [Accessed: 14-Jan-2020].

[7] T. Savel, K. Kuzmeskas, C. McFarlane, and M. Ulieru, "Tokens & The Internet of Value: Blending Game Theory, Computer Science, Psychology, and Economics," Blockchain in Healthcare Today, 2018. [Online]. Available: https://blockchainhealthcaretoday.com/index.php/journal/article/view/93. [Accessed: 14-Jan-2020].

[8] University of Minnesota, "Lawseq |Genomics Law." [Online]. Available: https://lawseq.umn.edu/. [Accessed: 14-Jan-2020].

[9] E. Chau, "Bill Text - AB-375 Privacy: personal information: businesses. CCPA," California Legislative Information, 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. [Accessed: 14-Jan-2020].

[10] D. Roland-Holst et al., Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations State of California Department of Justice Office of the Attorney General California Department of Justice Prepared for: Attorney General's Office Contents. .

[11] European Parliament and Council of the European Union, Regulation 5419/16 GDPR, vol. 2016, no. April. 2016, p. 261.

[12] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," Healthcare, vol. 7, no. 2, p. 56, Apr. 2019.

[13] E. Cantwell, Maria; Klobuchar, A; Markey, "16TH CONGRESS 1ST SESSION Consumer Online Privacy Act COPRA," Congress.gov, 2020. [Online]. Available: https://www.cantwell.senate.gov/imo/media/doc/COPRA Bill Text.pdf. [Accessed: 14-Jan-2020].

[14] D. Uribe, "International Workshop Data Protection in Real-Time: Transforming Privacy Law into Real Practice," in Distributive Biobanking Models: Why Biospecimens Need, 2019.

[15] Princeton University, "Machine-Language Programming," Computer Science: An Interdisciplinary Approach. [Online]. Available: https://introcs.cs.princeton.edu/java/63programming/. [Accessed: 14-Jan-2020].

[16] A. Regalado, "More than 26 million people have taken an at-home ancestry test - MIT Technology Review," MIT Technology Review, 2019. [Online]. Available: https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/. [Accessed: 14-Jan-2020].

[17] Y. Liu, "Progress review: genome sequencing - June 2019 - LessWrong 2.0," Lesswrong.com, 2019. [Online]. Available: https://www.lesswrong.com/posts/geE9t5Dm9iq6Y7nQ4/progress-review-genome-sequencing-june-2019. [Accessed: 14-Jan-2020].

[18] D. Netburn, "So many people have had their DNA sequenced that they've put other people's privacy in jeopardy," Phys.org, 2018. [Online]. Available: https://phys.org/news/2018-10-people-dna-sequenced-theyve-privacy.html. [Accessed: 14-Jan-2020].

[19] "Global Blockchain in Genomics Market: Focus on Business Models, Services, Applications, End Users, 11 Countries Data, and Competitive Landscape - Analysis and Forecast, 2019-2029."

[20] Y. Erlich, T. Shor, I. Pe'er, and S. Carmi, "Identity inference of genomic data using long-range familial searches," Science, vol. 362, no. 6415, pp. 690–694, Nov. 2018.

[21] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, Jan. 2018.

[22] Future of Privacy Forum, "Comparing privacy laws: GDPR vs CCPA."

[23] "What Businesses Need to Know About the California Consumer Privacy Act," American Bar Association, 2019. [Online]. Available: https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/. [Accessed: 14-Jan-2020].

[24] C.-H. Chen, I. O. S. Press, A. Trappey, M. Peruzzini, J. Stjepandić, and N. Wognum, "Transdisciplinary Engineering: A Paradigm Shift: Proceedings of the 24th ISPE Inc. International Conference on Transdisciplinary Engineering, July 10-14, 2017," 2017. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1640417&lang=es&site=ehost-live&scope=site. [Accessed: 14-Jan-2020].

[25] G. Leeming, J. Cunningham, and J. Ainsworth, "A Ledger of Me: Personalizing Healthcare Using Blockchain Technology," Frontiers in Medicine, vol. 6. Frontiers Media S.A., 24-Jul-2019.

[26] M. Wirth, Christian; Kolain, "Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data," in Proceedings of the ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies, 2018, no. 10, pp. 1–8.

[27] Research and Markets, Global Blockchain In Genomics Market By Type (Public, Federated, Private), By Application (Clinical Trials, IP Management, Drug Discovery, Data storage and security, Others), By Models, By Targets, By End User, By Region, Forecast & Opportunities, 2025, Technical Report, Research and Markets,, Dublin, IE, May 2020. Accessed on: May 26, 2020. [Online]. Available https://www.researchandmarkets.com/reports/5022662/global-blockchain-in-genomics-market-by-type#pos-1.

[28] "Get Ready, CCPA Is No GDPR Lite - SecurityRoundTable.org." [Online]. Available: https://www.securityroundtable.org/get-ready-ccpa-is-no-gdpr-lite/. [Accessed: 14-Jan-2020].

[29] "US Data Privacy Evolution, California's CCPA is King," National Law Review, 2019. [Online]. Available: https://www.natlawreview.com/article/digital-revolution-takes-new-meaning-among-calls-heightened-us-data-privacy-measures. [Accessed: 14-Jan-2020].

[30] L. Feiner, "Senate Democrats reveal new COPRA digital privacy bill," 2019. [Online]. Available: https://www.cnbc.com/2019/11/26/senate-democrats-reveal-new-copra-digital-privacy-bill.html. [Accessed: 14-Jan-2020].

[31] The Judicial Learning Center, "Why Do We Need Laws? | The Judicial Learning Center," 2015. [Online]. Available: http://judiciallearningcenter.org/law-and-the-rule-of-law/. [Accessed: 14-Jan-2020].

[32] S. Abdukadirov, Ed., Nudge Theory in Action, 1st ed. New York, New York, USA: Palgrave Macmillan, 2016.

[33] E. Genomics and H. Evolutionary, "What is genomics? •," Genome, 2008. [Online]. Available: https://www.news-medical.net/life-sciences/What-is-Genomics.aspx. [Accessed: 15-Jan-2020].

[34] "A reference standard for genome biology," 2018.

[35] D. Roland, "23andMe and GSK are mining customers' DNA data in a hunt for new drugs - MarketWatch," Wall Street Journal, 2019. [Online]. Available: https://www.marketwatch.com/story/23andme-and-gsk-are-mining-customers-dna-data-in-a-hunt-for-new-drugs-2019-07-23. [Accessed: 15-Jan-2020].

[36] "The NIH Is Bypassing Tribal Sovereignty to Harvest Genetic Data From Native Americans - VICE," Vice.com, 2018. [Online]. Available: https://www.vice.com/en_us/article/8xp33a/the-nih-is-bypassing-tribal-sovereignty-to-harvest-genetic-data-from-native-americans. [Accessed: 15-Jan-2020].

[37] L. O. Gostin, "National health information privacy: Regulations under the health insurance portability and accountability act," J. Am. Med. Assoc., vol. 285, no. 23, pp. 3015–3021, Jun. 2001.

[38] L. M. Slaughter, "The Genetic Information Nondiscrimination Act: Why Your Personal Genetics are Still Vulnerable to Discrimination," Surgical Clinics of North America, vol. 88, no. 4. pp. 723–738, Aug-2008.

[39] S. M. Suter, "GINA at 10 years: The battle over 'genetic information' continues in court," J. Law Biosci., vol. 5, no. 3, pp. 495–526, May 2018.

[40] J. K. Wagner, "Disparate impacts and GINA: Congress's unfinished business," J. Law Biosci., vol. 5, no. 3, pp. 527–549, May 2018.

[41] A. M. Yuengert and A. M. Yuengert, Practical Wisdom and Economic Models of Choice. Palgrave Macmillan US, 2012.

[42] "IEEE P7000 - Engineering Methodologies for Ethical Life-Cycle Concerns Working Group - IEEE P7000 Working Group," IEEE, 2016. [Online]. Available: https://sagroups.ieee.org/7000/. [Accessed: 15-Jan-2020].

[43] "P2418.6 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences," IEEE. [Online]. Available: https://standards.ieee.org/project/2418_6.html. [Accessed: 15-Jan-2020].

[44] E. W. Clayton, B. J. Evans, J. W. Hazel, and M. A. Rothstein, "The law of genetic privacy: Applications, implications, and limitations," J. Law Biosci., vol. 6, no. 1, pp. 1–36, 2019.

[45] A. Rosic, "What is Blockchain Technology? A Step-by-Step Guide for Beginners," Journal of Chemical Information and Modeling, 2013. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed: 14-Jan-2020].

[46] H. Shaw, "A Cryptographic System Based upon the Principles of Gene Expression," Cryptography, vol. 1, no. 3, p. 21, 2017.

[47] "IPFS Cluster - Pinset orchestration for IPFS." [Online]. Available: https://cluster.ipfs.io/. [Accessed: 14-Jan-2020].

[48] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," Health Informatics J., vol. 25, no. 4, pp. 1398–1411, Dec. 2019.

[49] A. S. Bajaj, Blockchain and Decentralized Applications.pdf, Volume 1. Kharkiv, Ukraine: Distributer Lab, 2018.

[50] R. Ribitzky, U. Broedl, C. McFarlane, and K. A. Clauson, "Data Sharing? The Case for Blockchain at the Global Convergence of Healthcare, Life sciences, and Consumer Markets," Blockchain Healthc. Today, vol. 0, no. 0, Nov. 2018.

[51] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain for the Next Generation of Cybersecure Industry 4.0 Smart Factories," IEEE Access, 2018.

[52] V. Nair, "What Will The Fourth Generation of Blockchain Look Like?," Hakernoon, 2019. [Online]. Available: https://hackernoon.com/what-will-the-fourth-generation-of-blockchain-look-like-daa5a4e90c59. [Accessed: 14-Jan-2020].
[53] "Blockchain Use Cases in 2020: Real World Industry Applications," Consensys.com, 2020. [Online]. Available: https://consensys.net/blockchain-use-cases/. [Accessed: 14-Jan-2020].
[54] Deloitte, "Deloitte's 2019 global blockchain survey," 2019.
[55] I. Barclay, A. D. Preece, I. Taylor, and D. Verma, "A conceptual architecture for contractual data sharing in a decentralised environment," in Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications, 2019, p. 15.
[56] O. Choudhury et al., "Enforcing Human Subject Regulations using Blockchain and Smart Contracts," Blockchain Healthc. Today, Mar. 2018.
[57] H. D. Zubaydi, Y. W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," Electron., vol. 8, no. 6, pp. 1–29, 2019.
[58] M. D. Sorani et al., "Genetic Data Sharing and Privacy," Neuroinformatics, vol. 13, no. 1, pp. 1–6, Jan. 2014.
[59] X. L. Jin, M. Zhang, Z. Zhou, and X. Yu, "Application of blockchain platform to manage and secure personal genomic data: A case study of lifecode.AI in China," J. Med. Internet Res., vol. 21, no. 9, 2019.
[60] R. M. Hendricks-Sturrup and C. Y. Lu, "Direct-to-consumer genetic testing data privacy: Key concerns and recommendations based on consumer perspectives," J. Pers. Med., vol. 9, no. 2, 2019.
[61] T. K. Mackey et al., "'Fit-for-purpose?' - Challenges and opportunities for applications of blockchain technology in the future of healthcare," BMC Med., vol. 17, no. 1, 2019.
[62] D. Grishin et al., "Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation," Blockchain Healthc. Today, vol. 1, pp. 1–23, 2018.
[63] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," F1000Research, vol. 5, 2016.
[64] A. M. Ileri, H. I. Ozercan, A. Gundogdu, A. K. Senol, M. Y. Ozkaya, and C. Alkan, "Coinami: A Cryptocurrency with DNA Sequence Alignment as Proof-of-work," Feb. 2016.
[65] M. Jones, M. Johnson, M. Shervey, J. T. Dudley, and N. Zimmerman, "Privacy-preserving methods for feature engineering using blockchain: Review, evaluation, and proof-of-concept," J. Med. Internet Res., vol. 21, no. 8, p. e13600, Aug. 2019.
[66] E. Ahmed and M. Shabani, "DNA Data Marketplace: An Analysis of the Ethical Concerns Regarding the Participation of the Individuals," Front. Genet., vol. 10, no. November, pp. 1–6, 2019.
[67] R. J. Cadigan, E. Juengst, A. Davis, and G. Henderson, "Underutilization of specimens in biobanks: an ethical as well as a practical concern?," Genet. Med., vol. 16, no. 10, pp. 738–740, Oct. 2014.
[68] J. J. Roberts and N. Rapp, "Lost Bitcoins: 4 Million Bitcoins Gone Forever Study Says | Fortune," Fortune, 2017. [Online]. Available: http://fortune.com/2017/11/25/lost-bitcoins/. [Accessed: 16-Apr-2020].
[69] "Squarelink Rolls Out Non-Custodial Private Key Recovery for New Wave of DApps | Business Wire," Business Wire, 2020. [Online]. Available: https://www.businesswire.com/news/home/20191202005335/en/Squarelink-Rolls-Non-Custodial-Private-Key-Recovery-New. [Accessed: 16-Apr-2020].
[70] R. U. I. Guo, H. Shi, Q. Zhao, and D. Zheng, "Special Section on Research Challenges and Opportunities in Security and in Electronic Health Records SystemsSecure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain," IEEE Access, vol. 6, 2018.
[71] D. Nuñez, I. Agudo, and J. Lopez, "Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation," J. Netw. Comput. Appl., vol. 87, pp. 193–209, 2017.
[72] F. Briscoe, "Innovations in Medical Genomics: What Are the Privacy and Security Risks?," 2017.
[73] D. Nunez, "Umbral: A Threshold Proxy Re-Encryption Scheme," Github, 2018. [Online]. Available: https://raw.githubusercontent.com/nucypher/umbral-doc/master/umbral-doc.pdf. [Accessed: 17-Apr-2020].
[74] A. Shamir, "How to Share a Secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[75] Cryptokitties, "CryptoKitties | Collect and breed digital cats!," Cryptokitties.Com, 2018. [Online]. Available: https://www.cryptokitties.co/about. [Accessed: 16-Apr-2020].
[76] M. Bal and C. Ner, "NFTracer: A Non-Fungible Token Tracking Proof-of-Concept Using Hyperledger Fabric," 2019.
[77] S. Chevet, "Blockchain Technology and Non-Fungible Tokens: Reshaping Value Chains in Creative Industries," 2018.
[78] K. Tut, "NFT and IPFS | Pinata," Medium, 2020. [Online]. Available: https://medium.com/pinata/who-is-responsible-for-nft-data-99fb4e8147e4. [Accessed: 16-Apr-2020].
[79] "solidity - ERC721 owned Tokens array length limitations on owners with thousands of tokens - Ethereum Stack Exchange." [Online]. Available: https://ethereum.stackexchange.com/questions/41937/erc721-ownedtokens-array-length-limitations-on-owners-with-thousands-of-tokens. [Accessed: 17-Apr-2020].
[80] "Developer Spotlight: Genobank.io - Oasis Labs - Medium." [Online]. Available: https://medium.com/oasislabs/developer-spotlight-genobank-io-7ebeb96dd0d2. [Accessed: 15-Jan-2020].
[81] R. Cheng et al., "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts."
[82] "State Agency & Regional Office CLIA Contacts | CMS." [Online]. Available: https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/State_Agency_and_Regional_Office_CLIA_Contacts. [Accessed: 15-Jan-2020].
[83] HIPAA, "Legal News," HIPAA JOURNAL, 2020. [Online]. Available: https://www.hipaajournal.com/category/legal-news/. [Accessed: 15-Jan-2020].
[84] Y. Huang, "An Environment-Wide Study of Adult Cognitive Performance in the 23andMe Cohort," medRxiv, vol. 60, 2019.
[85] C. Loizos, "23andMe underscores that privacy-loving customers need to opt out of its data deal with GlaxoSmithKline | TechCrunch," TechCrunch, 2018. [Online]. Available: https://techcrunch.com/2018/09/05/23andme-underscores-that-privacy-loving-customers-need-to-opt-out-of-its-data-deal-with-glaxosmithkline/. [Accessed: 15-Jan-2020].
[86] R. Kain et al., "Database shares that transform research subjects into partners," Nat. Biotechnol., vol. 37, no. 10, pp. 1112–1115, Oct. 2019.
[87] "P2089 - Standard for Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children," IEEE. [Online]. Available: https://standards.ieee.org/project/2089.html. [Accessed: 15-Jan-2020].
[88] P. Cihon, "Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development," 2019.
[89] Northeastern University, "The Wild West of IoT: Regulating Uncharted Territory - Level at Northeastern University | Blog," Level, 2019. [Online]. Available: https://www.northeastern.edu/levelblog/2018/04/11/wild-west-iot-regulating-uncharted-territory/. [Accessed: 15-Jan-2020].
[90] S. Spiekermann, J. Korunovska, and M. Langheinrich, "Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers," Proc. IEEE, vol. 107, no. 3, pp. 600–615, 2019.
[91] J. Hooker, "Ethics of Artificial Intelligence," Tak. Ethics Seriously, pp. 211–219, 2018.
[92] American Society of Human Genetics, "New file type improves genomic data sharing while maintaining participant privacy -- ScienceDaily," Science Daily, 2018. [Online]. Available: https://www.sciencedaily.com/releases/2018/10/181017141005.htm. [Accessed: 15-Jan-2020].

Competing Interests:
Daniel Uribe is CEO of the company Genobank.io, used as the case study in this paper.

Ethical approval:
Not applicable.

Author's contribution:
Daniel Uribe is the main author.

Funding:
None declared

Acknowledgements:
This paper was first presented at the 2nd Blockchain International Scientific Conference: ISC2020 at Edinburgh Napier University, Scotland (March 11, 2020). We would like to thank the session chairs and participants for their comments which significantly refined the conceptual landscape. We would also like to acknowledge, in no specific order, the help and guidance shared by the following individuals: Vitalik Buterin; Dulce Villarreal; Dr Naseem Naqvi FRCP, FHEA, MAcadMeded, MSc, FBBA; Dr Mureed Hussain MD, MSc, FBBA; Prof Bill Buchanan OBE, PhD, FBCS; Martin Docherty-Hughes; Dr Sean Manion, PhD; Prof Dr Marc Pilkington PhD; Prof. Daniel Catchpoole, PhD; Prof. Paul Kennedy, PhD; Gustavo Grillasca; Marco Montes; Everardo Barojas; Dr. Luis Garcia Puig; Angelica Estrada; Prof. Dawn Song, PhD and Vishwanath Raman, PhD. Finally, we thank the reviewers for their constructive feedback.

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(8)2020

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

Naseem Naqvi, Mureed Hussain
Centre for Evidence-Based Blockchain, The British Blockchain Association, UK
Correspondence: naseem@britishblockchainassociation.org
Received: 6 July 2020 **Accepted:** 15 August 2020 **Published:** 1 September 2020

Abstract

Evidence-based applications of resources remain one of the greatest challenges faced by governments, businesses, and policymakers. The United States Government Accountability Office (GAO) evaluated ten large programs, which together cost more than $10 billion/year, through randomised control trials – the highest standard of evidence-based practice (EBP) [1]. The evaluation found that nine of them had 'weak or no positive effects' on their participants. Many programs were not evaluated at all [2]. In January 2019, U.S. President signed the 'Foundations for Evidence-based Policy Making Act' into law [3]. A USAID (US Agency for International Development) study looked at 43 blockchain projects and companies claiming to have solved various problems using distributed ledgers [4]. The study found that almost no company was willing to share their results and MERL (monitoring, evaluation, research and learning) processes [5]. Other observational data revealed that 80–90% of blockchain-based token offering projects failed to deliver on their promises [6], a prediction also made by Vitalik Buterin, the founder of Ethereum blockchain, in 2017 [7].

The concept of evidence-based blockchain (EBB) was first introduced by Naqvi in 2018 [8]. We conducted an evaluation of 517 blockchain firms against PCIO framework of evidence-based practice: Problem – Comparison – Intervention and Outcomes. We define the fundamentals of EBB (Ask, Acquire, Appraise, Apply, Assess), provide a review of the literature on EBB, report findings of our study and propose an Assessment Framework of Evidence Based Blockchain (Figure 12).

Keywords: *Evidence-Based Blockchain, Distributed Ledgers, CEBB, Cryptocurrency, Critical Appraisal, Government, Enterprises, Peer Review*

JEL Classification: *O1, A1, C9, D8, E2, F4, L2*

1. Introduction

Evidence-based practice (EBP) is the idea that professional practices should be based on a combination of critical thinking and the best available evidence [9]. However, a study showed that 98% of managers failed to apply best practices when making decisions [10]. In blockchain, research showed that cognitive biases and behavioural heuristics can influence the decision support systems of professionals [11, 12].

In the United States, ten large decades-old social programs, which together cost more than $10 billion a year, were subjected to randomised controlled trials, the highest standard of evaluation. The evaluation found that nine of them had 'weak or no positive effects' on their participants. Many programs were not evaluated at all [2, 3]. In 2019, President Trump signed the Foundations for Evidence-Based Policy Making Act, making it a law to practice evidence-based policymaking [3]. The book Show me the Evidence [13] [Figure 3] describes the life story of Barack Obama's fight to ensure that government initiatives are based on robust scientific evidence.

2. Context and history of EBP

The concept of EBP was first introduced in medicine in 1972 by Archibald Cochrane in his landmark book *Effectiveness and Efficiency: Random Reflections on Health Services* [14]. Cochrane observed that patients were dying unnecessarily and expressed his concerns over the scarcity of scientific evidence used by the NHS to evaluate the effectiveness of therapies and the use of available resources [15]. In 1991, Gordon Guyatt of McMaster University formally coined the term 'evidence-based medicine' [16].

Over the past three decades, the idea of EBP has spread across most disciplines, such as: medical education [17], management [18], social policy [19], criminal justice [20], cybersecurity [21], nursing [22], employment [23], probation services [24] and blockchain [25].

2.1 Timeline

Important timelines of major disciplines embarking on the journey towards evidence-based practice:

1990: Medical Education (Professors Guyatt & Sackett, McMaster University, Canada)

1998: Probation Services (Professor Peter Raynor, University of Wales)

1999: Social Care (National Institute of Clinical Excellence, NICE, UK)

2000: Criminal Justice (Professor David Farrington, University of Cambridge, UK)

2005: Employment and HR (Denise Rousseau, Carnegie Mellon University, USA)

2006: Management (Centre for Evidence Based Management, The Netherlands)

2018: Blockchain and Distributed Ledgers (The British Blockchain Association, UK)

2.2 Centres advancing EBP

Around the globe, there are now over two dozen 'centres of excellence' advancing evidence-based practices (Figure 1). The Centre for Evidence-Based Blockchain (CEBB) operates under the auspices of the British Blockchain Association as the world's first centre for distributed ledger technologies advancing evidence-based practices (Figure 2). There are also numerous books written on the topic of evidence-based practice (Figure 3).

Figure 1. Centres of Evidence-Based Practice

2.3 What is the evidence for EBP?

A study was conducted that examined two groups of senior decision makers – one group was asked to make decisions based on the best available scientific evidence and the other was asked to simply make decisions based on factors such as instincts, organisational policies and personal experience. The results were striking: the group that utilised EBP achieved the desired result 90% of the time, had a 50% reduction in their failure rate and a six-fold increase in the number of correct business decisions. Furthermore, this group exceeded expectations only 40% of the time, compared to the other group that practiced conventional decision making [10].

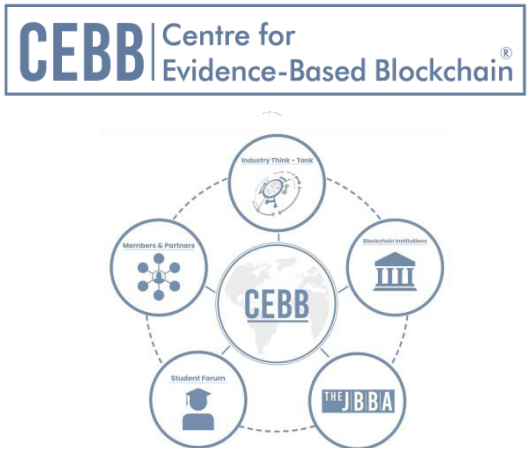


Figure 2. Centre for Evidence-Based Blockchain

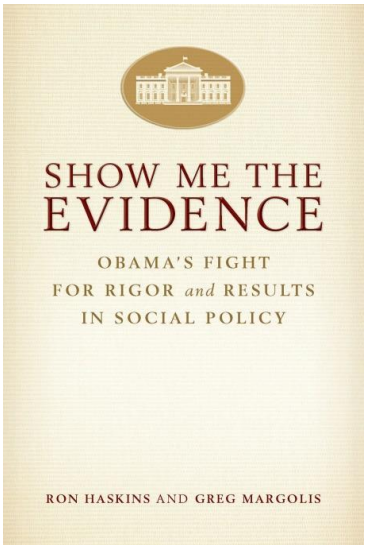


Figure 3. Books written on EBP

2.4 Why EBB?

EBB attempts to solve five major problems in the blockchain space. The first problem is the inability to clearly define the problem to be solved. Sometimes blockchain is applied to a problem that does not exist or is not significant enough to require a decentralised solution. There are many examples from the 2017–18 ICO boom where many projects, while not necessarily scams [26], failed to materialise. Many were considered to be seen as 'blockchain – a solution in search for a problem' also called excessive 'blockchainising' (or solutioneering) [27]. This is a significant problem as it wastes time and resources (Figure 5).

The second major problem is that we do not examine different sources of evidence and do not always start by searching for the best available scientific evidence. We often rely on superficial Google searches, magazines, expert opinions and blog posts to make judgements about a particular problem, which is often a significant mistake (Figure 5).

The third problem is inadequate evaluation of the quality of evidence. Often, this is because we have not been trained to provide adequate evaluations or do not think doing so is important. For example, we may go to an event and hear someone talking about their blockchain solution or idea and may not ask the speaker whether this been independently peer reviewed, externally validated or impartially evaluated.

The fourth problem is the lack of application of evidence to improve processes. Interventions and solutions are proposed with no objective scientific evidence to back up their efficacy or effectiveness (Figure 6).

The final problem is that we often inadequately report the outcomes and results of our experiments, especially when the results are unfavourable. A study by the US Agency for International Development examined 43 blockchain use cases and companies using blockchain that claimed to have solved various problems using distributed ledgers. They found that almost no company was willing to share the data on the results and MERL (monitoring, evaluation, research and learning) processes [5], an observation consistent with our research findings (Figure 10).

2.5 What is EBB?

We define EBB as *conscientious, explicit and judicious decision making based on professional expertise and evidence from organisations, stakeholders and scientific research.*

EBPs around blockchain and distributed ledger technologies (DLTs) are rapidly maturing. While these practices are still in the early stages of development, there is an emerging body of robust scientific, peer-reviewed evidence-based literature examining common use cases and specialties, such as the following: banking, fintech and payments [28,29,30,31,32]; digital identity, records and notary [33,34,35,36]; supply chain and trade finance [37,38]; health care and life sciences [39,40,41]; energy, climate and philanthropy [42,43]; networking, social impact and media [44,45,46,47,48,49]; government, law and public policy [50,51,52,53,54,55]; and cybersecurity, AI, quantum computing and IoT [56,57,58].

Figure 4. Sources of Evidence

While the focus of our research is scientific evidence, it is important to note that the other three sources of evidence are equally important when making decisions regarding blockchain.

2.6 How to practice EBB?

EBB is a five-step approach consisting of the **'5 As'**:

1. Formulate a precise question (**ASK**).
2. Search for the evidence and look for answers to the question (**ACQUIRE**).
3. Critically appraise the evidence (**APPRAISE**).
4. Apply the results to your practice (**APPLY**).
5. Monitor any changes and evaluate (**ASSESS**).

These five steps should be followed to evaluate both the problem and the solution.

2.6.1 ASK: Formulate a precise question

Clearly defining the problem is the first step to practicing EBB. One should always ask the following:

'What exactly is the problem here?'
'What is it that we are trying to solve?'
'How exactly are we trying to address this issue?'

Instead of asking 'should I use blockchain for my supply chain business?', one should clearly define the type of blockchain, the intervention, the comparison group and the desired outcomes by using the **PCIO approach**. An example of a more precise question using the PCIO approach is as follows:

Compared to existing traditional database infrastructure ***(Comparison)****, does private permissioned blockchain* ***(Intervention)*** *save time, reduce costs, improve food integrity, and increase consumer satisfaction* ***(Outcomes)*** *in the tracking of seafood via the supply chain* ***(Problem)*** *based in India?*

Consider the following examples – An organisation plans to use blockchain to streamline cross-border trade, or facilitate low-cost international payments for people in Africa, or provide disability funds in Germany, or verify provenance of drugs in Australia or create land registries in Sweden: In each case, there must first be a clear description of the extent and magnitude of the problem, what has been tried to address that particular problem (the conventional legacy systems) and why and how a blockchain-based system would be a better alternative than the existing models.

2.6.2 ACQUIRE: Search for high-quality evidence

While traditional search engines are useful in searching for online content, the vast majority of information from search engines is often unfiltered low-quality blogs, opinion articles, anecdotes and other social media posts. Evidence-based practitioners must ensure that their initial searches include all portals that index high-quality, peer-reviewed research. For scientific peer-reviewed evidence, one could consider the following:

- DOAJ
- Semantic Scholar
- Microsoft Academic
- SCOPUS
- EBSCO
- EU Open Aire
- World Cat
- Library catalogues
- Institutional repositories

Papers and case studies published at arXiv, ResearchGate or SSRN are not necessarily peer reviewed, so it is important to check the sources and platforms where these studies are published to determine if they are subjected to an independent peer review.

It is therefore important to understand the difference between filtered and unfiltered information [59]. Filtered or critically evaluated evidence include critically appraised, peer-reviewed research topics, systematic reviews and critically evaluated individual articles. Unfiltered evidence on the other hand includes non-peer-reviewed case studies, case reports essays, commentaries, blog-posts, magazine articles, opinions, surveys, analyses, company white papers, progress reports, industry or organisation reports, consensus reports and internal audits, stakeholder meetups and consortium presentations/publications.

2.6.3 APPRAISE: Evaluate the quality of evidence

Appraisal is 'a process of carefully and systematically examining research to judge its trustworthiness, its value, and relevance in a particular context' (Burls 2009). Carefully examining the data to establish its validity, applicability and effectiveness is an essential component of the EBP. A high-quality peer review ensures published research is subjected to scrutiny and evaluation by experts in the field, advancing scientific rigour and robustness to the scientific body of evidence.
Once sufficient evidence-based data has been collected, the next step is to apply the evidence to practice. It is important to be mindful of the limitations of the evidence and the inherent bias. As discussed earlier, not all evidence is the same; applying poor-quality, weak evidence to one's practice may result in economic, social and technical harm and waste of resources.

Why is an independent external peer review important? A peer-review process involves an independent, and usually a double-blind (i.e., the author and reviewers do not know each other's identity), review of research to check for accuracy and reliability and verify whether any claims of novelty are consistent and trustworthy. The reviewers ensure that the results and conclusion are consistent with the hypothesis put forward at the start of the paper. Any grandiose claims are also challenged. A review also ensures

that a paper follows the correct scientific method and cites appropriate references in support of the claims made in the paper. A review helps advance an emergent consensus among the scientific community and supports the foundations of scientific rigour.

2.6.4 ASSESS (and) PUBLISH results

The final step involves the structured evaluation of evidence to analyse the outputs, outcomes and impact of the EBP. This involves the evaluation of the process itself, the outcome measures and stakeholders' feedback.

It is important that an EBB professional

- Writes down the results.
- Presents the results.
- Submits them for peer review, if applicable.
- Publishes them, ideally in an open access journal.
- Evaluates and reports the inputs, outputs, outcomes, impacts and any recorded or otherwise auditable occasion of influence of the research findings.

Reporting outcomes is an integral component of the EBB; it completes the learning loop, provides an opportunity to reflect on the results, sets parameters for future research and encourages the evaluation of practices.

Traditionally, citations have been the cornerstone of measuring attention, impact and scholarly influence. More recently, alternative metrics, also called 'alt-metrics', have become a popular way to gauge impact. Alt-metrics analyse the online activity around research output in sources such as social networks, news outlets, policy documents, conferences and blogs, providing a more robust picture of the attention, influence and reach of published work.

What is a research impact? The London School of Economics defines an impact as *recorded or otherwise auditable occasion of influence from research on another individual or organization, demonstrated by references to, citations of or a discussion of the research or the researcher.*

3. Study design and methodology

There are four key constructs that emerge from the principles of Evidence-based Blockchain and these will form the foundations of our study **(PCIO questionnaire)**

- **Problem (P)**
- **Comparison/Control (C)**
- **Intervention (I)**
- **Outcome (O)**

We further categorise each PCIO item into 3 descriptive sub-sets of questions, making it a total of **12 fundamental questions**. These questions will form the foundations of EBB evidence assessment framework [Figure 11]. For the purpose of our research, we concluded that a firm was evidence based if there was an explicit evidence of demonstration of at least 2 of the 3 criteria.

The **problem** – A clear description of the problem to be solved is the first step to any blockchain-based solution offering. For the purpose of our research, we looked for explicit description of the following:

Q1: Is there a clearly defined problem?

Q2: What is the evidence that the problem exists? (Who is effected? Who is talking about it? source and quality of evidence)

Q3: How significant is the problem? (extent and magnitude)

The comparison - We searched for a documentary evidence of the existing solutions/legacy systems control/comparison. For the purpose of our research, we looked for explicit description of the following:

Q4: What are the existing solutions available to address the problem? Who is providing those solutions? What is the source and quality of evidence for this?

Q5: What are the results/outcomes of the existing solutions/systems?

Q6: Are these critically evaluated? Are the Results published?

The **intervention** – We searched for a clear description of the proposed solution and looked for explicit documentation of the following:

Q7: What is the intervention? Why and how is it different from other solutions?

Q8: Is there scientific evidence to back up the intervention?

Q9: Has the intervention been critically evaluated and, if so, by whom and what are the outcomes?

The **outcome** – We searched for documentary evidence of the following:

Q10: What are the key outcomes of the proposed solution?

Q11: Have the results shown an objective improvement in outcomes?

Q12: Are the outcomes independently evaluated, critically appraised (peer reviewed) and published open access?

3.1 Types of evidence

For the purpose of our research, we categorise evidence assessment into two groups:

Filtered evidence

This includes **peer-reviewed** meta-analysis; systematic review; original research; case studies; and critical reviews published in academic peer-reviewed, open access journals. We also include evidence of presentations at scientific/academic conferences, summits and academic society meetings as filtered evidence. An evidence synthesis underpinning national guidelines, government policy reports, outputs of scientific committee reports, regulations, national benchmarks and frameworks based on an independent evaluation of data are also considered as filtered evidence.

We considered evidence published in academic, peer-reviewed journals as filtered evidence. We scanned this information on the following sites:

DOAJ (Directory of Open Access Journals) [60]
Microsoft Academic [61]
Semantic Scholar [62]
Google Scholar [63]
SSRN [64]
ResearchGate [65]
SCOPUS [66]
WorldCat [67]
EBSCO [68]
EU OpenAire [69]
Libraries and academic/institutional repositories [70]

Unfiltered evidence

This includes non-peer reviewed essays and research papers on arXiv,

ResearchGate and SSRN; commentary; medium or other blog-posts; magazine articles; opinions; surveys; analyses; company white papers, progress reports, industry or organisation reports, consensus reports and internal audits; stakeholder meetups; and consortium presentations, publications (other than academic/scientific conferences).

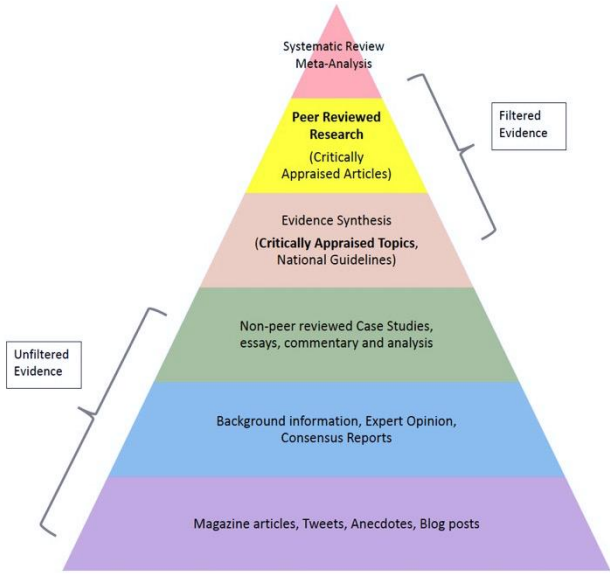


Figure 5. Filtered V Unfiltered Evidence

3.2 Sample

The Centre for Evidence-based Blockchain [24] analysed **517 blockchain projects and start-up companies** launched between **December** 2016 and **June 2020**. A random sample (Figure 3.1) of projects from **Angel.co**, a comprehensive database of over 4,800 blockchain companies (as of June 2020), was analysed. The data were collected and evaluated between December 2019 and June 2020. Findings are presented in aggregate and no company-/organisation-specific data is revealed. We collected and analysed the firm's data primarily from four main sources:

- Company website
- White papers
- Yellow and blue papers
- Google, Bing and YouTube searches for evidence of official industry talks, pitches and conference presentations by the company/organisation.

We collected data on blockchain companies and start-ups from **eight** main use cases:

Banking, fintech and payments
Digital identity, records and notaries
Supply chain and trade finance
Health care and life sciences
Energy, climate and philanthropy
Networking, social impact and media
Government, law and public policy
Cybersecurity, AI, quantum computing and IoT

The companies that were evaluated included a mix of:

a. fundraising-based blockchain projects (security token offerings, initial coin offerings, initial exchange offerings).
b. non-fundraising token companies and projects.
c. non-token blockchain companies and projects.

We included projects using blockchain or DLTs as a core-component of their solution, product or service offering. We excluded the following categories of companies from our research: Companies or projects in pre-launch or beta-phase, companies that did not provide evidence of white/yellow/blue papers on their website, or companies not using blockchain or DLT in their product or service offering.

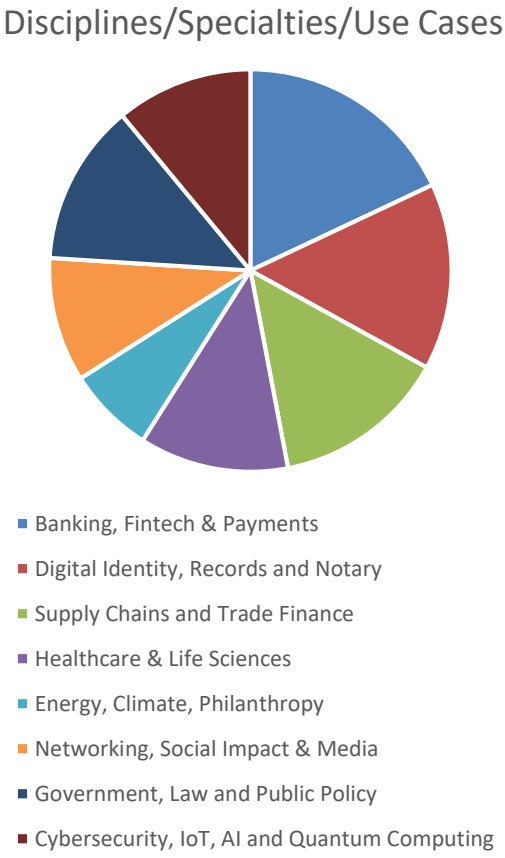


Figure 6.

4. Results

4.1 Problem

Q1: Is there a clearly defined problem?

No evidence: 160
Unfiltered evidence: 321
Filtered evidence: 36

Q2: What is the evidence that the problem exists? Who is effected? Who is talking about it? (stakeholders evidence)

No evidence: 189
Unfiltered evidence: 297
Filtered evidence: 31

Q3: How significant is the problem? (extent and magnitude)

No evidence: 238
Unfiltered evidence: 252
Filtered evidence: 27
Average score % : **(Figure 7)**
No evidence: **37.7 %**
Unfiltered evidence: **56.09 %**
Filtered evidence: **6.21%**

Here are some of the examples of statements that were not backed by any evidence:

'as been one the major global problems of this decade' (no evidence quoted to support the statement)

'is one of the biggest challenges faced by the governments around the globe' (no evidence cited)

'current processes are slow and inefficient' (no evidence cited to back up this claim)

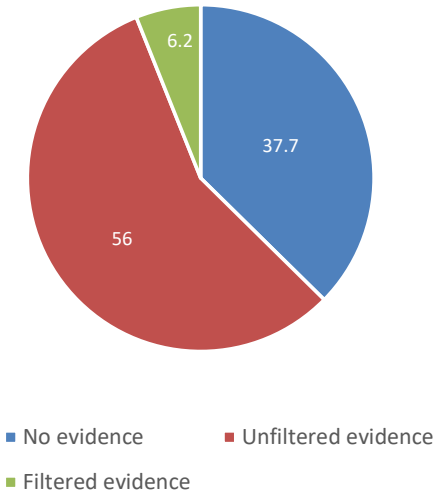


Figure 7: Evidence of the Problem (Average score %)

4.2 Comparison

We looked for objective evidence of data provided by the firms on existing legacy systems with reference to an externally validated study, public policy report, government documents or industry survey. This evidence included critical reviews of existing solutions to reinforce or highlight a clear need for improvement of existing models. In addition, we examined reviews of past and current interventions that attempted to address the problems at hand, the outcomes of those interventions and statements regarding the clear established need for alternative or DLT-based solutions.

Q4: What are the existing solutions available to address the problem?

No evidence: 279
Unfiltered evidence: 192
Filtered evidence: 46

Q5: What are the results/outcomes of the existing solutions/systems?

No evidence: 262
Unfiltered evidence: 230
Filtered evidence: 25

Q6: Are these critically appraised and independently evaluated?

No evidence: 388
Unfiltered evidence: 110
Filtered evidence: 19

Average score % : (Figure 8)

No evidence: **59.89 %**
Unfiltered evidence: **34.30 %**
Filtered evidence: **5.80 %**

The following quotes are examples from our search:

'Existing arrangements and technology providers are slow, inefficient, and costly' (no evidence/data to support this statement)

'In spite of numerous attempts by public institutions to address the…' (Which public institutions? What were the results of those attempts? No evidence cited to back up this statement.)

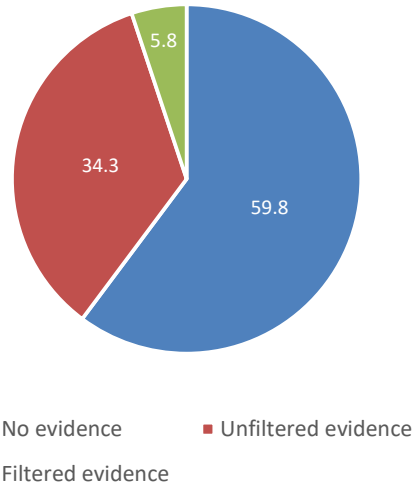


Figure 8: Evidence of Comparison/Control (Average score %)

4.3 Intervention

We scanned for clear documentation or references to evidence for proposed solution or intervention, and asked the following three questions:

Q7: What is the intervention? Why and how is it different or better than other existing solutions? (organisational evidence)

No evidence: 219
Unfiltered evidence: 284
Filtered evidence: 14

Q8: Is there evidence (from another similar experiment) to back up the intervention?

No evidence: 77
Unfiltered evidence: 405
Filtered evidence: 35

Q9: Is the intervention critically evaluated and if so, by whom and what are the outcomes?

No evidence: 316
Unfiltered evidence: 179
Filtered evidence: 22

Average score % : (Figure 9)
No evidence: **39.45 %**

Unfiltered evidence: **55.96 %**
Filtered evidence: **4.57 %**

Here are some examples of statements that were not backed by any evidence:

'Our blockchain solution will transform the way data is managed around the globe' (No specific measurable evidence regarding what exactly the transformation will look like and no information on how this will be evaluated based on objective evidence.)

'our blockchain will speed up the transactions and reduce costs for the customers' (No objective evidence for the improvement of speed and cost reductions in terms of data/numbers.)

'We managed to reduce the operational costs by 50%'
(No objective evidence provided.)

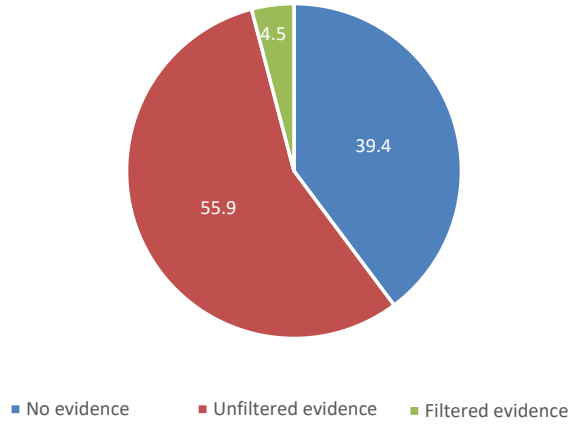


Figure 9: Evidence for the Intervention
(Average score %)

4.4 Outcomes

Q10: What are the key outcomes of interest?
No evidence: 118
Unfiltered evidence: 392
Filtered evidence: 11

Q11: Have the results shown an objective improvement in outcomes?

No evidence: 304
Unfiltered evidence: 206
Filtered evidence: 7

Q12: Are the outcomes independently evaluated?

(critically appraised or externally peer reviewed)

No evidence: 437
Unfiltered evidence: 74
Filtered evidence: 6

Average score % : (Figure 10)
No evidence: **55.38 %**
Unfiltered evidence: **43.32 %**
Filtered evidence: **1.54 %**

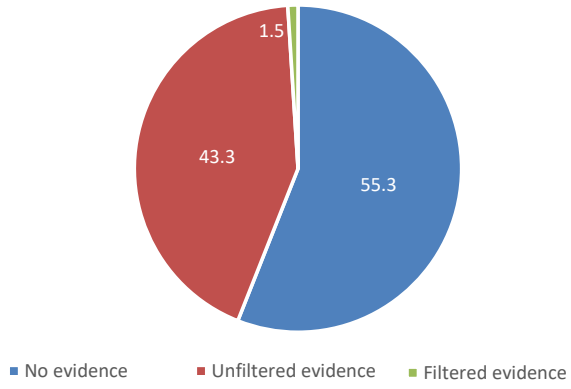


Figure 10: Evidence of Outcomes - (Average score %)

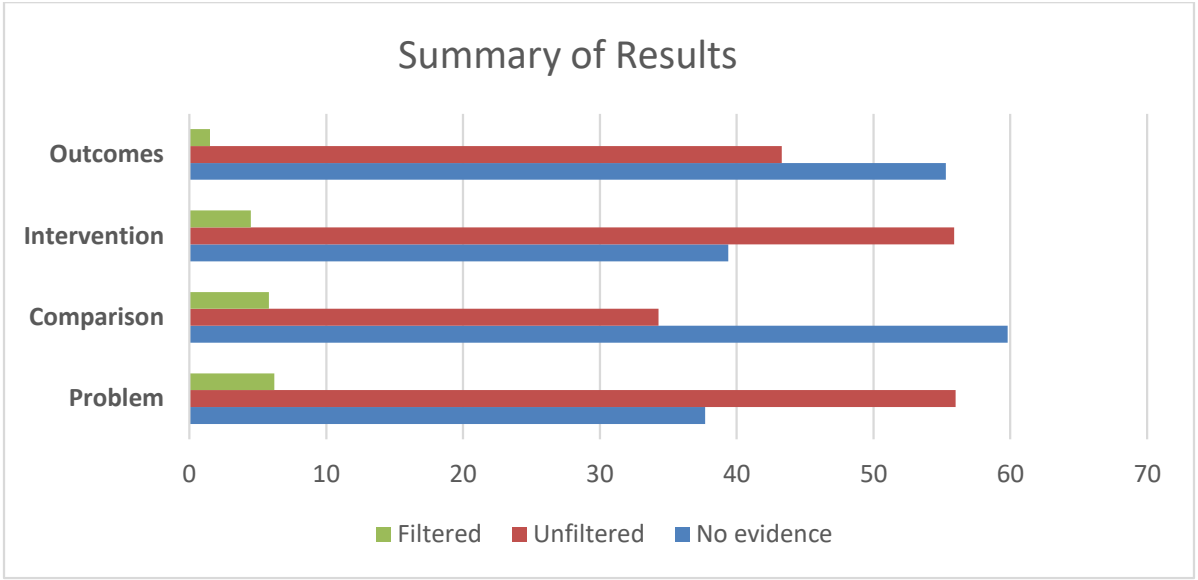


Figure 11: Summary of Results

5. Conclusion

Our study concluded that almost half of the blockchain firms show no explicit evidence of the problem to be solved. Approximately one-third fail to cite a comparison and intervention analysis, and less than 2% demonstrate evidence of outcomes backed by filtered (critically appraised, peer reviewed) information. (Figure 11).

6. Limitations

Our search for evidence was limited to the platforms described in the methodology section. However, it is possible that other research documents or pieces of evidence would have been available on search engines other than Google or Bing. That being said, we focused our search on the two widely used platforms. Similarly, our search for scientific/academic evidence was limited to the academic search engines and portals cited in the methodology section. We analysed the research evidence and other data in open access (CC-BY) journals and publications only. Some of the research evidence published in closed subscription journals could not be fully evaluated.

We were only able to collect and comment on the data provided by companies on their websites and in their white/yellow papers. It is possible that a project may have received a review from a third party that referenced the project in question.

Figure 12: Evidence Assessment Framework for Blockchain Applications

We collected the data over the six-month period between January to June 2020. Some projects might release a new version of their platform or research about their project at a later date, which we could not comment on at the time of writing this paper.

7. Discussion

Why are most practitioners not using EBB?

The reasons are multifactorial:

- Most practitioners do not know about it or how to practice it.
- They may think it is 'too academic'.
- They may oversimplify or overcomplicate issues.
- Their own beliefs and cognitive biases may prevent them from adopting it.
- Their organisational culture may be incompatible with it.

What are the risks of not following EBB?

- It is unethical not to do so.
- Waste or poor allocation of resources.
- Practitioners may adopt poor benchmarks and frameworks.
- Practitioners may engage in ineffective policymaking.

8. Recommendations

We propose an '**Evidence Assessment Framework**' (Figure 12) for all distributed ledger technology projects. This should be undertaken for all existing and new blockchain solutions before they are deployed in real-world settings. We make a case for a 'Chief Evidence Officer' for all organisations where blockchain is being deployed, to ensure that blockchain products, services and solutions are built on best available scientific evidence; this will ensure efficacy, efficiency, impact and effectiveness.

We recommended that the governments, organisations and enterprises looking to invest in blockchain projects ensure that uses of blockchain are based on scientific evidence. For every £100 spent on blockchain and distributed ledgers, we propose that at least £2 should be dedicated to making sure the other £98 actually works.

Policymakers, c-suite executives, investors and senior decision makers in blockchain should be equipped with the fundamental skills of EBB. We must ensure that they have the tools and strategies to critically evaluate both their problems and their proposed solutions. Any investments of time and resources into blockchain projects must be preceded by critical appraisal of the strengths and weaknesses of their project and its potential long-term impact. At the Centre for Evidence-Based Blockchain, we will continue to play our part in advancing the best standards in blockchain.

References:

[1] Amstat.org. 2020. Bill To Implement Evidence Based Policymaking Recommendations Becomes Law. [online] Available at: <https://www.amstat.org/asa/News/Congress-Approves-Bill-to-Implement-Commission-for-Evidence-Based-Policymaking-Recommendations.aspx> [Accessed 30 June 2020].

[2] P. R. Orszag, "One small step for sensible policymaking," Bloomberg, 23-Jan-2019. [Online]. Available: https://www.bloomberg.com/opinion/articles/2019-01-23/evidence-based-policymaking-gets-boost-from-trump. [Accessed: 30 June 2020].

[3] https://www.congress.gov/bill/115th-congress/house-bill/4174

[4] Guest Post, "Blockchain for International Development: Using a Learning Agenda to Address Knowledge Gaps - MERL Tech," Merltech.org, 29-Nov-2018. [Online]. Available: http://merltech.org/blockchain-for-international-development-using-a-learning-agenda-to-address-knowledge-gaps/. [Accessed: 30 June 2020].

[5] A. Hankin, "Blockchain companies go silent when their tech promises fall short, research group finds," MarketWatch, 04-Dec-2018. [Online]. Available: https://www.marketwatch.com/story/blockchain-companies-go-silent-when-their-tech-promises-fall-short-research-group-finds-2018-12-04. [Accessed: 30 June 2020].

[6] Finance Magnates | Financial and business news. 2020. Failed Expectations: Why 86% Of ICOs Are Worth Less Than When They Started. [online] Available at: <https://www.financemagnates.com/cryptocurrency /news/failed-expectations-why-86-of-icos-are-worth-less-than-when-they-started/> [Accessed 30 June 2020].

[7] "WEF 2016: What financial leaders said about bitcoin and blockchain," Coinjournal.net, 27-Oct-2017. [Online]. Available: https://coinjournal.net/news/vitalik-buterin-90-icos-will-fail/. [Accessed: 30 June 2020].

[8] N. Naqvi, "Editorial, Volume 1, Issue 2, December 2018," The JBBA, vol. 1, no. 2, 2018.

[9] https://cebma.org/wp-content/uploads/Evidence-Based-Practice-The-Basic-Principles-vs-Dec-2015.pdf

[10] E. Larson, "Don't fail at decision making like 98% of managers do," Forbes Magazine, 18-May-2017

[11] 2020. [online] Available at: <https://www.tandfonline.com/doi/full/10.1080/12460125.2019.1646509> [Accessed 30 June 2020].

[12] M. Stanley, "The application of behavioural heuristics to Initial Coin Offerings valuation and investment," The JBBA, vol. 2, no. 1, 2019.

[13] Jstor.org. [Online]. Available: https://www.jstor.org/stable/10.7864/j.ctt7zsvr9. [Accessed: 30 June 2020].

[14] Nih.gov. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/. [Accessed: 30 June 2020].

[15] Researchgate.net. [Online]. Available: https://www.researchgate.net/publication/. [Accessed: 30 June 2020].

[16] R. Smith and D. Rennie, "Evidence-based medicine—an oral history," JAMA, vol. 311, no. 4, pp. 365–367, 2014.

[17] R. M. Harden, J. Grant, G. Buckley, and I. R. Hart, Adv. Health Sci. Educ. Theory Pract., vol. 5, no. 1, pp. 71–90, 2000.

[18] J. Pfeffer and R. I. Sutton, "Evidence-Based Management," Harvard business review, 01-Jan-2006.

[19] https://media.nesta.org.uk/documents/evidence_for_social_policy_and_practice.pdf

[20] A. S. Burke, "SOU-CCJ230 introduction to the American criminal justice system," 2019.

[21] "Evidence-based cybersecurity research group," Gsu.edu. [Online]. Available: https://ebcs.gsu.edu/. [Accessed: 30 June 2020].

[22] A. Carter, "Evidence-Based Nursing," Rcni.com, 09-May-2017. [Online]. Available: https://rcni.com/write-us/explore-our-journals/evidence-based-nursing-85406. [Accessed: 30 June 2020].

[23] G. R. Bond, "Supported employment: evidence for an evidence-based practice," Psychiatr. Rehabil. J., vol. 27, no. 4, pp. 345–359, Spring 2004.

[24] P. Raynor, "Evidence-based probation and its critics," Probation J., vol. 50, no. 4, pp. 334–345, 2003.

[25] "CEBB," Britishblockchainassociation.org. [Online]. Available: https://www.britishblockchainassociation.org/cebb. [Accessed: 30 June 2020].

[26] D. Liebau and P. Schueffel, "Cryptocurrencies & Initial Coin Offerings: Are they scams? - an empirical study," The JBBA, vol. 2, no. 1, 2019.

[27] "Blockchain: A solution in search of a problem?," Cgap.org. [Online]. Available: https://www.cgap.org/blog/blockchain-solution-search-problem. [Accessed: 30 June 2020].

[28] S. Correa, "Crypto governance: Analysing and comparing platforms for crypto assets trading," The JBBA, 2020.

[29] R. W. Greene and D. L. K. Chuen, "Singapore's open digital token offering embrace: Context & consequences," The JBBA, 2019.

[30] J. Pazos, "Valuation of utility tokens based on the quantity theory of money," The JBBA, vol. 1, no. 2, 2018.

[31] J. Pazos, "Valuation method of equity-based security token offerings (STO) for start-up companies," The JBBA, vol. 2, no. 1, 2019.

[32] M. Novak and A. Pochesneva, "Toward a crypto-friendly index for the APEC region," The JBBA, vol. 2, no. 1, 2018.

[33] S. Schwerin, "Blockchain and privacy protection in the case of the European General Data Protection Regulation (GDPR): A Delphi study," The JBBA, vol. 1, no. 1, 2018.

[34] C. Castro-Iragorri, F. Lopez-Gomez, and O. Giraldo, "Academic Certification using Blockchain: Permissioned versus Permissionless Solutions," The JBBA, 2020.

[35] A. Shahaab, R. Maude, C. Hewage, and I. Khan, "Managing gender change information on immutable blockchain in context of GDPR," The JBBA, 2020.

[36] N. Naqvi and M. Hussain, "Medical Education on the blockchain," The JBBA,

vol. 1, no. 2, 2018.
[37] D. W. E. Allen, A. Berg, and B. Markey-Towler, "Blockchain and supply chains: V-form organisations, value redistributions, DE-commoditisation and quality proxies," The JBBA, vol. 2, no. 1, 2019.
[38] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," The JBBA, vol. 1, no. 1, 2018.
[39] D. Uribe and G. Waters, "Privacy laws, genomic data and non-fungible tokens," The JBBA, 2020.
[40] S. F. Dyson, "Blockchain investigations - beyond the 'money,'" The JBBA, 2019.
[41] N. Naqvi, "Interview with Chrissa McFarlane," The JBBA, vol. 1, no. 2, 2018.
[42] S. Herko, "A blockchain infrastructure for transportation in Low Income Country Cities, and beyond," The JBBA, 2019.
[43] D. Chen, "Utility of the blockchain for climate mitigation," The JBBA, vol. 1, no. 1, 2018.
[44] F. Knauer and A. Mann, "What is in it for me? Identifying drivers of Blockchain acceptance among German consumers," The JBBA, 2019.
[45] L. Laidin, K. A. Papadopoulou, and N. A. Dane, "Parameters for Building *Sustainable Blockchain Application Initiatives," The JBBA, vol. 2, no. 1, 2019.*
[46] P. Goorha, "Blockchains as Implementable Mechanisms: Crypto-Ricardian Rent and a Crypto-Coase Theorem," The JBBA, vol. 1, no. 2, 2018.
[47] J. Reynolds, "The Internet of Public Value," The JBBA, vol. 1, no. 1, 2018.
[48] A. Shahaab, R. Maude, C. Hewage, and I. Khan, "Blockchain - A Panacea For Trust Challenges In Public Services? A Socio-technical Perspective," The JBBA, vol. 3, no. 2, 2020.
[49] J. O. Atherton, A. Bratanova, and B. Markey-Towler, "Who is the blockchain employee? Exploring skills in demand using observations from the Australian labour market and behavioural institutional cryptoeconomics," The JBBA, vol. 3, no. 2, 2020.
[50] D. W. E. Allen and C. Berg, "Blockchain Governance: What we can Learn from the Economics of Corporate Governance," The JBBA, vol. 3, no. 1, 2020.
[51] A. Ferreira, "Emerging regulatory approaches to blockchain based token economy," The JBBA, 2020.
[52] W. Buchanan, S. Dyson, and L. Bell, "The challenges of investigating cryptocurrencies and blockchain related crime," The JBBA, vol. 1, no. 2, 2018.
[53] K. Curran, "E-Voting on the Blockchain," The JBBA, vol. 1, no. 2, 2018.
[54] S. O. Husain, D. Roep, and A. Franklin, "Prefigurative post-politics as strategy: The case of government-led blockchain projects," The JBBA, vol. 3, no. 1, 2020.
[55] M. Atzori, "Blockchain governance and the role of Trust Service Providers: The TrustedChain® network," The JBBA, vol. 1, no. 1, 2018.
[56] E. P. Moro and A. K. Duke, "Distributed ledger technologies and the internet of things: A devices attestation system for smart cities," The JBBA, vol. 3, no. 1, 2020.
[57] R. Campbell, "The need for cyber resilient enterprise distributed ledger Risk Management Framework," The JBBA, vol. 3, no. 1, 2020.
[58] R. Campbell, "Transitioning to a Hyperledger Fabric quantum-resistant classical hybrid Public Key Infrastructure," The JBBA, vol. 2, no. 2, 2019.
[59] H. Westerlund, "Academic guides: Home: Library," 2017.
[60] https://doaj.org/
[61] https://academic.microsoft.com
[62] https://www.semanticscholar.org/
[63] https://scholar.google.com/
[64] https://www.ssrn.com/
[65] https://www.researchgate.net/
[66] https://www.elsevier.com/en-gb/solutions/scopus
[67] https://www.worldcat.org/
[68] https://www.ebsco.com/
[69] https://www.openaire.eu/
[70] C. Mondschein, "Browser-based crypto mining and EU data protection and privacy law: A critical assessment and possible opportunities for the monetisation of web services," JBBA, vol. 3, no. 2, 2020.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared

Acknowledgements:
We would like to thank the entire team at the Centre for Evidence Based *Blockchain for their contributions – IT staff, statisticians, data managers, research assistants, CEBB Leads and advisors.. We would also like to thank Liz Trinder, Shirley Reynolds, Martyn Hammersley, Rob Briner, Jeffrey Pfeffer, Denise Rousseau and Robert Sutton for being a source of inspiration and future direction through their work on evidence based practice.*

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

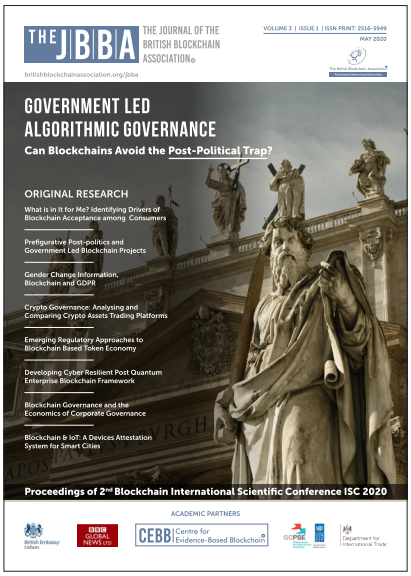
Obtain leadership experience driving BBA student chapter activities

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

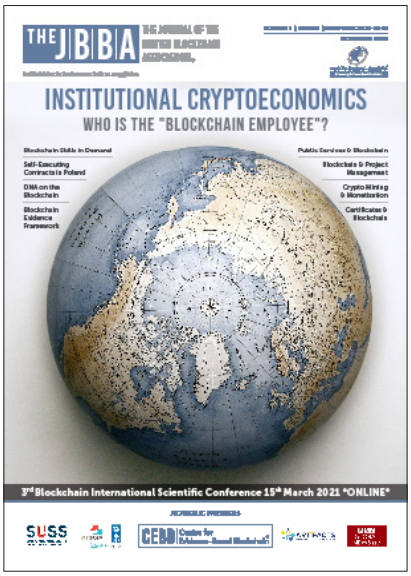
Compete in hacking events

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 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: jbba.scholasticahq.com

Advertising

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

Distribution

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

Article Submission

To submit your manuscript to The JBBA, please visit:
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 BENEFITS

- 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 February 2021)

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

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

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

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®