THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION®

VOLUME 3 | ISSUE 1 | ISSN PRINT: 2516-3949

MAY 2020

The British Blockchain Association®
Advocating Evidence Based Blockchain

britishblockchainassociation.org/jbba

GOVERNMENT LED ALGORITHMIC GOVERNANCE

Can Blockchains Avoid the Post-Political Trap?

ORIGINAL RESEARCH

What is in It for Me? Identifying Drivers of Blockchain Acceptance among Consumers

Prefigurative Post-politics and Government Led Blockchain Projects

Gender Change Information, Blockchain and GDPR

Crypto Governance: Analysing and Comparing Crypto Assets Trading Platforms

Emerging Regulatory Approaches to Blockchain Based Token Economy

Developing Cyber Resilient Post Quantum Enterprise Blockchain Framework

Blockchain Governance and the Economics of Corporate Governance

Blockchain & IoT: A Devices Attestation System for Smart Cities

Proceedings of 2nd Blockchain International Scientific Conference ISC 2020

ACADEMIC PARTNERS

British Embassy Lisbon

BBC GLOBAL NEWS LTD

CEBB Centre for Evidence-Based Blockchain®

GCPSE Global Centre for Public Service Excellence

UN DP Empowered lives. Resilient nations.

Department for International Trade

TABLE OF CONTENTS

Editorial 9

Editorial Board 10

Testimonials from Authors & Readers 14

PEER-REVIEWED RESEARCH

Prefigurative Post-Politics as Strategy: The Case of Government-Led Blockchain Projects 16

Managing Gender Change Information on Immutable Blockchain in Context of GDPR 23

Emerging Regulatory Approaches to Blockchain Based Token Eco 29

The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework 35

Crypto Governance: Analysing and Comparing Platforms for Crypto Assets Trading 42

Blockchain Governance: What we can Learn from the Economics of Corporate Governance 47

What is in It for Me? Identifying Drivers of Blockchain Acceptance among German Consumers 54

Distributed Ledger Technologies and the Internet of Things, a Devices Attestation System for Smart Cities 67

CONFERENCE PROCEEDING

Cryptocurrencies and Cyberlaundering: the need for Regulation 73

Jurisdiction on the Blockchain 73

5 W's of workers compensation insurance, compliance and fraud 74

The need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework 74

Blockchain Governance: What we can learn from the Economics of Corporate Governance 75

Are Blockchain based systems the future of Project Management? A preliminary exploration 75

Browser-based crypto mining and EU data protection and privacy law:
a critical assessment and possible opportunities for the monetisation for web services 75

Algebraic methods in the analysis of persistency of attacks in decentralised systems 76

Blockchain to negate Malware 76

Distributed Ledger Technologies and Internet of Things, a Devices Attestation System for Smart Cities 76

Privacy Laws, Non-fungible-tokens and Genomics(DNA) 77

Transformation or Adaptation of Blockchain at Crossroad of Institutional to Distributed Trust Journey?
A Public Sector Perspective 77

Modern portfolio theory: a Blockchain theoretical model 77

Cost Benefit Analysis of Permissioned and Permissionless Blockchain solutions 78

Emerging Regulatory Approaches to Blockchain Based Token Economy 78

Using Blockchain for Evidence purpose in Civil Cases in Poland 78

Solidity+ : A language for Robust programming of Smart Contracts 79

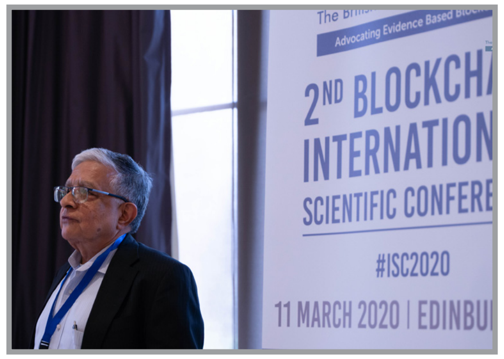
A Peer-To-Peer Publication Model on Blockchain 79

2ND BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
11 MARCH 2020, EDINBURGH

Photos by Bircan Birol

The British Blockchain Association
Advocating Evidence Based Blockchain
BLOCKCHAIN

The British Blockchain Association
2ND BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2020
11 MARCH 2020 | EDINBURGH | UK
CONFERENCE PARTNERS
Motivation


The British Blockchain Association
Advocating Evidence Based Blockchain
2ND BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2020
11 MARCH 2020 | EDINBURGH

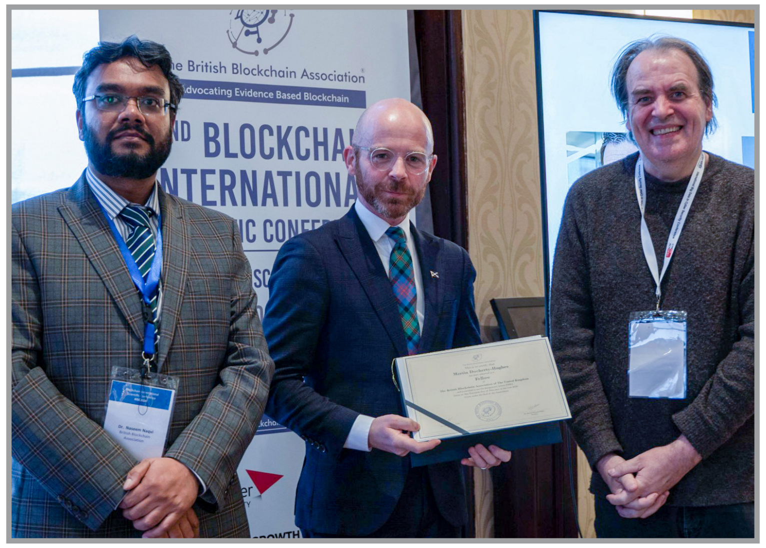
The British Blockchain Association
Bridging the Blockchain Research and Practice Gap
CEBB
JBBA

The British Blockchain Association
2ND BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2020
11 MARCH 2020 | EDINBURGH
CONFERENCE PARTNERS

The British Blockchain Association
Advocating Evidence Based Blockchain
BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2020
20 | EDINBURGH
CERTIFICATE OF PARTICIPATION

The British Blockchain Association
Advocating Evidence Based Blockchain
CERTIFICATE OF PARTICIPATION

The British Blockchain Association
Advocating Evidence Based Blockchain
BLOCKCHAIN INTERNATIONAL CONFERENCE


The British Blockchain Association
Advocating Evidence Based Blockchain
BLOCKCHAIN INTERNATIONAL

The British Blockchain Association
BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE

2ND BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2020
11 MARCH 2020 | EDINBURGH | UK
CONFERENCE PARTNERS

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

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 THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION is a trade mark of the Journal of the British Blockchain Association.

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

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

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

DOAJ DIRECTORY OF OPEN ACCESS JOURNALS   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:

Crossref   PORTICO   REVIEWER CREDITS Registered Journal   ARTiFACTS BUILDING THE LEDGER OF RECORD FOR RESEARCH   ed!tage by CACTUS   publons

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

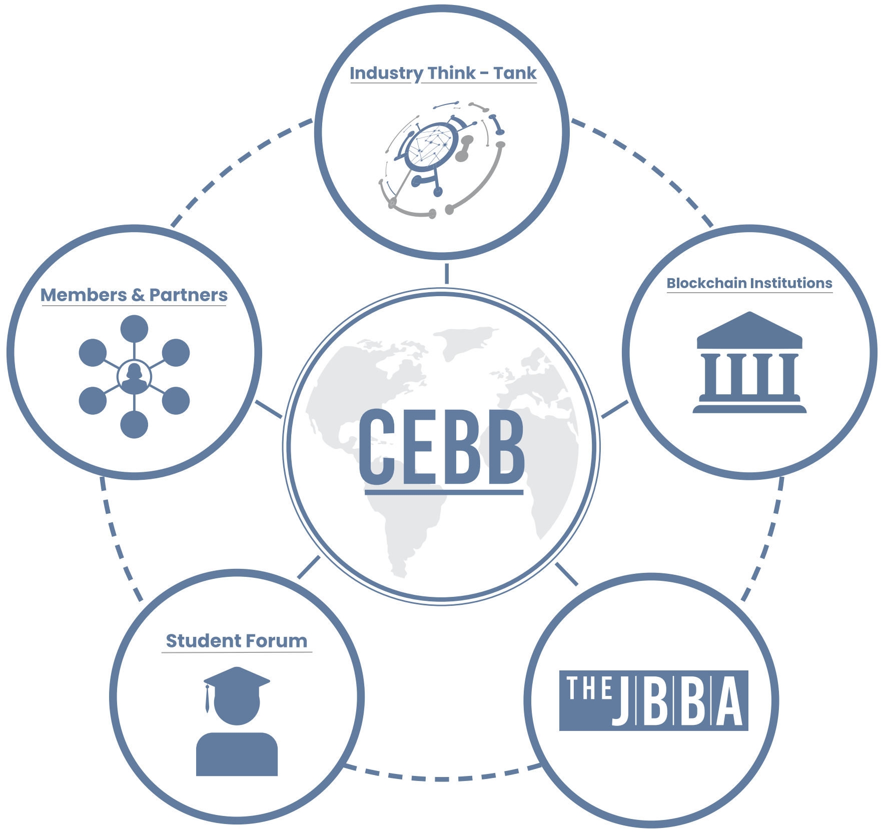
All advertisements and sponsorships are expected to conform to ethical and business standards. The appearance of an advertisement or sponsorship material does not constitute an endorsement by the British Blockchain Association or by the Editor of this Journal.

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



EDITORIAL

It gives me great pleasure to introduce the fifth issue of the Journal of the British Blockchain Association. This edition comes at a time of profound uncertainty around the globe, as societies take extraordinary measures to curb the spread of COVID-19. The JBBA salutes healthcare workers and other workers doing their essential work in the frontlines and expresses our appreciation for their commitment to this fight. The pandemic is having a profound effect on our lives and livelihoods. While life as we know it may have temporarily come to a halt, the JBBA, with the commitment of its contributors, continues its mission of publishing the best, evidence-based research that pushes the boundaries of blockchain technology.

The following papers were accepted for publication in this issue:

'Prefigurative Post-Politics as Strategy: The Case of Government-Led Blockchain Projects', 'Managing Gender Change Information on Immutable Blockchain in Context of GDPR', 'Emerging Regulatory Approaches to Blockchain-Based Token Economy', 'The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework', 'Crypto Governance: Analysing and Comparing Platforms for Crypto Assets Trading', 'Blockchain Governance: What we can Learn from the Economics of Corporate Governance', 'What is in It for Me? Identifying Drivers of Blockchain Acceptance among German Consumers' and 'Distributed Ledger Technologies and the Internet of Things, a Devices Attestation System for Smart Cities'.

These research papers address timely and essential issues of governance, government-led initiatives, strategy, regulation, risk management, incentives, and project management in blockchain development. The JBBA is delighted to publish cutting-edge research that broadens the frontiers of blockchain knowledge. The authors of these papers are respected researchers and scientists who understand the importance of having a conducive environment for blockchain innovation and the appropriate conditions for social scalability.

Under the leadership of our Editor in Chief, Dr Naseem Naqvi, and the journal's editorial board, the JBBA has developed a strong reputation for bringing together thoughtful research on the most dynamic areas of blockchain technology. The journal is regularly receiving tens of thousands of page views and thousands of unique visitors each month from more than 150 countries and territories. It has become an engine-driver for the industry, stimulating exchange, exploration and implementation of ideas - I am delighted to be involved in many of the JBBA's projects.

Here I would like to thank all contributors for their support of the Journal - To the authors, for trusting us with your work and the task of making it available open access to major universities and research centres - To the reviewers and fellow editors for their devotion to maintaining the highest standards in this publication - To the BBA staff for their contributions to the smooth production of each edition of the Journal - and last, but not the least - to our extended global network of academic partners, friends and well-wishers for their ongoing support.

I hope that the papers in this edition will be useful and edifying. As always, we welcome your comments and suggestions to assist the Journal in meeting the needs of the blockchain community.

Yours truly

Professor David Lee Kuo Chuen PhD FBBA
Associate Editor-in-Chief

EDITORIAL BOARD

TESTIMONIALS FROM AUTHORS AND READERS

“ "I always enjoy reading the JBBA."

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

“ 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 ”

“ 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 ”

PEER-REVIEWED RESEARCH

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

Prefigurative Post-Politics as Strategy: The Case of Government-Led Blockchain Projects

Syed Omer Husain[1], Dirk Roep[1], Alex Franklin[2]
[1]Rural Sociology Group, Wageningen University, The Netherlands
[2]Centre for Agroecology, Water and Resilience, Coventry University, UK
Correspondence: omer.husain@gmail.com

Received: 23 October 2019 **Accepted:** 25 November 2019 **Published:** 14 December 2019

Abstract

Critically engaging with literature on post-politics, blockchain and algorithmic governance, and drawing also on knowledge gained from undertaking a three-year empirical study, the purpose of this article is to better understand the transformative capacity of government-led blockchain projects. Analysis of a diversity of empirical material, which was guided by a digital ethnography approach, is used to support the furthering of the existing debate on the nature of the post-political as a condition and/or strategy. Through these theoretical and empirical explorations, the article concludes that while the post-political represents a contingent political strategy by governmental actors, it could potentially impose an algorithmically enforced post-political 'condition' for the citizen. It is argued that the design, features and mechanisms of government-led projects are deliberately and strategically used to delimit a citizens' political agency. In order to address this scenario, we argue that there is a need not only to analyse and contribute to the algorithmic design of blockchain projects (i.e. the affordances and constraints they set), but also to the metapolitical narrative underpinning them (i.e. the political imaginaries underlying the various government-led projects).

Keywords: *blockchain, post-political, decentralization, e-government, technopolitics, prefigurative politics, digital ethnography, civic tech*

1. Introduction

A growing body of thought has begun to theoretically and empirically investigate the dynamics of contemporary depoliticization and the alleged 'disappearance of the political'. Uniting a diverse set of opinions is the idea that "contemporary forms of depoliticization are characterized by the erosion of democracy and the weakening of the public sphere, as consensual mode of governance has colonized, if not sutured, political space" [1, p. 5]. This emerging literature across the social sciences conceptualizes the processes as 'post-politics', 'post-political' and 'post-democratic' [2]–[5]. An important debate within this highly contested sphere concerns the nature of the post-political itself: whether it is a "condition" of contemporary society or a "contingent political strategy" imposed upon it to shrink political agency [6, p. 39]. Using blockchain as a civic or political technology, that could potentially transform political agency, as well as, political processes, has become an oft-cited claim [7]–[9]. While there are many empirical studies that use the lens of the post-political to explore, for instance, governmentality [10], social enterprise [11] or radical politics [12], we think government-led blockchain projects provide an apt case for addressing some of the crucial questions surrounding the post-political.

It is argued that blockchain projects personify "prefigurative politics" [13] by design: they embody the politics and power structures they want to enable in society. These technopolitical systems achieve this by setting certain "affordances and constraints" [14, p. 726] i.e. the possible courses of action available to an actor. Through this, such systems can influence the behaviour, outcomes, and so forth of any individual taking part in a political process or action within or through it. In other words, the design of these systems prefiguratively determines the agency actors have while using the system. As explained elsewhere, these contingences are deeply political, where they are specifically set up by the designers to delimit an actor's political agency (anon, forthcoming) [15]. Moreover, particular political imaginaries guide and inform how and why these contingencies will be set up within the system. If governments are beginning to experiment with blockchain as a technopolitical infrastructure to restructure governance, and allegedly, alter the political agency of citizens, it becomes fruitful to investigate why and how from a post-political perspective. In that, the aim of this discussion paper is two-fold: first, to reflect upon whether and how government-led blockchain projects are politically transformative; and second, in follow on, to contribute to existing debate on the nature of the post-political as a condition and/or strategy.

The fundamental question this paper aims to explore is whether all government-led technopolitical projects (blockchain or otherwise) are inevitably confined within or structured by the 'post-political condition'? Alternatively, is the post-political a strategy that is being actively implemented to curtail and delimit a citizen's political agency, and, by effect, recentralize power under the guise of a decentralized technopolitical system?

We begin the article by contextualizing blockchain projects in the language of the post-political literature. After a note on methods, we analyse and discuss our empirical findings. In drawing the discussion to a conclusion, we return to the research questions, reflecting also on whether and how blockchain projects can avoid the "post-political trap" [6].

2. The prefigurative post-politics of crypto-anarchists and crypto-institutionalists

Within the blockchain space, one way of understanding the different types of projects is by clustering them. Two higher level clusters of blockchain projects have previously been categorized as: crypto-anarchists and crypto-institutionalists (anon, forthcoming) [15]. The prior cluster denotes initiatives that use blockchain as government, while the latter use it in, for and with government. In this article, we will focus on the latter, crypto-institutionalists, which comprise predominantly of government-led blockchain projects. There are estimated to be more than 100 of such projects currently attempting to transform governmental systems in more than 40 countries [16, p. 1]. Moreover, IBM's executive report claims that 9 in 10 governmental organizations will invest in blockchain in 2018 and that "a group of government organizations are embracing blockchain technology to reduce frictions to innovation and information and facilitate more extensive collaboration", which will stimulate trust between citizens and government [17, p. 1]. Blockchain as, in, for and with government is, however, a highly contestable field of study – including, for example, in academic literature [18], online spaces (Slack teams of various projects[i]), popular media [19], governmental reports [20] and even European Commission launched forums [21]. This contestation, much of it surrounding blockchain's transformative potential, can be understood historically. Bitcoin (whose underlying technology is blockchain), for instance, was launched in the midst of the 2008 economic crash and accompanying democratic crisis, as a response to the features of what is now commonly referred to as the 'post-political condition'. Bitcoin was to enable individuals to politically exit from the dominant financial system, while blockchain became the prospective 'liberator' from all other state and corporate run institutions [22].

While the precise nuances of the post-political condition are contestable, the general consensus is on the fact that the genuinely political has vanished [5], [23], [24] and "the parameters of political discussion and political action have narrowed to preclude alternatives to neoliberalism" [6, p. 33]. Swyngedouw, following the post-foundational theorists like Badiou, Mouffe, Ranicière and Žižek, explains that the post-political:

"refer to a situation in which the political – understood as a space of contestation and antagonistic engagement – is increasingly colonised by politics – understood as technocratic mechanisms and consensual procedures that operate within an unquestioned framework of representative democracy, free market economics, and cosmopolitan liberalism" [1, p. 6]

While this widely shared belief is useful in grasping the general idea, it is the subtleties of post-political conceptualizations which arguably provide a more fertile ground to investigate blockchain projects. Mouffe believes that the hegemonic economic regime has not completely obliterated the political, but rather "repressed" it [5, p. 18]. She believes that there is an absence or lack of political channels that can challenge the "hegemony of the neoliberal model of globalisation" [1, p. 12]. For Rancière, it is not repression, but rather, three types of "disavowal" that explain the post-political: archi-politics (closed communitarian groups such as nationalists), para-politics (where political conflict is reformulated to fit in the representative democratic system), and meta-politics (where politics is reduced to systemic governing of things rather than people) [25, pp. 60–95]. Žižek adds another layer, by explaining that politics is not merely repressed or disavowed in post-politics, but "foreclosed"; it asks us to "leave old ideological divisions behind and confront new issues" [26, p. 188]. In other words, for Žižek, the contemporary political system effectively places the genuinely political outside of the realm of possibilities.
In sum, we can see most of the post-foundational theorists believe that exercise of genuine political agency can only be from outside of the dominant institutional setting. Similar to the conceptualization of blockchain projects, the global socio-economic system seems to prefiguratively embody values and features of the post-political condition: global consensus, economic logic and depoliticization. In the language of blockchain studies, this could be rephrased as depoliticization by design. In any techno-social system that is depoliticised by design, the "potentialities and plurality of agencies are reduced to the heroic, anti-heroic and demagogic" [6, p. 36]. For instance, in the blockchain space, crypto-anarchists consider Bitcoin as a technological 'hero', which (debatably) operates outside of dominant institutional systems of finance and economics [27].

In fact, blockchain projects are polarized between those creating parallel systems outside the dominant institutional setting (crypto-anarchists) and those providing efficiency gains within it (crypto-institutionalists) [28, p. 4]. Though very different political imaginaries guide these projects, both groups seem to depoliticise in some way. They share an appeal to, and utilization of, blockchain's oft-cited design principles: access, disintermediation, decentralization, empowerment and equality [7]. For instance, Bitcoin, as global cryptocurrency, is disintermediated from traditional intermediaries of the financial system such as central banks and stock exchanges. However, its so-called technological hero is an algorithm, which effectively depoliticizes its economy by automating it. There is no agent (governmental or otherwise) politically responsible for its fair functioning (at least, not yet).[ii] Similarly, government-led blockchain projects that decentralize services, or disintermediate processes, by effect, also depoliticize them in that they 'foreclose' any possibility of an exercise of (political) agency. Hypothetically, by automating a governance service like a petition system using blockchain, it could be argued that the political responsibility of the service is handed over to the algorithm. However, the political power could and would remain with the government in two ways: first, the government chooses the affordances and constraints and therefore, delimits an individual's agency by design; second, it leaves itself an affordance to choose or veto certain decisions.

This leads us back to our main question: with regards to government-led blockchain projects, is the post-political a societal condition or a politically contingent strategy to recentralize power?

3. Methods: digital ethnography and experts

The empirical data used in this article is predominantly the outcome of a three-year period of immersion in the spaces and practices of blockchain initiatives of the first author. Following a digital ethnography approach, we acknowledged that the "digital has become a part of the material, sensory and social worlds that we inhabit, and the implications there are for ethnographic research" [29, p. 7]. The socio-political and innovation worlds of blockchain are, in part, so fast-paced because of their hybrid nature: geographical, temporal and practical obstacles are less of a hinderance because of the features and possibilities of the digital. Any developments within the field, whether narrative building, political actions, decision making, or planning, take place both online and offline. Hence, only a methodological approach that is responsive to this online-offline dynamic is appropriate and adequate for research in this space.

For this research, we began to search for the social worlds where blockchain innovation for political change was taking place. Unruh expounded that the concept of the "social world" refers to "a form of social organization which cannot be accurately delineated by spatial, territorial, formal or membership boundaries" but instead, by lines and channels of communication and interaction [30, p. 271]. Hence, as digital ethnographers, we entered the hybrid (online and offline) social world of blockchain innovation to understand the communication norms, rules, networks, behaviors, activity infrastructures and operational structures. The socio-political worlds of blockchain and civic tech were located on team collaboration platforms such as Slack, online forums such as Reddit, blogs, social media platforms, conferences, Meetups, GitHub projects and hackathons. Their depth, interrelationships, networks and infrastructure were vastly diverse. While there are many purely online data sources used, this did not replace gathering data from institutional actors and experts that were only accessible in-person. Different methods were used to collect data across the different sites, but were guided by: (i) everyday immersion routines and participant observation (following debates daily); and (ii) participatory action (starting and contributing to online debates, conducting workshops, participating in hackathons and other long-term events). Data used for reflection was mainly in the form of:

a) Field notes and diary reflections: theoretical and praxis-based reflections engaging in many spontaneous conversations at blockchain events with practitioners, figureheads, government officials, coders, researchers and activists.

b) Online immersion routine (participant observation): daily and weekly involvement in forums and working groups; mapping and following the debates.
i) 6 team collaboration platforms (unnamed) and 4 Reddit Forums

c) Digital social archiving: data (mainly in the form of linked pages) formed visual mind-maps with descriptions and storyboards on software such as Pearltrees and Raindrop which are open for the public collaboration and recommendations.

d) Experts: reflexive and tailored interview methods (from semi-structured to informal) for consulting experts; recorded in audio and/or non-verbatim notes. Twenty-five semi-structured and informal expert interviews were used for reflection in this article. They were conducted at numerous events, meetings and forums occurring between September 2016 to August 2019. While the names of the experts are kept anonymous at their request, the geographical location of the events are included:
i) EU Parliament 'spotlight on blockchain' and relevant European Commission working groups at the Week of Regions and Cities (Brussels)
ii) EU Blockchain Observatory discussion groups (Brussels)
iii) Blockchain Pilots Netherlands (meetings) (The Hague, Amsterdam)
iv) Dutch Blockchain Coalition (meetings)(Amsterdam)
v) Blockchain events in Amsterdam (Bitcoin Wednesday and misc. Meetups)
vi) Blockchain Live London – GovTech stream
vii) Welsh Council for Voluntary Action (meetings and workshop) (Cardiff)
viii) Satori Labs, (Cardiff)
ix) Ex civil servants in Welsh Government (Cardiff)
x) Welsh Government Chief Technology Office (Cardiff)
xi) Decode (EU project – Amsterdam)
xii) D-Cent (EU project – Amsterdam)
xiii) P2P Models (ERC Project – Spain/Online)

All this data was used in concert with an analytical frame comprising of three core themes: blockchain and government, post-political theory and algorithmic governance. For field notes, interviews and diary reflections: open coding according to grounded theory comprised of 'conceptual labelling' which later developed into the two clusters of blockchain innovation (crypto-institutionalists and crypto-anarchists). These higher-level categories were used to find relationships within and between projects leading to an abstract variation of axial coding, on paper. Furthermore, the most interesting data to analyse was nuances and divisions between the different social worlds of innovators which would rarely interact with each other. The use of the same terms and language (such as decentralization, disintermediation, access etc.) with completely different meanings added a layer of complexity which prohibited us from using traditional forms of coding. Interviewees and forum/team participants were asked to reflect on patterns and categories to validate and cross-check the inferences.

4.1. Shrinking political agency by algorithm

There is a growing body of literature that refers to algorithmic governance as a technological model of governance that leads to the formulation of political practices [31]–[34]. These scholars engage with the strategies that lead to new forms of decision-making and governance through algorithms. They identify how code, data and technical infrastructure (software) are core features underlying the new modes of governance [35]–[37]. These studies claim and explain how algorithms form new affordances and constraints, new modulations of command and control, and new processes for political engagement and subjectivation. Ontic politics, in this domain, is the study of how a citizen's political agency is produced within an algorithmic institutional setting. Critical theorists in this field align themselves with post-foundational theorists, claiming that algorithmic governance essentially entails the depoliticization or subjectivation of the political sphere. For instance, Rouvroy claims that algorithmic governmentality constitutes the disappearance of the political subject [34], where individual agency is subjugated by data metrics such as norm, consensus drivers and protocols.

As Lessig elaborates, algorithmic governance signals the ascendance of technopolitical infrastructure over normative and judicial infrastructure [38]. Accordingly, "code has progressively established itself as the predominant way to regulate the behaviour" [39]. With blockchain and smart contracts, some scholars see a shift from 'code is law' (code has the effect of law) to 'law is code' (law is actively being defined as code). While the judicial system is enforced "ex-post" (after the event) through state intervention, algorithmic systems enforce it "ex ante" (before the event) through code [39]. This sort of "power through the algorithm" [40] prefiguratively determines what is and is not allowed, where the government could remove the possibility of disobedience altogether [41]. For instance, several governments[iii] are experimenting with a land registry system on the blockchain, which would use smart contracts to "increase transparency, speed and trust in property transactions" [42]. Taking the case of Georgia, the National Agency of Public Registry (NAPR) regulates all property transactions in that the blockchain is "private with regards to who can validate the transactions" [43, p. 19]. Though the transparency of this system leads to security and reliability of land titles, it also implicitly means that the only actors with an affordance to commit fraud is NAPR itself. A case study by the JRC shows that the project "does not provide any disintermediation of organizations nor replaces any existing system" [43, p. 20]. Thus, it is safe to assume that while political disobedience is prefiguratively constrained by the algorithm, political power remains with the same actors. Political power is effectively recentralised under the pretence of a decentralized governance system.

Data arising from our own empirical research further supports the claim that most crypto-institutional projects have similar aims. One interviewer explained that blockchain from their government's perspective is not experimented with to alter power relations or decision-making procedures, but rather "automate" processes that no longer require "politicians to be responsible". Another respondent reiterated "efficiency gains and cost-cutting" are the primary reasons for experimenting with blockchain, rather than "altering political agency of citizens". Similarly, our interactions and immersion in the world of 'GovTech' (technology for (e-)government) at conferences and online spaces, highlighted analogous themes of 'handing over responsibility', 'algorithm-ing', simplifying and enhancing political processes. These intentions and themes, albeit not always explicitly, nor with bad intentions, pointed in the direction of depoliticization as an active strategy employed by governmental actors.

4.2. Meta-political reduction to economic order building

Earlier, we mentioned how the dominant economic regime has repressed, disavowed or foreclosed the political from being actualized in the post-political condition [5], [25], [26]. Similarly, we can note that post-politics in "institutional terms is defined by the reduction of the political to the economic – the creation of 'welcoming business environment', which inspires 'investor confidence'" [1, p. 8]. A prime example of this logic is Estonia's e-residency program [44], [45]. Estonia is regarded as the pioneer in e-government leveraging blockchain and other emerging technologies for managing public affairs. Within their multiple programs, e-residency is "essentially a commercial initiative" that functions as an "international passport" to the virtual business world for anyone to carry out commercial activities [46]. "Like citizens and residents of Estonia, e-residents receive a government-issued digital ID and full access to Estonia's public e-services. This enables them to establish a trusted EU business with all the tools

needed to conduct business globally" [47]. In this scheme Estonian authorities hold and control data, and arguably use e-residency as a "tool for exerting power as knowledge" [48]. We gathered data to understand the affordances and constraints that the e-residency would impose and how it would regulate the behaviour of an individual. This data was tabulated and fit into the patterns identified within the crypto-institutional space. Furthermore, it also offered cross-validation for the categories assigned to identify differing political imaginaries [15].

Our expert interviews and conversations with crypto-institutionalists, as well as document analysis of vision statements and white papers, show how the Estonian digital project allows for an efficient acceleration of global economic order building. Interviewees were presented prompts about e-Estonia (and other crypto-institutional systems) and were asked to reflect and debate these statements. These corroborated patterns identified from the immersion and digital ethnography of the crypto-institutional space. We found that the Estonian experiments fit neatly within the category of crypto-institutional projects where there is a recentralization of power through data management. Moreover, decision making power and political processes are relatively unchanged, albeit more efficient and transparent. The project may claim to transform political agency of the citizen, yet, our findings failed to demonstrate any systematic way this was taking place. With regards to the changing role of the citizen or resident and enable more participation, our findings resonated with others claiming that citizens are depoliticized and transformed into passive "consumers" of governance services [49]. We learnt that majority of the 'benefits' for e-residents are economic, and, as such, allow an easy, reliable and geographically neutral entry into the EU economy through Estonia.

The Estonian example shows us how a national government can use a post-political blockchain strategy to simplify bureaucratic procedures, open up new markets, and create global consensus. Furthermore, it opens up its borders for business, thereby depoliticizing many local economies where place-based norms, cultures and political structures would have inhibited particular businesses from forming. Contrarily, it can also be said that by allowing detachment from the immediate geopolitical boundaries, it also allows an escape from place-based prejudices, politico-economic structures and constricting norms. While interviewing officials from two national governments (Wales and The Netherlands), we found that the intention of both their offices to use blockchain was indeed to create efficiency and speed up bureaucratic processes. Similarly, the delivery of a workshop at a national third-sector institution (anonymous, in Wales) on collaboration through the blockchain resulted in a Q&A session on the potential efficiency gains for internal management via the blockchain. During another workshop, an expert running several blockchain pilots explained how it takes a lot of cross-departmental collaboration and "traditional project work" to actually implement solutions which would change "anything political". Emblematically, the JRC even states that "contrary to how it is often portrayed, blockchain, so far, is neither transformative nor even disruptive for the public sector" [43, p. 7].

Crypto-institutionalists show us how it is possible to utilize the hype around blockchain's transformative potential to reinforce and enhance economic order building and representative democracy. As Atzori points out, democratic transformation cannot simply be "consensus ex post, typical of decentralized networks" since this would require "adequate quality and extension of participation, consensus ex ante and legitimacy of procedures, protection of minority rights, freedom of participants, and again equal opportunities of access to decision-making" [50, p. 58]. Furthermore, it could be argued that even governments that "cluster around specific interests and temporarily agree on a common set of (algorithmic) rules" [50, p. 58], depoliticize the space for transformative change. Most of the crypto-institutional strategies and rhetoric researched for this article are used to not only reinforce the processes of depoliticization of the socio-economic apparatus, but also, to structurally bound citizens from disobeying or opting for a political exit [28], [51].

4.3. The absence of collaboration in the 'political'

The research underpinning this article began by examining the different citizen-led movements that were working to create and experiment with technologies that transformed the democratic political process. Their efforts were perceived as being rooted in Europe's democratic deficit [52], lack of participation and collaboration in governance [53], and more generally in political apathy towards government. The radical municipalist movement [54] launched city-platforms for collaborative democracy, participatory budgeting, open consultation and direct democracy projects. In an earlier article, we called this phenomenon 'place-based civic tech': citizen engagement technology co-designed by local government, civil society and global volunteers [55]. We noted that "combining online tools with offline collaborative practices presents a unique opportunity for decentralization of power and decision-making" [55]. These initiatives attempt to transform the apparatus of the dominant system by working with it. In the blockchain space, we see some of the same rhetoric of the civic tech movement, but a completely different typology of projects. None of the projects in Jun's extensive survey of government-led blockchain projects, for example, explicitly leads to a change in democratic processes or participation [16, pp. 3–6]. Conversely, as another study asserts, blockchain experiments can even enable a sort of "technological populism" by exploiting "the rhetoric of empowering the disenfranchised through decentralized decision-making process, enabling anonymous of transactions, dehumanizing trust (trust in computation rather than trust in humans and institutions)" [56].

While carrying out our digital ethnography, by being involved in the online and offline social worlds, carrying out interviews, and attending various digitally mediated events, one of the predominant themes we noted was the complete separation of the crypto-anarchist projects (i.e. blockchain as government) from the crypto-institutional projects (i.e. blockchain in, for and with government). The paradox of projects operating in parallel planes sheds light on the power of the post-political condition. As asserted earlier, the post-political casts true political agency only on those acts that operate outside and beyond the dominant institutional setting. From this perspective, all crypto-anarchist projects would be genuinely political as they attempt to create new worlds as opposed to work within the established system. Mouffe would, we anticipate, disagree with this approach explaining that strategies to overcome hegemonic forces must engage with "visible nodes of power, which ultimately are apparent in existing institutions of politics" [6, p. 37]. If any blockchain approach fails in doing so, it denies the political potential and "reproduces the very post political condition it wants to attack – by not directly engaging with the institutions of power through which it operates" [6, p. 37].

Two of our interviewees voiced the opinion that blockchain practitioners have several lessons to learn from the ethos and functioning of civic technologists. Another one of our interviewees, who piloted several crypto-institutional projects, lamented about how actors from both sides of the spectrum wholly refuse any form of collaboration or cross-learning. Furthermore, this interviewee stated how some of the most fascinating and feasible political technologies will not make it to the mainstream precisely because of this absence in collaboration. Whereas we see the radical municipalist movement creating a "translocal geography of political action" [55, p. 12] in collaboration with local government, crypto-anarchists such as BitNation or Democracy Earth, seemingly rather create one without any established nodes of power [44], [57]. With regards to collaboration with these nodes, some scholars agree that conceptualizing the post-political as a 'condition' is politically disempowering, since it "denies the political status of less explosive forms of contestation" [1, p. 18]. It is through such experimentation that "new political formations will emerge" [11, p. 190].

4.4. The strategy of structures over agency

If the post-political is a condition that contemporary society endures, who are the agents that create and maintain it? According to most post-political thinkers, it would be the hegemonic forces of capital or the structures of representative democracy. This approach proposes that:

'Any transition initiative and governance arrangement are inevitably confined within – or dictated by – neoliberal and financialization market logics, which themselves resist their own transition. Institutional structures and socially innovative groups which do not – or insufficiently – challenge the larger political economy that frames social services…will constantly find themselves interacting in post-political, consensus-oriented governance arenas' [58]

In the context of blockchain, it would be the algorithm that creates the institutional structures which would, or would not, challenge the larger political economy. Furthermore, this shows how governmental agents actively design and implement the algorithm, which then creates and enforces contingencies upon its users. Accordingly, we would tend to agree with the critics who consider that post-politics as a field of study "is dominated by description of meta-level discourses and ultimately relies on the analysis of structures rather than agencies" [6, p. 37]. From our research, we learnt that there is a lot of misinformation about the mysterious closed-door decision making and unchanging political agendas of both crypto-anarchists and crypto-institutionalist blockchain initiatives. In fact, any ontological claim about the 'political' when it comes to the blockchain space negates the plurality and reflexivity of the agencies that operate in the field. Given that business lobbies, banks, national governments and other institutional agents heavily influence the development of the field, we learnt through our interviews that a lot of the projects are unaware of what could be called their 'post-political' strategies.

When it comes to a using blockchain in, for and with government, the two different layers of agency are easier to identify than in the judicial-democratic system. There are those who create the technical design of the system i.e. governmental actors that set the affordances and constraints, and those that participate within this system of contingencies i.e. the citizen or user. While it could be argued that the affordances and constraints are structured by the post-political condition, in this early stage of blockchain experimentation, it is clear that it is being used as a strategy to recentralize power. As one of our interviewees put it, "there's no way government is going to let this be disruptive…ceding power requires someone to cede power to, and it's not going to be an algorithm". Our data analysis pointed in the direction that though the post-political may be a strategy for the governmental actors, it is an unchangeable, and indeed ex ante set of rules for the citizens i.e. a condition.

5. Concluding remarks: can blockchain avoid the "post-political trap"?

Our main research question for this discussion paper was whether all crypto-institutionalist projects are structured by the so-called 'post-political condition' or whether the post-political is it used a contingent political strategy to delimit citizens' political agency. Drawing on the above discussion of findings, our conclusion, in response to this question is that the post-political is a contingent strategy employed by crypto-institutionalists to depoliticize various politico-economic processes. However, perhaps a more troubling finding is that it a government-imposed blockchain architecture has the potential to create an algorithmically enforced post-political condition for the citizen. In this scenario, there will not even be the symbolic room we have in contemporary representative democracy for the 'political moment', let alone contest the design of the process. Our analysis suggests that this strategy of post-political is underpinned by an almost path-dependent idea of the recentralization of power. The above cited interviewee's comment "ceding power requires someone to cede power to" helps us, however, to outline some modest suggestions of how blockchain projects can avoid the post-political trap.

The Radical Municipalist and civic tech movement give us one example of how a translocal political network and local government can be operationalized to re-politicize some aspects and features of the socio-political system. In Madrid, for example, there was a self-organized and self-managing group of citizens, along with local government officials that eagerly accept the responsibility of processes such as participatory budgets, citizen assemblies, random election [59], [60] and founding the "Madrid Citizens' Council" [61]. The political, in this space, is constantly being reconfigured and redefined to incorporate new affordances for the citizen; in the case of Madrid, for self-government. If the political imaginary underlying crypto-institutional projects continues to feature depoliticization, individualism, order building and global consensus, it becomes hard to imagine any technopolitical infrastructure enabling any sort of radical political transformation, at least with regards to a citizens' political agency. The fact, though, that we are still far from mainstream implementation of blockchain in government creates a space of hope by providing the opportunity to influence the design and implementation of the different solutions.

If we accept that blockchain, as a general-purpose technology, does have the capacity to be politically transformative, to redraw boundaries of access, empower the citizenry, create new forms of organization and re-politicise the economy, it becomes imperative for researchers, activists and governmental practitioners to collaborate in order to code new values into the architecture of these systems. Our interviewees all express the difficulty of fostering and scaling collaboration between different parties, explaining that it is necessary to be realistic about moving forward. Reflecting on our individual responsibilities and agency, it is necessary that we, as researchers and practitioners, not only analyse and contribute to the design of the crypto-institutional algorithms (i.e. the affordances and constraints they set), but also the meta-political narrative underpinning them (i.e. the political imaginaries underlying the various projects). Without investigating and influencing both, we fall into the post-political trap which focusses on structures and not agencies. One of the strategies that we explored during our research that ontologically reconfigured 'the political' was the collaborative effort through the implementation of new 'politics' in the Radical Municipalist Movement (where citizens collaborated with the local governments and global group of volunteers to enable a translocal geography of political action). As Swyngedouw and Wilson exert in ending their book, the post-political conclusion is not an "invitation to ditch forms of institutional and political organization…it calls for a new beginning in terms of thinking through what institutional forms are required at what scale and what forms of political organization are adequate to achieve this" [62, p. 309].

It is widely held that the politics and political imaginaries of blockchain require urgent cross-disciplinary attention to guide both conceptualization and experimentation [50], [63]–[68]. This discussion paper is a product of our interest in analysing blockchain in, with and for government through a post-political lens, tying together literature in blockchain studies and algorithmic governance spaces to post-political and post-foundational theory. Continuing to pursue the connections between these bodies of literature and practice together opens up an extensive research agenda regarding both the future of blockchain and study of the post-politics.

References:

[1] J. Wilson and E. Swyngedouw, "Seeds of Dystopia: Post-Politics and the Return of the Political," in The Post-Political and Its Discontents, Edinburgh University Press, 2014, pp. 1–22.

[2] C. Crouch, Post-democracy. Polity, 2004.

[3] E. Swyngedouw, "Apocalypse Forever?," Theory, Cult. Soc., vol. 27, no. 2–3, pp. 213–232, Mar. 2010.

[4] E. (Erik) Swyngedouw, Promises of the political : insurgent cities in a post-political environment. .

[5] C. Mouffe, On the political. Routledge, 2005.

[6] R. Beveridge and P. Koch, "The post-political trap? Reflections on politics, agency and the city The post-political trap?," Crit. Comment. Urban Stud., vol. 54, no. 1, pp. 31–43, 2017.

[7] D. Tapscott and A. Tapscott, Blockchain revolution : how the technology behind bitcoin and other cryptocurrencies is changing the world. 2016.

[8] S. Davidson, P. De Filippi, and J. Potts, "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology." 2016.

[9] B. Markey-Towler, "Anarchy, Blockchain and Utopia: A Theory of Political-Socioeconomic Systems Organised using Blockchain," SSRN Electron. J., Jan. 2018.

[10] I. Blühdorn, "Post-Ecologist Governmentality:," in The Post-Political and Its Discontents, Edinburgh University Press, 2014, pp. 146–166.

[11] W. Larner, "The Limits of Post-Politics:," in The Post-Political and Its Discontents, Edinburgh University Press, 2014, pp. 189–207.

[12] E. Swyngedouw, "Insurgent Architects, Radical Cities and the Promise of the Political," in The Post-Political and Its Discontents, Edinburgh University Press, 2014, pp. 169–188.

[13] B. Scott, "A Dark Knight is better than no Knight at all - King's Review Magazine," Kings Review, 2015. [Online]. Available: http://kingsreview.co.uk/articles/a-dark-knight-is-better-than-no-knight-at-all/. [Accessed: 19-Oct-2018].

[14] Y. Benkler, "Networks of Power , Degrees of Freedom," Int. J. Commun., vol. 5, no. 1932–8036/20110721, pp. 721–755, 2011.

[15] S. O. Husain, A. Franklin, and D. Roep, "The political imaginaries of blockchain projects: transition, transformation or creative destruction?," Forthcoming, 2019.

[16] M. Jun, "Blockchain government - a next form of infrastructure for the twenty-first century," J. Open Innov. Technol. Mark. Complex., vol. 4, no. 1, p. 7, Dec. 2018.

[17] IBM Institute for Business Value, "Building trust in government," IBM , 2018. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN. [Accessed: 24-Jan-2019].

[18] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," Electron. Commer. Res. Appl., 2018.

[19] ConsenSys, "Building Blockchain for Government: Why Governments Need Blockchain," Medium , 2019. [Online]. Available: https://media.consensys.net/building-blockchain-for-government-why-governments-need-blockchain-9691d1e21e3d. [Accessed: 30-Jul-2019].

[20] European Union Blockchain Observatory & Forum, "Blockchain for Government and Public Services," 2018.

[21] European Commission, "EUBlockchain | An initiative of the European Commission," 2019. [Online]. Available: https://www.eublockchainforum.eu/. [Accessed: 30-Jul-2019].

[22] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," 2015.

[23] J. Rancière and S. Corcoran, Dissensus : on politics and aesthetics. Continuum, 2010.

[24] S. Žižek, In defense of lost causes. Verso, 2008.

[25] J. Rancière, Disagreement : politics and philosophy. University of Minnesota Press, 1999.

[26] S. Žižek, The ticklish subject : the absent centre of political ontology. Verso, 1999.

[27] D. Golumbia, "Bitcoin as Politics: Distributed Right-Wing Extremism," Ssrn, 2015.

[28] D. Allen, "Discovering and Developing the Blockchain Cryptoeconomy," 2016.

[29] S. Pink, H. A. Horst, J. Postill, L. Hjorth, T. Lewis, and J. Tacchi, Digital Ethnography: Principles and Practice. London: SAGE Publications, 2016.

[30] D. R. Unruh, "The Nature of Social Worlds," Pac. Sociol. Rev., vol. 23, no. 3, pp. 271–296, Jul. 1980.

[31] R. Bellanova, "Digital, politics, and algorithms," Eur. J. Soc. Theory, vol. 20, no. 3, pp. 329–347, Aug. 2017.

[32] L. Introna, D. W.-S. & Society, and undefined 2004, "Picturing algorithmic surveillance: The politics of facial recognition systems," ssoar.info.

[33] L. D. Introna, "Algorithms, Governance, and Governmentality," Sci. Technol. Hum. Values, vol. 41, no. 1, pp. 17–49, Jan. 2016.

[34] A. Rouvroy and B. Stiegler, "The Digital Regime of Truth: From the Algorithmic Governmentality to a New Rule of Law *," 2016.

[35] R. Kitchin, "Thinking critically about and researching algorithms," Information, Commun. Soc., vol. 20, no. 1, pp. 14–29, Jan. 2017.

[36] C. Coletta and R. Kitchin, "Algorhythmic governance: Regulating the 'heartbeat' of a city using the Internet of Things," Big Data Soc., vol. 4, no. 2, p. 205395171774241, Dec. 2017.

[37] danah Boyd and K. Crawford, "Critical questions for big data," Information, Commun. Soc., vol. 15, no. 5, pp. 662–679, Jun. 2012.

[38] L. Lessig, Code and other laws of cyberspace, 2. ed. New York: Basic Books, 2008.

[39] P. De Filippi and S. Hassan, "Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code," Jan. 2018.

[40] S. Lash, "Power after Hegemony," Theory, Cult. Soc., vol. 24, no. 3, pp. 55–78, May 2007.

[41] D. Beer, "Power through the algorithm? Participatory web cultures and the technological unconscious," vol. 11, no. 6, pp. 985–1002, 2009.

[42] A. Mari, "HM Land Registry completes blockchain trial," Computer Weekly , 2019. [Online]. Available: https://www.computerweekly.com/news/252461839/HM-Land-Registry-completes-blockchain-trial. [Accessed: 23-Aug-2019].

[43] D. Allessie, M. Sobolewski, and L. Vaccari, "Blockchain for digital government: an assessment of pioneering implementations in public services," 2019.

[44] C. Sullivan and E. Burger, "E-residency and blockchain," Comput. Law Secur. Rev., 2017.

[45] N. Heller, "Estonia, the Digital Republic," The New Yorker, 2018. [Online]. Available: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic. [Accessed: 31-Oct-2018].

[46] C. Sullivan and E. Burger, "E-residency and blockchain," Comput. Law Secur. Rev., vol. 33, no. 4, pp. 470–481, Aug. 2017.

[47] Republic of Estonia, "What is e-Residency | How to Start an EU Company Online," 2019. [Online]. Available: https://e-resident.gov.ee/. [Accessed: 23-Aug-2019].

[48] F. Björklund, "E-government and moral citizenship: the case of Estonia," Citizensh. Stud., vol. 20, no. 6–7, pp. 914–931, Oct. 2016.

[49] R. Karakaya Polat and L. Pratchett, "Citizenship in the age of the Internet: a comparative analysis of Britain and Turkey," Citizensh. Stud., vol. 18, no. 1, pp. 63–80, Jan. 2014.

[50] M. Atzori, "Blockchain Governance and The Role of Trust Service Providers: The TrustedChain® Network," J. Br. Blockchain Assoc., vol. 1, no. 1, pp. 1–17, Jul. 2018.

[51] B. Markey-Towler, "Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using Blockchain," J. Br. Blockchain Assoc., vol. 1, no. 1, pp. 1–14, Jul. 2018.

[52] I. Sánchez-Cuenca, "From a Deficit of Democracy to a Technocratic Order: The Postcrisis Debate on Europe," Annu. Rev. Polit. Sci., vol. 20, no. 1, pp. 351–369, May 2017.

[53] P. Parvin, "Democracy Without Participation: A New Politics for a Disengaged Era," Res Publica, vol. 24, no. 1, pp. 31–52, Feb. 2018.

[54] Weareplanc, "Radical Municipalism: Demanding the Future," We are Plan C, 2017. [Online]. Available: https://www.weareplanc.org/blog/radical-municipalism-demanding-the-future/. [Accessed: 22-Jan-2018].

[55] S. O. Husain, A. Franklin, and D. Roep, Decentralizing Geographies of Political Action: Civic tech and Place-Based Municipalism, vol. 13. 2019.

[56] A. A. Gikay and C. G. Stanescu, "Technological Populism and Its Archetypes: Blockchain and Cryptocurrencies," SSRN Electron. J., Apr. 2019.

[57] Democracy Earth, "The Social Smart Contract - DemocracyEarth White Paper," 2018. [Online]. Available: https://docs.google.com/gview?url=http://bit.ly/defpaper&embedded=true. [Accessed: 14-Mar-2018].

[58] F. Moulaert, A. Paidakaki, and Blotevogel H, "Exploring the politico-institutional dimension of social innovation to repoliticize urban governance arrangements," Soc. Innov. Urban Reg. Res. ISR. Vienna Verlag der Österreichischen Akad. der Wissenschaften., pp. 11–22, 2018.

[59] B. Garcia, "New citizenship in Spain: from social cooperation to self-government," Citizensh. Stud., vol. 21, no. 4, pp. 455–467, May 2017.

[60] Y. B. Abati, "Random election, the G1000 and deliberation to change Madrid," openDemocracy, 2017. [Online]. Available: https://www.opendemocracy.net/en/democraciaabierta/random-election-g1000-and-deliberation-to-change-madrid/. [Accessed: 04-Oct-2019].

[61] newDemocracy Foundation, "The City of Madrid Citizens' Council," 2019.

[Online]. Available: https://www.newdemocracy.com.au/2018/11/15/the-city-of-madrid-citizens-council/. [Accessed: 04-Oct-2019].

[62] J. Wilson and E. Swyngedouw, "Conclusion: There Is No Alternative," in The post-political and its discontents : spaces of depoliticisation, spectres of radical politics, 2014, p. 326.

[63] P. De Filippi and B. Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure." 2016.

[64] S. Davidson, M. Novak, and J. Potts, "The Cost of Trust: A Pilot Study," J. Br. Blockchain Assoc., vol. 1, no. 2, pp. 1–7, Dec. 2018.

[65] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," 2015.

[66] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services-Use cases, security benefits and challenges," in 2018 15th Learning and Technology Conference, L and T 2018, 2018.

[67] Dutch Blockchain Coalition, "Vision Document: Blockchain for Good."

[68] V. Shermin, "Disrupting governance with blockchains and smart contracts," Strateg. Chang., vol. 26, no. 5, pp. 499–509, Sep. 2017.

[69] C. Green, "Real World Examples of Governments Moving Land Titles to a Blockchain - ZKY Token Sale," Zooky, 2019. [Online]. Available: https://zky.io/2018/07/16/moving-land-titles-to-blockchain/. [Accessed: 23-Aug-2019].

[i] Slack teams of Democracy Earth, Ashoka, Consul, Decidim and several others which requested for anonymity

[ii] In blockchain studies, there is a growing body of literature around algorithmic governance. This is also one of the reasons why there is urgent call for regulation within the blockchain space, particularly with regard to cryptocurrencies.

[iii] India, Sweden, U.K., Ghana among others are launching pilots and experiments. For instance, refer to [69].

Competing Interests:
None declared.

Ethical approval:
All interviewees gave permission to be quoted, and anonymity has been kept as requested.

Author's contribution:
[1]SOH designed and coordinated this research and prepared the manuscript in entirety.

Funding:
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 674962.

Acknowledgements:
[1]SOH would like to thank all those individuals and groups who contributed to the project.

PEER-REVIEWED RESEARCH

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

Managing Gender Change Information on Immutable Blockchain in Context of GDPR

Ali Shahaab[1], Ross Maude[2], Chaminda Hewage[1], Imtiaz Khan[1]
[1]Cardiff Metropolitan University, United Kingdom
[2]Companies House, United Kingdom
Correspondence: ashahaab@cardiffmet.ac.uk

Received: 30 September 2019 **Accepted:** 25 November 2019 **Published:** 6 January 2020

Abstract

The transgender community faces serious socio-economic predicaments due to the discrepancy that its members face between their current gender expression and the assigned gender identity at birth. Even though, a considerable amount of work has been done to protect their basic human rights such as security, equality and social acceptance; trans people are still large victims of hate-related crimes. With general data protection regulation (GDPR) and other data protection laws and policies in place, now it is ever more important to protect the confidentiality of gender change information as well as to establish technical solutions that can prevent from inferring any sense of gender change from historical data. In this context, distributed ledger technologies such as blockchain present great opportunities for information integrity, security, privacy and access. However, at the same time provenance information extracted from immutable blockchain can be exploited to infer gender change. Addressing this paradox here, we propose recommendations for managing gender change information in the blockchain environment in the context of the present socio-political, legislative and technical challenges associated with gender change.

Keywords: *blockchain, distributed ledger technology, personal information on blockchain, immutability, public sector, gender change, GDPR*

JEL Classifications: *D02, D71, H11, P16, P48, P5*

1. Introduction

1.1. Transgenders and social injustice

Sweileh [1] analyzed 5772 peer-reviewed documents published between the year 1900 and 2017 from 80 different countries in order to quantify and map keywords used in relation to transgender health. The term "HIV" obviously ranked the top keyword used, but interestingly the second and third top keywords were "mental health" and "discrimination". Figure 1a shows the network of these keywords and clearly indicates that transgender health is not only related to physical health but to other mental and social issues also. In fact several studies have argued that mental health issues faced by transgender people are due to discrimination, victimisation, cultural intolerance, social stigma and violence [2]–[4].

According to the definition of the Government Equalities Office (GEO; this is the official UK government's unit responsible for work on policy relating to women, transgender equality and sexual orientation). "Trans" is a general term for people whose gender is different from the gender assigned to them at birth. For example, a trans man is someone that transitioned from woman to man. [5] Accurate data for trans people living in the UK are not available, as it is not asked in the census and no statistically significant research has ever been conducted in this context. However, it is estimated that there are 200,000 to 500,000 trans people living in the UK [5]. Trans people are exposed to widespread social stigma, abuse, harassment and discrimination. Gender change has severe social, economical and political consequences for these subjects, and in some cases it can be life-threatening, even in free societies like US (Figure 1b) [6] and UK (Figure 1c) [7].

Beyond statistics, the following quotes from victims of identity-related hate crimes underpin the general attitude of the society towards trans people:

Beyond statistics, the following quotes from victims of identity-related hate crimes underpin the general attitude of the society towards trans people:

> *I am a trans man and I have been stalked for over two years now from an unknown person. During this time, I have received anonymous threatening letters. I've had two letters containing razor blades, one which contained a toxic substance which burnt my hands, face and eye. I have been beaten up three times. —James, 47 (South East England, UK) [7]*

> *I was raped. Police kept referring to me as 'she' and 'female' and using my birth name. The doctor they brought to examine me made me uncomfortable and continued calling me female. —Angus, 24 (Scotland, UK) [7].*

To understand the sheer scale of the problem, we would like the reader to take into account the fact that the physical, emotional, sexual and verbal abuse of trans people is so common that it has been given a name "trans bashing." Also, a dynamic list of unlawfully killed transgender people is being maintained on Wikipedia [8].

Considering the consequences and the severity of the matter, it is utterly important that the information about gender change is dealt with highest confidentiality and no unauthorised person is ever be able to infer about the gender change. Section 22 of the Gender Recognition Act (GRA) declares the revelation of gender change request without the explicit permission of a trans person as a criminal offence [9]. However, revealing anonymised data or in accordance with the GRA-defined criteria is acceptable.

1.2. Gender in the context of personal data

Gender is an attribute of "personal data." The Information Commission Office (ICO) [10] and the Organization for Economic Cooperation and Development (OECD) [11] defines personal data as "information that relates to an identified or identifiable individual." Personal data could be

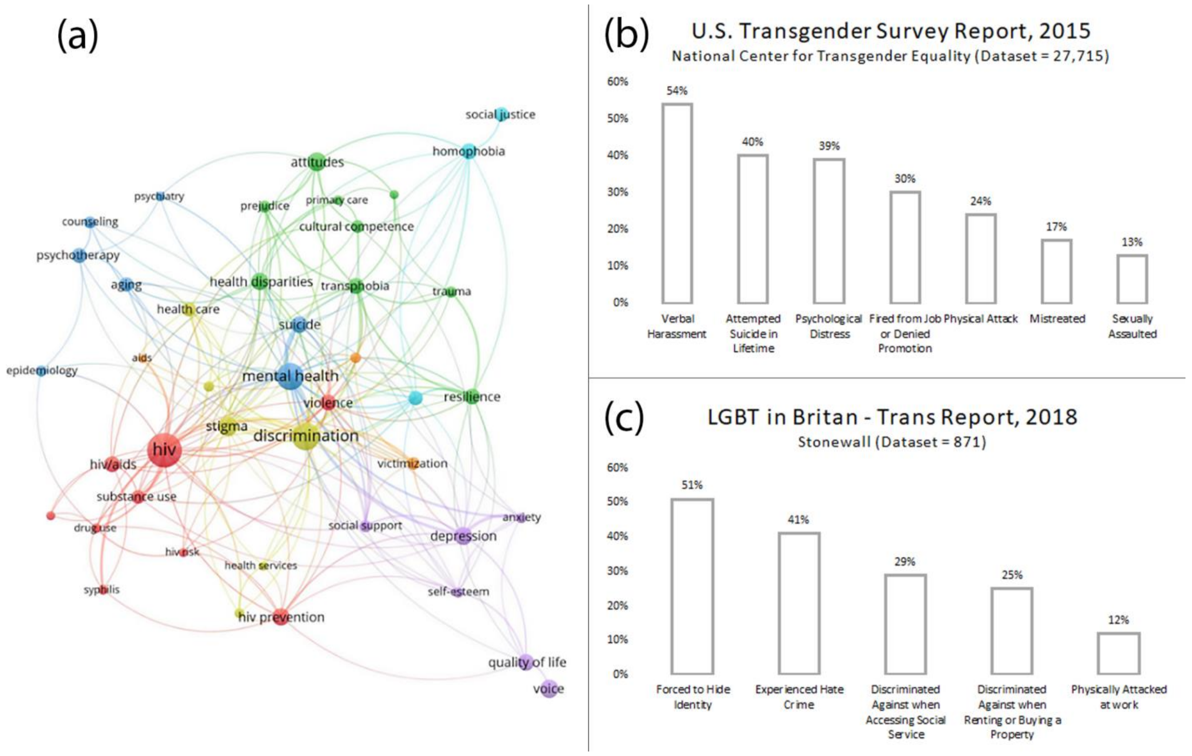


Figure 1: (a) Inter-relationship of different health-related keywords extracted and analyzed from 5772 peer reviewed articles by Sweileh [1] (The figure was reproduced under the creative commons licence). Different experiences that transgender people face in (b) USA and in (c) UK.

as simple as a subject's name or email address, or it could include other identifiers such as browser cookies, IP address or location data. In short, any information that could possibly result in the identification of a subject, directly or indirectly, is personal data. Introduced in May 2018, the general data protection regulation (GDPR) [12] requires data controllers (entity that determines the reason and the need for the processing of personal information) and data processors (entity that processes personal data on behalf of the controller) to take strict measures in securing fair usage of personal data. Sexual orientation is considered as a special category of personal data under GDPR, and sensitive data under the Data Protection Act (DPA) 1998. Data controllers need explicit consent from the data owner for data processing. Encrypted data (pseudonymised) or hashes of deterministic datasets are also considered personal data under GDPR. For example, one can easily compare the hash (a deterministic message digest that can be used to store the cryptographic proof of the data instead of the raw data itself) of the subject's gender attribute to devise if the subject is a male or female and a subject's date of birth can be revealed by iterating over a very low subset of possible outcomes (gender will only take two and date of birth in dd/mm/yyyy format will take less than 50,000 attempts). Adding random noise to the data before hashing results in a non-deterministic hash, hence deeming the data as not personal anymore.

Chen and Zhao have discussed seven phases of personal data – generation, transfer, usage, sharing, storage, archival and destruction [13]. There are several security and privacy challenges associated with each step of the lifecycle. The subject has the right to know what information is collected on them, how it is stored and managed, how the integrity of the data is guaranteed, storage and usage of data and finally how it is destroyed once it is no longer used [13]. Data controllers and processors are required to take all the necessary steps in protecting personal data in all steps of the data lifecycle.

1.3. Potentiality of the blockchain technology

Computer scientists and information security experts continuously propose different methodologies and frameworks for secure sharing and protection of personal data collected on the subjects. Distributed ledger technologies (DLTs), such as blockchain, have also attracted a wide spectrum of researchers for secure dissemination of valuable information and as a tamper-proof medium for the storage of personal information. Blockchain basically is a global distributed digital ledger or database system where the updated copy of the ledger is available to all participants (also known as nodes) at all time. Blockchain is also a "trustless" system where instead of a trusted third party (e.g. banks and government organizations), trust on each transaction is asserted by general consensus within the participants in a democratic, competitive and incentivized manner. Once validated, each transaction is recorded on the ledger in an immutable fashion, and the updated copy of the ledger is available to all participants on a real time basis. In addition to the nodes maintaining the blockchain network, the state and history of the ledger can be accessed by anyone (public DLTs) or restricted to only a few (private DLTs) through blockchain explorers.

Cryptographic capability of the blockchain ensures security and privacy, and with smart contract technology, a data usage control mechanism – commonly known as "disclosure without exposure" can be established within the blockchain network [14], where data owners can define the level, duration and authorities using their data. It is the latter capability that provides blockchain unique advantage over traditional database management systems by empowering data owners to determine which aspect of their personal information can be exposed to whom and for how long – a debatable issue of GDPR commonly known as the "right to be forgotten" (RTBF) [15]. Despite this empowerment, the immutable block of information and the ability to extract provenance information from the chain can be a liability for trans people, because anyone with the right access on the blockchain can trace and detect any gender change by comparing the current gender attribute value with the past value.

Addressing the technical complexity of blockchain in relation to the reality of GDPR and the contemporary social stigma and insecurity of trans people, here we aim to investigate the suitability of blockchain for storing and sharing the personal data of trans people. This article is set as follows:

Section 2 discusses related work in the space of handling personal data on the blockchain and we discuss our recommendations in Section 3 about how gender change should be managed as part of personal data on the blockchain. We end the article with our conclusion and prospective future work in section 4.

2. Related work

We found several articles discussing the techniques around sharing, storing and managing personal data on the blockchain but we have not come across any piece of literature discussing the challenges associated with the change in gender. Here we present some of the common techniques of handling personal data on the blockchain.

a. Blockchain and medical data

Medrec [16], a blockchain-based system to handle electronic medical records (EMRs), aims to provide users with an immutable log and access to their EMRs. Personal data are stored on patients' smartphones and service providers' databases. Access to the data is managed through permissioned setup of the Ethereum [17] blockchain. No personal data are put on the blockchain, but a 'DNS-like' link is created between the already established identity and the Ethereum address. Cryptographic hash of the data is stored on the blockchain to ensure data integrity while data are kept off-chain. Smart contracts are used to manage access permissions to the externally stored patient data. [16] A service provider such as GP can update patient records and notify observers about the update, and a patient can at any time revoke permissions to their data. The query string for data retrieval is affixed to the hash of data subsets for tamper evidence. Even though, no personal information is put on the blockchain, this fixed query string can indicate a gender change in the gender data set.

b. Blockchain and personal data

CareerChain [18], a platform to host jobseekers profile, also uses a private instance of the Ethereum blockchain. The subject's data are encrypted using private keys and stored on an interplanetary file system (IPFS) [19], and the address to the latest profile is stored in a smart contract, where access is controlled by the subject. [18] assumes that RTBF is preserved as the subject can delete their private key, making the data unreadable and hash meaningless. However, the subject cannot exercise their RTBF if they lose their private key, compromising their personal details forever.

Engima [20] protocol stores the data off-chain and pointers to the data are stored in distributed hash tables (DHTs), which are distributed across several nodes. Access control is governed by the blockchain, and computations on the data are performed using multi-party computation (MPC), without revealing the complete data to any of the nodes. Even though Engima guarantees private computation on the blockchain, it does not secure the raw data, making it possible for someone to change the data. This change can be easily identified as the data pointers will change with the data modification.

Hossein et al. has proposed a blockchain-based solution for Internet of Things (IoT) devices. Their approach is similar to [16] such that the data layer is separated from the access layer, having access control on a blockchain and data resides in an off-chain centralised storage such as a cloud or decentralised storage such as DHTs or IPFS [21]. Chang et al. also suggest storing personal data in off-chain storages and storing a hash on the blockchain for authenticity and verification purposes [22]. Nazaré et al. uses a similar approach for certificate verification. The hash of the certificate containing the subject's personal details is placed on the blockchain and requires the verifier to have access to the original document and knowledge of the location of the hash on the blockchain [23]. This approach requires a new hash to be posted onto the blockchain if any personal details are changed for the user. Observers may notice the change and may also be able to decipher the change if they have previously had the original document for verification purposes.

c. Blockchain for data integrity

Ancile [24] also puts the hash of the data and the pointers on the blockchain while storing the data in traditional databases. Its purpose is to guarantee data integrity, as underlying data can be changed or removed. However, the issue of an identity update is not addressed as the network will be able to track the update to the existing record. Igor et al. propose the use of blockchain technology to ensure the integrity of files on the cloud. Hashes of the files are added on the blockchain as a reference of the change [25]. Though the authors do not deal directly with personal data, the files may contain personal data, indicating a change in personal data whenever a new hash is posted. Zyskind et al. propose the use of shared identity for data access and storage. Encrypted data are stored off the blockchain, and pointers (hash of data) to the data are stored on the blockchain [26]. Users remain anonymous while the service's profile can be verified on the blockchain.

d. Blockchain as identity service

Identity as a service-based blockchain focuses greatly on privacy. The goal of these blockchains is to allow the subject to prove their identity and relation to any verifier. Shocard [27] keeps the encrypted personal data on the user's device and posts the full record of signed hashes and a code (to prevent discovery) on to the blockchain. Verification involves the user presenting the raw data and the code for the verifier to be able to verify the data on the blockchain. The subject's identity is confirmed by other authorities when they verify its claim of identity. If any part of the identity changes, the subject has to get new certification for that part of the identity. For example, if the subject changes their address, new certification on the new address will be required but their other claims about age, gender, etc. will stay valid. Figure 2 shows the change of gender and attestation recorded with new timestamps on the blockchain.

Even though the solution is practical, it still poses a threat to the trans person as the certification's timestamps become a proof that the subject has changed gender at a later point. Figure 3 shows a subject sharing their identity credentials with different attestation dates, revealing a later change in gender.

Sovrin [28] allows interactions using distributed identifiers (DIDs), which are unique for each relation. The subject's data are kept in private ledgers, and claims about the identity can be kept private or public. The use of zero knowledge proofs (ZKPs) enables the subject to disclose the proofs for verification.

The challenge with the identity on blockchain schemes is that the subject needs to reveal (a) more than one verification to establish trust, (b) the timestamp of the verification so the verifier can see that the subject is sharing the valid claims, (c) claims regarding more than one attribute. Hence, for example, if a trans person is to reveal their date of birth and gender to a verifier, they will be able to spot the gender change because there will be more attestations on the date of birth than on a recent gender change.

3. Our recommendations

Gender change is a delicate subject with severe consequences for the subject and also for the authority dealing with the information around gender change. The solution to obfuscating the change of personal data change, such as gender, on the blockchain must meet the following criteria:

a) On-chain activity should not de-anonymise the subject.
b) Change in gender should not be visible to unauthorised observers.
c) Any historical transactions should not reveal the previous gender but only show the recently acquired gender.

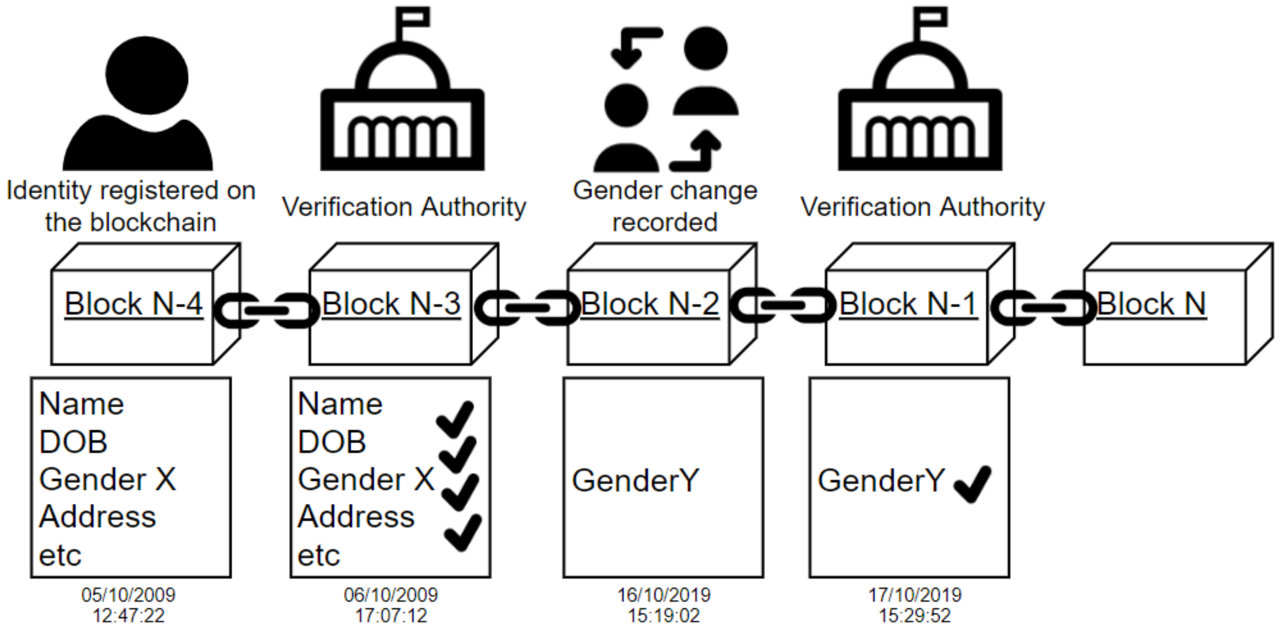


Figure 2: Establishing identity on the blockchain. Subject's identity attributes are verified by a verification authority and a verification claim to the blockchain. Any changes in the identity attributes yields the old claim to be invalid and new verification is required in order to establish trust. Each claim has a timestamp and possibly a validity period.

d) Gender change should not be revealed when accessing multiple personal identity attributes.

e) Any such solution should be future proof in both technological and legal perspectives.

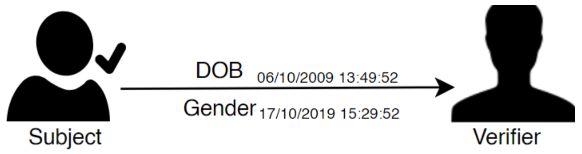


Figure 3: Subject revealing verification claims about their identity to a verifier. The timestamp of the claim can reveal a gender change to the verifier as it is obvious that gender change has a later verification from DOB. DOB may also have several more claims then gender.

We recommend the following approach to satisfy the aforementioned criteria.

a. On-chain activity should not de-anonymise the subject

"Identity" on the blockchain is only a random string (public key). However, identity can be exposed by the reuse of public keys. Bos et al. were able to identify several bitcoin account owners by analysing the repetition of public keys [29]. Supplementary data may also aid in ring fencing the subjects, for example, IP address or spending patterns. Anonymisation can be achieved by avoiding the reuse of public keys. It becomes difficult to deanonymise a subject if they are using a unique public key for every transaction across the network. For example, using the same public key if the subject's previous transactions revealed the subject's gender as male, then an observer may be able to infer the gender change if the new transactions reveal the subject as female. ZKPs [30] and homomorphic encryption [31] techniques should be deployed to obfuscate the details of transactions, such that the subject cannot be linked to the transaction.

b. Change in gender should not be visible to unauthorised observers

It is important that not only the personal information is secure but the change in personal information, such as gender, should also be kept private. As blockchain links the new transactions with the previous ones, it makes it difficult to "hide" the change from the observers. We suggest including an encrypted transaction belt in the transaction schema, which can only be decrypted with the symmetric keys shared with the authorities. All participants in the network will see the encrypted transaction belt with every transaction but will not be able to see what has changed, hence removing the "sense of change." Off-chain storage should be used for storing personal information and the hash pointer on the blockchain will only point to the latest transaction on the blockchain. Authorities will be able to decrypt the belt and see the changes, such as the information about gender change. Key delegation [32] and rotation should be used to renew the symmetric keys. Role-based encryption and proxy re-encryption techniques can also be used to manage access to the encrypted transaction belt. We also recommend managing the detection of the change using a similar approach to [27]. Grouping of identity attributes for certain access levels can significantly obfuscate the detection of the change. Personal data can be graded into different levels and access can be managed based on the observer's clearance level. Smart contracts can be used to manage notifications for different observers. A member of the public may only be notified of a change, and credit referencing agencies can be on-boarded for notification of more detailed changes such as change of address, marital status or name. Law enforcement can be notified on the exact change that has taken place (Figure 4). As the access is managed by a smart contract on the blockchain, individuals can verify who can access what part of their identity, encouraging fair usage of the system.

c. Any historical transactions should not reveal the previous gender but only show the recently acquired gender

We conclude from section 2 that any personal details (gender included) should never be put on the blockchain but only a cryptographic proof should be put on the blockchain. As discussed in section 3b, the off-chain record of personal data will point to the most recent identity transaction.

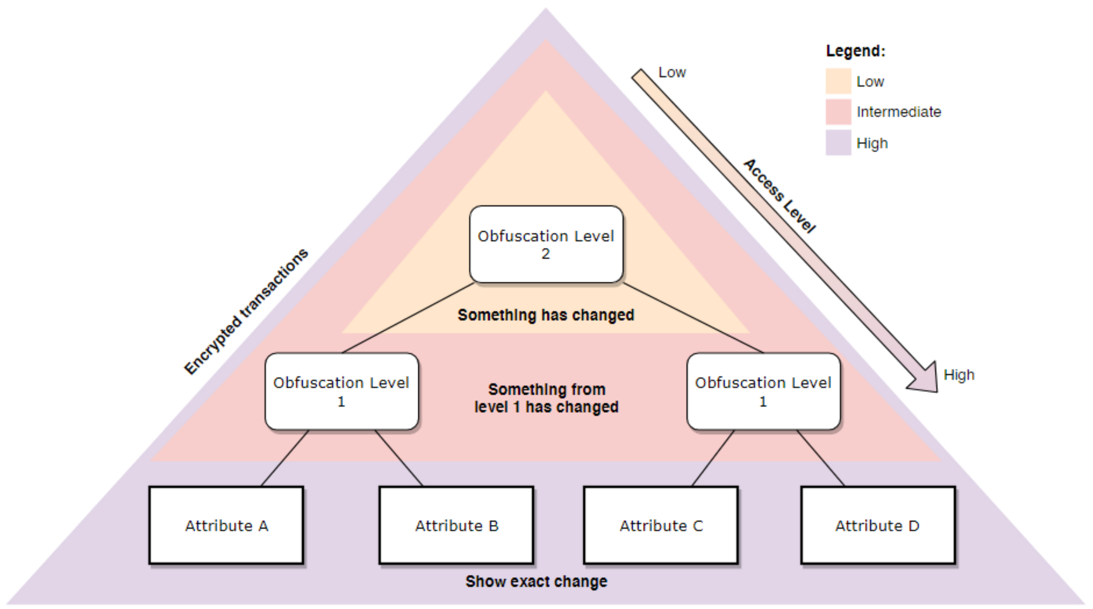


Figure 4: Different level of observers get a different level of view of the encrypted transaction. A Physician may get highest access and can see the change in gender, credit reference agency get intermediate access and can see a category change while any sort of details will be hidden from the public with visibility to undelaying data.

We therefore recommend that where possible, static personal data should not be stored as a part of the transaction but "looked-up" at the point of retrieval so that only the up-to-date information is retrieved. This approach will also aid the blockchain network to comply with the accuracy principle of GDPR [33].

d. Gender change should not be revealed when accessing multiple identity attributes

To satisfy this, we recommend that standards should be developed that allows sharing the claims about identity in such a way that it obfuscates any less common and severe change such as gender. Multiple attributes should be shared together in such a way that they do not compromise personal identification and privacy. Only recent timestamps should be accessible to the verifier so they cannot "sense" the change. For example, people move addresses quite frequently, so a subject sharing their claims for the last three residential durations with verification timestamps should be acceptable; however, a subject sharing their date of birth and gender claims with timestamps pose the risk of revealing the identity of the trans person. We conclude that timestamped information should not be shared for the somewhat static personal information, but it can be shared for dynamic personal information.

e. Any such solution should be future proof in both technological and legal perspectives

These recommendations require foresight of the constantly changing socio-political landscape and evaluation of the continuous advancements in the technical space. The transparency versus privacy pendulum swings from one side to another with social awareness, technological change, media and recent events. Technical solutions must be flexible to adhere to the ever-changing socio-political landscape. Increased technical developments also lure threats to the cryptographic techniques used in the blockchain space. Bitcoin, Ethereum and several other blockchains rely on public key cryptography for transaction signing and funds locking. Advancements in quantum computing pose a serious threat to public key cryptography, and it is anticipated that commercially available quantum computers soon will be powerful enough to derive the private keys used to encrypt the personal information, making the subject vulnerable. Therefore any DLT/blockchain solution for personal information must ensure a safe migration towards the post-quantum era, and we should already be considering building systems using quantum-resistant cryptographic techniques [34].

4. Conclusion

DLTs such as blockchain are critical for establishing digital identity and protecting personal data online. No subset of personal data should be treated as "static," and personal data should never be uploaded to the immutable ledger. The revelation of an identity attribute such as gender change can have life-threatening consequences for trans people. This information must be protected and treated with confidentiality and must never leave any trail on the permanent blockchain. Gender change related information must be kept off-chain and declared in such a way that no unauthorised observer can detect the change in gender. New technological developments like homomorphic encryption, secure multi-party computation (SMPC), ZKPs and verifiable claims can significantly improve the odds of blockchain being a suitable technology stack for managing personal data. With the tightening of data protection laws around the world and classification of metadata of personal data such as encrypted data being classified as personal data, it may not be far that even the hash of the personal data is classified as personal data. Hence, we argue that gender-related information should never go on a blockchain. Only the commitment and a claim about the data should be put on the immutable ledger such as blockchain, and homomorphic encryption will also help in protecting and managing personal data.

References:

[1] W. M. Sweileh, "Bibliometric analysis of peer-reviewed literature in transgender health (1900–2017)," BMC Int. Health Hum. Rights, vol. 18, no. 1, p. 16, 2018.

[2] K. D. Jaffee, D. A. Shires, and D. Stroumsa, "Discrimination and delayed health care among transgender women and men," Med. Care, vol. 54, no. 11, pp. 1010–1016, 2016.

[3] T. C. Carmel and L. Erickson-Schroth, "Mental health and the transgender

population," Psychiatr. Ann., vol. 46, no. 6, pp. 346–349, 2016.

[4] S. Page, J. Burgess, I. Davies-Abbott, D. Roberts, and J. Molderson, "Transgender, mental health, and older people: an appreciative approach towards working together," Issues Ment. Health Nurs., vol. 37, no. 12, pp. 903–911, 2016.

[5] Government Equalities Office, "Trans People in the UK," 2018.

[6] S. E. James, J. L. Herman, Susan Rankin, M. Keisling, L. Mottet, and M. Anaf, "The Report of the US Transgender Survey," 2015.

[7] B. Chaka and G. Becca, "LGBT in Britain - Trans Report," 2017.

[8] Wikipedia. "List of unlawfully killed transgender people." [Online]. Available: https://en.wikipedia.org/wiki/List_of_unlawfully_killed_transgender_people. [Accessed 21. Apr 2019].

[9] The Gender Recognition Act - Section 22. United Kingdom: Statute Law Database, 2004.

[10] ICO, "What is personal data?," 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. [Accessed 12 Apr. 2019].

[11] "The OECD Privacy Framework 2013," 2013.

[12] The European Parliament and the Council of the European Union, Regulation (EU) 2016/679 (GDPR). 2016, pp. 1–88.

[13] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012.

[14] R. H. Campbell Rab, Thompson Gillian, Ferry Peter, "Distributed Ledger Technologies in Public Services," no. June, 2018.

[15] Information Commissioner's Office, "Right to erasure," 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/. [Accessed: 12-May-2019].

[16] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016, pp. 25–30, 2016.

[17] V. Buterin, "A next-generation smart contract and decentralized application platform," Etherum, no. January, pp. 1–36, 2014.

[18] R. Gibson, A. Evans, L. Tatarov, D. Mulder, and A. Dowdalls, "Careerchain Foundation Whitepaper," 感染症誌, vol. 91, pp. 399–404, 2017.

[19] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXiv Prepr. arXiv1407.3561, 2014.

[20] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," pp. 1–14, 2015.

[21] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards Blockchain-based Auditable Storage and Sharing of IoT Data," pp. 25–30, 2017.

[22] H. Chang, G. Tortora, C. Esposito, K.-K. R. Choo, and A. De Santis, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE Cloud Comput., vol. 5, no. 1, pp. 31–37, 2018.

[23] J. Nazaré, K. Hamilton, and P. Schmidt, "What we learned from designing an academic certificates system on the blockchain." [Online]. Available: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196. [Accessed 21 Feb. 2019].

[24] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustain. Cities Soc., vol. 39, pp. 283–297, 2018.

[25] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in Proc. 52nd Hawaii Int. Conf. Syst. Sci., 2019, vol. 6, pp. 6855–6864.

[26] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. 2015 IEEE Secur. Priv. Work. SPW 2015, pp. 180–184.

[27] ShoCard Inc., "ShoCard Shitepaper: Identity Management Verified Using the Blockchain," p. 20, 2017.

[28] 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.

[29] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in International Conference on Financial Cryptography and Data Security, 2014, pp. 157–175.

[30] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash Protocol Specification," pp. 1–53, 2017.

[31] C. Gentry and others, "Fully homomorphic encryption using ideal lattices.," in Stoc, 2009, vol. 9, no. 2009, pp. 169–178.

[32] M. Abdalla, E. Kiltz, and G. Neven, "Generalized key delegation for hierarchical identity-based encryption," in Proc. European Symposium on Research in Computer Security, 2007, pp. 139–154.

[33] "GDPR Principle (d): Accuracy," 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/. [Accessed: 24-Apr-2019].

[34] L. Chen et al., "Report on Post-Quantum Cryptography," 2016.

Competing Interests:
None.

Ethical approval:
Not applicable.

Author's contribution:
AS, RM, CH and IK designed and coordinated this research and prepared the manuscript in its entirety.

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:
The authors acknowledge Mr Ben Lidgey for his continuous input on the subject and Mr Farhan Khan for his valuable feedback on the approach.

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/ jbba-3-1-(6)2020

Emerging Regulatory Approaches to Blockchain-based Token Economy

Agata Ferreira
Department of Administrative Law and Public Policies Sciences, Warsaw University of Technology, Poland
Correspondence: aferreira@ans.pw.edu.pl

Received: 20 February 2020 **Accepted:** 13 March 2020 **Published:** 19 March 2020

Abstract

Blockchain-enabled digital scarcity has opened up a whole new dimension of possibilities for the token economy, particularly with regard to rights and assets that have not been traded electronically before. Blockchain-based tokenization of rights and assets has also brought a new set of legal and regulatory challenges. Regulators and legislators are yet to address many of the issues raised by blockchain-based tokenization, from decentralisation and token characterisation to cross-border harmonisation and regulatory compliance with traditional market infrastructure. Lack of regulatory alignment can undermine many of the benefits of the token economy. Lack of legal certainty may not only stifle innovation and slow down mainstream adoption of blockchain-based tokenization, but can also raise the risks for investors and harm the reputation of the industry. The emerging regulations vary in approach. Liechtenstein became the first country to have a comprehensive technology-neutral regulation of the token economy. Malta and Singapore also represent progressive jurisdictions for blockchain regulation. However, most jurisdictions, including the United States and the European Union, have not yet formed a clear policy for blockchain regulation, and many legal questions remain open. The paper examines whether there is an emerging predominant regulatory approach or prevailing regulatory direction for the future of the token economy. It also highlights the existing regulatory void and divergent approaches to blockchain-based tokenization. Finally, the paper concludes that there is an urgent need to provide a clear legal and regulatory framework if the potential of the token economy is to be realised.

Keywords: *token economy, blockchain regulation, blockchain law, securities law, technology law*

JEL Classifications: *K20, K22, K23, K24, O31, O38, G28*

1. Introduction

According to the European Central Bank, the market capitalisation of cryptoassets reached an all-time high of €650 billion in January 2018 [1]. While the global value of the cryptoassets market is still relatively small compared to the entirety of the financial system, its absolute value is substantial, and as rapid development continues, it is gaining increased attention and market acceptance [2].

Mining native blockchain tokens or digitalizing assets and recording them on a blockchain in a trusted, immutable and reliable way and then trading those digital tokens on peer-to-peer, decentralised and disintermediated networks brings endless possibilities which the industry is only beginning to explore. There are several advantages to blockchain-based tokenization, including the democratisation of the investment market by allowing fractional investment with minimised costs. Executing transactions on a blockchain without intermediaries not only allows cheaper and faster transactions, but also increases market efficiency by removing the time and calendar constraints of the world markets. Blockchain transactions are more easily audited, facilitated by the transparency and immutability of blockchain records. Blockchain-based tokenization can unlock the value of previously illiquid assets and allow for trading them cheaply and instantly. Initial Coin Offerings (ICOs) in particular, as a form of raising capital, provide unprecedented access to liquidity and capital while minimizing costs and the legal and jurisdictional constraints associated with public fundraising [40].

Blockchain developments have challenged and somewhat overwhelmed regulators, due to both the technological novelty and the speed of this technological innovation and its borderless and decentralised nature. The regulatory response has varied so far, from embracing to prohibiting, from adopting a tentative "wait and see" approach to proactively formulating bespoke regulatory frameworks for cryptoassets. Regulators struggle to formulate a consistent and coherent regulatory regime for blockchain tokenization.

Without focusing on any jurisdiction in particular, this paper aims to analyse the overall challenges and trends in regulation applying to blockchain-based tokenization and contribute to the existing research in this area. The first part of the paper explains the issues related to token taxonomy and the attempts at token classification. The subsequent section analyses the main challenges facing regulators when confronted with blockchain tokenization. The next part outlines the main emerging regulatory responses with a few examples illustrating different approaches. Finally, the paper offers concluding remarks.

2. Token taxonomy issues

A blockchain token effectively constitutes a digital bearer bond, and ownership is determined by the data embedded on the blockchain [5]. Transfer of the ownership of blockchain tokens takes place on a peer-to-peer basis, without the need for approval from any intermediating party. Initially, blockchain tokens were limited to native cryptoassets, protocol tokens, specific to a particular blockchain platform, like Bitcoin. Native tokens function as a crypto-economic [4] incentive mechanism that encourages participation, induces trust and maintains the functioning of the system. The launch of the Ethereum network in 2015 unlocked new opportunities for blockchain tokenization and brought significantly improved utility of blockchain technology in general. The open source, public Ethereum network allowed the building of decentralised applications and permitted relatively easy issuance of tokens. The expansion of blockchain utility beyond native protocol tokens and the flexibility of building decentralised applications on the Ethereum network have notably accelerated growth of blockchain technology beyond the financial application of cryptocurrencies. It has become possible to issue any kind of token, from simple tokens consisting of a few lines of code to sophisticated instruments. While most tokens issued on Ethereum are fungible, ERC-20 standard compliant tokens, since 2017 Ethereum has allowed the creation of non-fungible tokens based on ERC-721 standards. Non-fungible tokens can represent unique non-substitutable assets, like artwork, real estate or collectibles. Introducing non-fungibility into the digital world is quite an extraordinary development. It enables replicating scarcity in the physical world in a digital dimension. A scarce unique asset can now be represented in a verifiable way on a blockchain by a non-fungible token.

The first regulatory hurdle is to establish definitional boundaries. There is no single and commonly agreed definition of a blockchain-based token. Several attempts have been made to classify tokens based on jurisdiction, functions, properties and other characteristics [5], [6], [8]. There are a variety of terms that are used interchangeably with no clear definitional demarcation. Tokens can be understood broadly as including any type of cryptoasset issued on any type of distributed ledger technology. A narrow definition would include only tokens issued on permissionless and open blockchain networks. As such, the term token can take on different meanings depending on the regulatory, legal or business context in which it is being used. Blockchain-based tokens can be distinguished based on their purpose, utility, technical layer on which they are placed, legal status or underlying value [6]. Depending on their purpose, tokens can be divided into cryptocurrencies, network tokens or investment tokens. When their underlying value is taken into account, blockchain tokens can be grouped into asset backed, network value tokens or share-like tokens representing participation in an enterprise. Tokens can be issued as native to a specific blockchain platform – protocol tokens, or through a decentralised application. They can represent non-financial assets or financial assets, either native like cryptocurrencies or tokenised [7]. The lack of a uniform approach to token classification is challenging for regulators. The most common regulatory approach to the classification of tokens is functional and focusses on the purpose the token serves, rather than its technical specifications or other properties. It distinguishes cryptocurrencies, security tokens (sometimes referred to as investment tokens), utility tokens and hybrid tokens [3], [8], [9].

Currency tokens (like Bitcoin), the original and most straightforward type of blockchain tokens, are created to provide an alternative and decentralised means for the payment of goods and services. Currency tokens do not perform any other function. They are meant to work as a means of exchange and a store of value. Their value depends entirely on the value that users attribute to them.

Utility tokens provide the holders with other functions than just a means of payment, for example, access to services or products directly linked with the platform on which they are issued. They are not mineable and are intended for use within a specific blockchain platform, in contrast to cryptocurrencies, which have a multilateral reach and use beyond their issuing platform. Utility tokens do not embed any ownership or equity rights in anything other than the tokens themselves. Their value derives from their utility.

Finally, security tokens, sometimes referred to as investment, equity or asset tokens, derive their value from external tradeable assets. They are designed as an investment, which means that the motivation for their purchase is the anticipation of future profits, in the form of dividends, revenue share or price appreciation. Tokens classified as securities are usually subject to a heavy regulatory and compliance burden. Many regulators provide guidance or regulatory assistance to facilitate distinguishing security tokens from other types of cryptoassets. In the United States, the famous Howey Test is applied to determine whether a given instrument qualifies as a security. According to the Howey Test, a transaction that is a mere investment in common enterprise made with an expectation of profits from the efforts of a promoter or a third party falls within the scope of the definition of a security. Even though the Howey Test is commonly applied to determine the character of a token, it is not always reliable and, for now, a case-by-case approach is preferred by US regulators. In Europe, security tokens tend to be defined by reference to the relevant EU regulations governing financial instruments [10].

3. Regulatory challenges

Cryptocurrencies were the first blockchain tokens that attracted the attention of regulators, due to their rapid increase in value, widespread presence in the mainstream media and appeal to a wider audience [7]. Consumer protection, money laundering and financing illicit activities were just a few of the main concerns that brought cryptocurrencies onto the regulators' agenda. The main issues and challenges noted by regulators were concerns regarding price and financial stability, impact on monetary policy and the overall integrity of traditional payment systems. One of the first issues examined was the capacity of cryptocurrencies to affect demand for fiat currencies and interfere in the control of the supply of money through open market operations. It has been feared that a potential challenge to central banks' balance sheets could come from widespread substitution of central bank money for privately issued cryptocurrency. If cryptocurrencies ended up dominating the monetary space, central banks could effectively lose their control and influence over money and credit developments. The inherent lack of stability and high volatility of cryptocurrencies could also contribute to the overall financial instability, particularly if traded at high volumes and widely accepted in the economy. In the absence of regulation or public authority oversight, users of cryptocurrencies and participants in cryptocurrency blockchain platforms are exposed to various risks, including credit, liquidity, operational and legal risks [11].

The next wave of regulatory concerns around cryptocurrencies was brought on by the emergence of stablecoins, which retain the main features of traditional cryptocurrencies. They are also blockchain tokens, which apply cryptographic methods of validation, but aim to stabilise their price by linking the value of the coin to an asset or pool of assets. The most prominent stablecoin project is Libra, which caused worldwide consternation among regulators and authorities. Stablecoins created a new set of challenges for regulators. A G7 working group on stablecoins investigated the impact of global stablecoins and identified a long list of risks from stablecoins of any size [12]. The risks relate to legal certainty, governance, the investment rules of the stability mechanism, illicit finance, safety, efficiency and the integrity of payment systems, cyber security, operational resilience and market integrity. Stablecoins are also considered to pose challenges to data privacy and protection, consumer and investor protection and tax compliance. The biggest concerns are raised over global stablecoins, which are feared to be able to affect monetary policy, monetary sovereignty, financial stability, fair competition and the international monetary system overall.

Regulators have also focussed lots of attention on ICOs. These are considered to pose many risks, particularly with regard to retail investors [13]. The risks associated with an investment in the tokens issued through an ICO are much higher than the traditional form of investing in regulated financial instruments. For a start, investors have very limited or no control over promoters. They usually invest in the very early stages of an investment life cycle, only on the basis of a project or an idea, and with the information asymmetry scale tipped heavily against them. The lack of disclosure obligations that accompanied most early ICOs provided limited transparency. ICOs that fall outside any regulation or corporate governance regime create a legal and regulatory void, in which investors find themselves exposed to high risks and volatility. Investors also have no legal or regulatory protection or recourse, particularly in cases of

bankruptcy or project termination.

What proved to be the real challenge for regulators, legislators and supervisory bodies was the lack of clarity in the legal framework applicable to blockchain tokens. On top of that, the borderless, disintermediated and distributed character of blockchain networks hinder any attempts to identify applicable jurisdictions, the location of participants and addressees of potential regulations. Apart from identifying the risks and challenges of a nascent token economy, regulators face the dilemma of balancing risk mitigation measures with enabling innovation and fostering the development of new technology. The regulators have several factors to consider when establishing their regulatory perimeter and mandate. These include public interest, maintaining system stability, market integrity and oversight over business behaviour. They can choose a functional approach to regulation and focus on token products and services, or an institutional approach, where regulations target the providers of products and services [14].

One of the fundamental regulatory questions is whether cryptoassets should be integrated within existing legal frameworks (which could be adjusted if necessary) or provided with a separate bespoke regulatory treatment or, perhaps, even left unregulated [41]. This dilemma has been presented by Mark Carney, the governor of the Bank of England, who stated that the authorities need to decide whether to isolate, regulate or integrate cryptoassets and their associated activities [39]. Regulators must continuously evaluate the "newness" of the technology against the nature and function of financial markets in order to ascertain whether blockchain-based cryptoassets introduce new market solutions beyond innovative technological parameters. Perhaps the very attempt at pigeonholing cryptoassets and grouping them into classifications and definitional parameters would hamper innovation. Equally, providing regulatory legitimacy to a new and rapidly evolving technology could prematurely grant umbrella validation for that technology, not all facets of which have yet passed the tests of time, quality and resilience. On the other hand, not recognising the potential of the technology and not embracing innovation by isolating cryptoassets from existing regulatory regimes can stifle technological development and encourage regulatory arbitrage. Yet, opting for a case-by-case approach to blockchain regulation, to allow unhampered innovation, might be undermined by the lack of legal certainty and the resulting regulatory void.

The Cambridge Centre for Alternative Finance identified [7] several considerations for the regulatory process with regard to cryptoassets. One of the first steps in such a process is to understand the concepts involved, underlying technological infrastructure and associated potential harms and risks. The next regulatory consideration is to understand which part of a token lifecycle needs regulatory intervention. To this end, it is imperative for regulators to understand issuance, distribution, transfer mechanisms and intermediating activities for tokens and related risks.

Large-scale tokenisation has a number of potential economic and legal implications for financial markets and their participants. Those challenges vary from regulatory and legal questions to technology-related issues of scalability, interoperability or cyber risks. The next section illustrates how regulators have tackled some of these challenges so far.

4. Emerging regulatory approaches

It comes as no surprise that regulators struggle not only to keep up but also to maintain a unified and consistent approach while scrambling to formulate a coherent regulatory response, given the speed of technological advancement, novelty, complexity and the enormous potential of the blockchain-based token economy. What emerges is a piecemeal approach and a regulatory landscape in constant and fluid evolution. It is a major task for regulators to develop a regulatory approach that adequately captures the transition from the existing regulatory system built on the basis of bilateral relationships to an increasingly distributed financial world of blockchain-based tokenization [15]. Among the diverse array of regulatory initiatives, statements and policymaking efforts, few prevailing approaches emerge. Either current laws are applied to blockchain tokens, sometimes with adjustments, including prohibitive modification and specific extensions, or bespoke legal frameworks are enacted [16].

When applying an existing regulatory framework to blockchain-based tokens, often the first regulatory step is to distinguish cryptoassets deemed to be securities from other types of cryptoassets [7]. Guidance and official statements are often issued clarifying whether and which tokens are included within the regulatory compliance regime applicable to regulated financial markets. For example, the Australian Securities and Investments Commission advised that the nature of the asset determines whether it can be considered a financial product falling under the scope of the Corporations Act 2001 and thus subject to several licencing and regulatory compliance requirements on the part of issuers, intermediaries, processes and exchanges [17]. Similarly, in Canada, the Ontario Securities Commission issued a series of notices stating that most of the offerings of tokens, including cryptocurrency offerings and utility token offerings, such as ICOs and initial token offerings (ITO), involve a distribution of securities – usually as investment contracts – and would be subject to relevant regulatory requirements [18], [19]. Even when cryptoassets are not in themselves securities or derivatives, platforms involved in trading these assets might still be subject to securities legislation. Germany is an example of a broad approach to the application of existing legislation to cryptoassets, by recently adopting new rules which provide that cryptoassets qualify as financial instruments. This means that trading and custodian entities may require a licence and banks and investment firms are subject to specific regulatory requirements relating to financial services and financial instruments. The new definition of cryptoassets is broad enough to include utility tokens, investment tokens and payment tokens, as well as hybrids [20]. The UK Financial Conduct Authority issued comprehensive guidance on cryptoassets, which specified which participants involved in activities relating to security tokens, or to tokens that constitute e-money, or are involved in payment services, should seek authorisation or registration for carrying out a regulated activity [21]. Lithuania also opted to follow this approach by issuing guidelines on ICOs and STOs (security token offerings) stating that any digital asset akin to financial instruments – such as security tokens – must comply with the applicable national and EU regulatory regime [22], [23]. If the issued tokens grant the right to participate in the company management process, receive part of the company's profit or income, receive interest, recover the funds invested including through redemption of the tokens, or sell the tokens to another person, they will most likely be considered security and need to follow strict compliance requirements. In the United States, the Strategic Hub for Innovation and Financial Technology of the US Securities and Exchange Commission (SEC) published in 2019 two documents as guidance on digital assets. In the No-Action Letter [24] SEC's Division of Corporate Finance has stated that no enforcement action would be recommended if the tokens' issuer relied on the counsel's opinion that the tokens are not securities. The second document, "Framework for 'Investment Contract' Analysis of Digital Assets," [25] is intended as an analytical tool helping to determine whether the security laws apply to the offer, sale or resale of particular assets.

Application of the existing regulatory framework to certain cryptoassets potentially leaves other categories of cryptoassets, such as utility cryptoassets, outside the regulatory framework. It remains to be seen whether this approach remains the prevailing tendency or whether the regulators will develop bespoke and comprehensive regulatory solutions as the technology matures and the increasing amount of real case studies provide a valuable learning curve. Some jurisdictions have already introduced such bespoke regulations. Liechtenstein is one of the first countries to adopt a bespoke and comprehensive regulatory framework dedicated to tokenization [26]. Liechtenstein's unique and broad regulatory approach covers all applications of the token economy now and in the future and not only the ones related to financial markets. Liechtenstein's regulators see the potential of the token economy's ability to reproduce the physical world in a digital dimension in a legally certain way. They therefore focus on the two most important levels: the legal certainty of representation of the physical world on a blockchain and the reliability of service providers. In recognition of the vast spectrum of potential applications for the token economy and the limitations of existing definitions of cryptoassets, Liechtenstein regulators introduced a token container model with the abstract construct of a token, being a new, independent legal object recognised under the law as representing all kinds of rights. What is crucial in this model is that the creation of a token does not create a new right, but only subjects an existing right "uploaded" into the token to the storage and transfer rules of a blockchain network. To ensure the synchronisation of the digital and real world, the disposal of the token equals disposal of the right it represents.

Malta has also proved to be a very proactive jurisdiction in blockchain regulation with its own bespoke legal and regulatory framework in the form of three legal acts aimed at regulating blockchain technology, cryptocurrencies and service providers. These are the Malta Digital Innovation Authority Act, the Innovative Technology Arrangements and Services Act and the Virtual Financial Assets Act (VFAA). The VFAA is one of the first legislative acts in the word dedicated to regulating cryptocurrencies by evaluating the features and rights attached to the tokens through the "financial instruments test". This classifies tokens into virtual utility – non-exchangeable tokens, financial instruments, e-money and virtual financial assets. The VFAA deals with all blockchain-based assets. It also creates a bespoke regime for virtual financial assets which do not fit under any other category of blockchain-based assets [27].

The state of Wyoming also stands out as a jurisdiction with a novel and bespoke approach. It has passed 13 new acts to provide a comprehensive and blockchain friendly legal framework and to support the blockchain industry in its development. These include recognising direct property rights in all types of digital assets and adopting effective negotiability rules, which ensure digital token liquidity equal to that of money [28]. The state of Wyoming also created a fintech sandbox for up to 3 years to encourage financial innovation [29]. It established a new state-chartered depository for banking services for blockchain businesses [30]. In addition, Wyoming's new legislation created a new type of qualified digital asset custodian. This will recognise direct ownership of digital assets and clients will retain direct ownership of an asset, unlike in traditional securities custody arrangements, where investors own the securities indirectly and are subjected to the relationship with the custodian [28]. The legal proposition of direct ownership under bailment (giving up only control over an asset) of digital assets is truly an innovative and progressive solution [31].

Bermuda, Gibraltar, Mexico and Mauritius are other jurisdictions with specific regulations aimed at cryptoassets and service providers.

At the other end of the spectrum are jurisdictions, like China, Taiwan, Vietnam or Pakistan, for example, which have, to some extent, restricted blockchain technology activities. China's approach is particularly interesting as it is not only evolving towards better acceptance of blockchain technology, but it is characterised by a peculiar split attitude towards cryptocurrencies and other applications of blockchain technology. Individuals are not prevented from holding cryptocurrencies, but financial institutions are prohibited from offering cryptocurrency related services, making cryptocurrency tokens a grey legal area in China. In 2017, China banned all ICOs and all cryptocurrency and token exchanges through an "Announcement on Preventing ICOs Risks". At the same time the Central bank of China is moving towards launching their Central Bank Digital Currency. In February 2019, China enacted a legal framework for blockchain-based business (Blockchain Information Services Management Regulation), setting out registration and monitoring obligations, reporting obligations and obligations to provide records to authorities on demand. The distinctiveness of this approach consists of blocking specific content from blockchain networks through monitoring obligations and linking users to blockchain content through real name registration requirements. China has increasingly recognised the strategic importance and potential of blockchain technology. President Xi Jinping encouraged accelerating the development of blockchain technology as the core for innovation [32]. In October 2019, China passed a cryptography law and, while still banning cryptocurrency trading, the new law aims to answer regulatory and legal challenges in commercial cryptography and encourage research and development in the field and promotion of coherent blockchain industry standards [33].

Given the wide spectrum of regulatory approaches to blockchain tokens and mindful of cross border risks including money laundering, terrorism finance, tax evasion and regulatory arbitrage, international bodies and organisations have stepped in to address issues, assess regulatory gaps and foster international collaboration on global standards for the blockchain-based token economy.

After issuing a statement in March 2019, setting out high standards for banks engaging in cryptoasset activities, the Basel Committee on Banking Supervision published a discussion paper in December 2019 seeking views on matters related to the regulatory treatment of cryptoassets. These were intended to guide the design of a prudential treatment of banks' exposures to cryptoassets, including capital and liquidity requirements for high risk exposures [2]. The Committee for Payments and Market Infrastructures is mandated to promote the safety and efficiency of payments, clearing and settlement arrangements to support financial stability. It has been monitoring digital innovation and developing reports and working papers on matters involving distributed ledger technologies [34]. It also closely cooperates with the International Organization of Securities Commissions (IOSCO). The IOSCO closely monitors the cryptoasset market to ensure that risks, issues and key considerations are appropriate. In May 2019, the IOSCO published a report on the issues, risks and considerations relating to cryptoasset trading platforms, in which it defines three core objectives of securities regulation relevant to cryptoassets: protection of investors, fairness, efficiency and transparency of markets and reduction of systemic risk [35]. The Financial Stability Board also closely observes cryptoassets and monitors financial stability, regulatory implications and risks. It has issued a report on financial stability and regulatory and governance implications for decentralised financial technologies [36]. A number of other international bodies participate in the debate about blockchain technology and its implications for the financial system and the economy in general. The Financial Action Task Force (FATF) expanded the scope of its recommendations to broadly understand virtual assets and virtual assets service providers, who are required to comply with anti-money laundering and combating financial terrorism laws [37]. At the EU level, the Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG) published several recommendations for the regulation of distributed financial networks and cryptoassets [38]. The ROFIEG recognised the transformational potential of financial innovation and reaffirmed its readiness to establish an accommodative regulatory framework, while maintaining high standards of consumer protection, market integrity and the stability of the EU financial system. It also noted the absence of clear regulation on cryptoassets and distributed ledger technologies and the need for immediate and bold action. Particular recommendations for distributed financial networks and cryptoassets include the need to determine the relationship between participants for regulatory and supervisory purposes, ensure adequate applicability of terms and concepts, communicate regulations to addressees and address issues of operational resilience, exposure to cyber risks and systemic network failures. The ROFIEG emphasises the urgent need to complement and complete existing legal frameworks to address the lack of a common taxonomy for cryptoassets, resolve fragmented national approaches and legislate relevant conflicts of law, among other issues. Against the background of many international

reports, notes, studies and recommendations, the European Union has now taken the first step to assume its competence over cryptoassets by launching a consultation on an EU regulatory framework [42]. The objective of the consultation initiative is to provide clarity in relation to cryptoassets within the EU regulatory framework and to lay down a regulatory framework for those cryptoassets to which the existing regulations are not applicable. The consultation is an example of an attempt to find a comprehensive approach to all cryptoassets, those which fall under the existing financial regulations regime (like security tokens) and those which are new to the system (like utility tokens). The EU Commission aims to reduce the risk of regulatory arbitrage, minimise legal barriers, uncertainties and compliance costs and facilitate access to the market. The objective is to contribute to financial stability and market integrity while fostering technological innovation. The EU-wide regulatory framework would consolidate previous initiatives and reports on the subject by various EU and international organisations, standard setting bodies and industry stakeholders and provide much needed harmonisation and clarity across the EU territory. The EU-wide regulations could also provide a benchmark and standard for other regions and could be the first step towards international convergence in regulatory approaches to cryptoassets. The EU initiative illustrates that regulators are starting to approach cryptoassets in a broad sense, analysing all facets of this phenomenon and aiming to assess the whole cryptoasset ecosystem.

5. Conclusions

Designing an adequate regulatory framework for the blockchain-based token economy is a major challenge. Embracing the potential of and opportunities within blockchain tokenization while competently addressing new risks and challenges at national levels and across jurisdictions is a considerable task. So far, the technological developments of blockchain tokenization have not undermined the current structure of financial markets. They carry a promise of enormous opportunities for equity issuance, capital raising, efficiency gains and improved liquidity. The current broad array of regulations of blockchain-based cryptoassets and related activities vary considerably across jurisdictions and aim at meeting diverse policy objectives. When existing legal and regulatory frameworks are applied, authorities issue guidance, clarifications and warnings to market participants. Several jurisdictions have banned or restricted specific cryptoasset activities, although attitudes towards blockchain technology are evolving. Overall, more and more jurisdictions adopt a friendly regulatory approach towards cryptoassets by enacting dedicated regulation or by introducing various arrangements to promote blockchain technology, like regulatory sandboxes, for example. Nevertheless, the resulting overall picture is fragmented. This sketchy regulatory landscape is still far from achieving much needed consistency and even further from international harmonisation. Increasing disintermediation and decentralisation brought by blockchain tokenization warrants a more encompassing approach to regulation of the expanded financial ecosystem. The technology has developed faster than regulators have been able to comprehend and cater for so far. The emerging fragmentary and inconsistent regulatory approaches illustrate this lag of the law behind the technology. There are a few more dynamic and proactive jurisdictions like Liechtenstein and Malta, which have designed leading and creative regulatory solutions for cryptoassets. However, the vast majority of jurisdictions have a more reactive than proactive approach, which is often limited to clarification, guidance or a restrictive stance towards cryptoassets. Such regulatory discrepancies are undesirable for a unique, borderless and fast developing phenomenon like blockchain-powered cryptoassets. The risks to investors, established financial systems and market integrity are increasing with the continuing lack of adequate regulations. At the same time, opportunities can be missed and innovations stifled in the regulatory void. There are, however, some positive regulatory developments. Cryptoassets are no longer in obscure marginal territory, rather their potential has been recognised and they are firmly on the regulatory agenda. The EU regulatory initiative is an attempt at a thorough and comprehensive regulatory assessment of cryptoassets and can potentially represent a pivotal point for cryptoasset regulation. The appropriate recommendation for regulators is to step up, learn from those jurisdictions that have already competently responded and assist the industry, mitigating risks while fostering innovation. Achieving this elusive regulatory balance between embracing innovation and combating emerging risks is a major and urgent regulatory challenge that requires determination and international cooperation, since blockchain tokenization is designed with little regard to jurisdictional borders.

References:

[1] *European Central Bank, "Crypto-assets – trends and implications", June 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.en.html*

[2] Basel Committee on Banking Supervision, "Discussion paper: Designing a prudential treatment for cryptoassets, December 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.bis.org/bcbs/publ/d490.pdf

[3] P. Hacker, C. Thomale, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", European Company and Financial Law Review, vol. 15, pp. 645-696, 2018. Available: https://ssrn.com/abstract=3075820 or http://dx.doi.org/10.2139/ssrn.3075820

[4] S. Voshmgir, "Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy", BlockchainHub Berlin, Berlin, 2019.

[5] P. Tasca and C. J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification", Ledger, vol. 4, 2019. Available: 10.5195/ledger.2019.140.

[6] T. Euler, "The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens– Untitled INC", Untitled-inc.com, 2020. Accessed on: Jan. 7, 2020. [Online]. Available: http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

[7] A. Blandin, A.S. Cloots, H. Hussain, M. Rauchs, R. Saleuddin, J.G. Allen, B. Zhang, and K. Cloud, "Global Cryptoasset Regulatory Landscape Study", Cambridge Centre for Alternative Finance, University of Cambridge, Judge Business School, 2018.

[8] L. Oliveira, L. Zavolokina, I. Bauer and G. Schwabe, "To Token or not to Token: Tools for Understanding Blockchain Tokens", International Conference of Information Systems (ICIS 2018), San Francisco, USA, 12 December 2018 - 16 December 2018. Accessed on Jan. 8, 2020. [Online]. Available: https://doi.org/10.5167/uzh-157908

[9] ThinkBLOCKtank, "Position paper on the regulation of tokens in Europe (version 1.0)", ThinkBLOCKtank, June 2019. Accessed on: Jan. 8, 2020. [Online] Available: http://thinkblocktank.org/wp-content/uploads/2019/10/thinkBLOCKtank-Token-Regulation-Paper-v1.0.pdf

[10] Markets and Financial Instruments Directive (MFID II) 2014/65/EU and Regulation (EU) 600/2014; The Prospectus Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 replacing and repealing Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 and related measures; The Prospectus Directive 2010/73/EU; Market Abuse Regulation (EU) 596/2014.

[11] European Central Bank, "Virtual Currency Schemes.", 2012. Accessed on Jan. 8, 2020. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[12] G7 Working Group on Stablecoins, "Investigating the impact of global stablecoins", October 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.bis.org/cpmi/publ/d187.pdf

[13] R. Amsden and D. Schweizer, "Are Blockchain Crowdsales the New 'Gold Rush'? Success Determinants of Initial Coin Offerings", 2018. Accessed on Jan. 8, 2020. [Online]. Available online: https://ssrn.com/abstract=3163849

[14] L. Perlman, "Regulation of the Financial Components of the Crypto-Economy", SIPA's Entrepreneurship & Policy Initiative Working Paper Series, 2019. Available: https://ssrn.com/abstract=3493342 http://dx.doi.org/10.2139/ssrn.3493342

[15] D. Cumming, S. Johan and A. Pant, "Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty", Journal of Risk and Financial Management, vol. 12, no. 3, p. 126, 2019.

[16] Law Library Congress (US), Global Legal Research Directorate, "Regulatory

Approaches to Cryptoassets in Selected Jurisdictions", Law Library of Congress, Washington D.C., April 2019. [Online]. Available: https://www.loc.gov/law/help/cryptoassets/cryptoasset-regulation.pdf

[17] Australian Securities and Exchange Commission, "Information Sheet INFO225", May 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-assets/

[18] Ontario Securities Commission, "CSA Staff Notice 46-308, Securities Law Implications for Offerings of Tokens", Jun. 11, 2018. Accessed on Jan. 8, 2020. [Online]. Available: https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm

[19] Ontario Securities Commission, "CSA Staff Notice 46-307, Cryptocurrency Offerings (SN 46-307)", Aug. 24, 2017. Accessed on Jan. 8, 2020. [Online]. Available: https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm

[20] M. Huertas, R. Michels, and H. Schelling, "New German rules on cryptoassets", Dec. 2, 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.jdsupra.com/legalnews/new-german-rules-on-crypto-assets-78964/

[21] Financial Conduct Authority, "Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3", Policy Statement PS19/22, July 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.fca.org.uk/publication/policy/ps19-22.pdf

[22] Bank of Lithuania, "Guidance on Securities Token Offerings", May 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.lb.lt/en/consultations/guidelines-on-securities-token-offerings

[23] Bank of Lithuania, "Bank of Lithuania on Virtual Assets and Initial Coin Offering", October 2017, as amended on 21 January 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.lb.lt/en/news/bank-of-lithuania-position-on-virtual-assets-and-initial-coin-offering-reflects-changing-market-realities

[24] U.S. Securities and Exchange Commission, "Response of the Division of Corporate Finance, Re: TurnKey Jet, Inc. Incoming letter dated April 2, 2019, 3 April 2019. Accessed Jan. 8, 2020. [Online]. Available: https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.html.

[25] U.S. Securities and Exchange Commission, Strategic Hub for Innovation and Financial Technology, "Framework for "Investment Contract" Analysis of Digital Assets", 3 April 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.sec.gov/files/dlt-framework.pdf

[26] "Unofficial Translation of the Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) (Blockchain Act)." Accessed on Jan. 8, 2020. [Online]. Available: https://impuls-liechtenstein.li/wp-content/uploads/2019/11/054_Report-and-Application_TVTG_extract.pdf

[27] P.M. Parker, "Malta: FinTech Comparative Guide", Mondaq, 13 November 2019. Accessed on Jan. 8, 2020. [Online]. Available: http://www.mondaq.com/article.asp?articleid=857888

[28]State of Wyoming 65th Legislature, "SF0125 - Digital assets-existing law". Accessed on Jan. 8, 2020. [Online]. Available: https://www.wyoleg.gov/Legislation/2019/sf0125

[29] State of Wyoming 65th Legislature, "HB0057 - Financial technology sandbox". Accessed on Jan. 8, 2020. [Online]. Available: https://www.wyoleg.gov/Legislation/2019/hb0057

[30] State of Wyoming 65th Legislature, "HB0074 - Special purpose depository institutions". Accessed on Jan. 8, 2020. [Online]. Available: https://www.wyoleg.gov/Legislation/2019/hb0074

[31] C. Long, "What Do Wyoming's 13 New Blockchain Laws Mean?", Forbes, 4 March 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#36e724395fde

[32] H. Wu and R. Liu, "China's Xi urges acceleration of development of blockchain technology", Reuters, 25 October 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.reuters.com/article/us-china-economy-xi/chinas-xi-urges-acceleration-of-development-of-blockchain-technology-idUSKBN1X419Y

[33] D. Pan, "China's Congress Passes Cryptography Law, Effective Jan. 1, 2020", Coindesk, 26 October 2019. Accessed: Jan. 8, 2020. [Online]. Accessed on Jan. 8, 2020. [Online]. Available: https://www.coindesk.com/chinas-congress-passes-cryptography-law-effective-jan-1-2020

[34] https://www.bis.org/list/cpmi_all/sdt_1/index.htm

[35] Board of The International Organization of Securities Commissions Issues, "Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms Consultation Report", CR02/2019, May 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf

[36] Financial Stability Board, "Decentralised financial technologies Report on financial stability, regulatory and governance implications", June 2019. Accessed on Jan. 8, 2020. [Online]. Available: https://www.fsb.org/wp-content/uploads/P060619.pdf

[37] Financial Action Task Force, "Guidance for A Risk-Based Approach, Virtual Assets and Virtual Asset Service Providers", June 2019. Accessed on Jan. 8, 2020. [Online]. Available: http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[38] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, "Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): 30 Recommendations on Regulation, Innovation and Finance - Final Report to the European Commission", December 2019. [Online]. Available: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

[39] M. Carney, "The Future of Money", Speech given by Mark Carney, Governor of the Bank of England to the inaugural Scottish Economics Conference, Edinburgh University, 2 March 2018. Accessed 14 February 2020. [Online]. Available: https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418

[40] W. Kaal, "Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses", CodeX Stanford Journal of Blockchain Law & Policy, U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-07, 2018. Accessed on Jan. 8, 2020. [Online]. Available: https://ssrn.com/abstract=3117224 or http://dx.doi.org/10.2139/ssrn.3117224

[41] M. Demertzis and B. Wolf, "The economic potential and risks of cryptoassets: is a regulatory framework needed?", Policy Contribution, N.4, September 2018.

[42] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, 'Consultation Document on an EU framework for markets in crypto-assets', 19 December 2019. Accessed on 14 February 2020. [Online]. Available: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Agata Ferreira is the main author.

Funding:
None declared.

Acknowledgements:
None declared.

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(5)2020

The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework

Robert E. Campbell, Sr.
Capitol Technology University, USA
Correspondence: rc@medcybersecurity.com

Received: 24 February 2020 **Accepted:** 02 March 2020 **Published:** 16 March 2020

Abstract

Critical infrastructure sectors are increasingly adopting enterprise distributed ledgers (DLs) to host long-term assets, systems, and information that is considered vital to an organization's ability to operate without clear or public plans and strategies to migrate safely and timely to post-quantum cryptography (PQC). A quantum computer (QC) compromised DL would allow eavesdropping, unauthorized client authentication, signed malware, cloak-in encrypted session, a man-in-the-middle attack (MITM), forged documents, and emails. These attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. In 2018, Gartner revealed that a QC is a digital disruption that organizations may not be ready and prepared for, and CIOs may not see it coming.[1] On September 18, 2019, IBM announced that the largest universal QC for commercial use would be available in October 2019.[2] On October 23, 2019, Google officially announced "Quantum Supremacy," "by performing a calculation in 200 seconds that would take a classical supercomputer approximately 10,000 years."[3] DL cyber resilience requires "reasonable" measures, policies, procedures, strategies, and risk management before large-scale deployment. Cyber resilience implementations must be a critical component during the design and building phase, or during the initialization phase. The most significant existing attack vector for enterprise DLs is the public key infrastructure (PKI), which is fundamental in securing the Internet and enterprise DLs and is a core component of authentication, data confidentiality, and data and system integrity [1] [2]. Effectively implementing and managing a quantum-resistant PKI solution requires adherence to PKI standards, industry requirements, potential government mandates, certificate management policies, training personnel, and data recovery policies that currently do not exist. This research discusses security risks in enterprise DL PKI, areas that can be compromised, and provides an idea of what should be in a PKI DL Risk Management Framework plan.

Keywords: *token economy, blockchain regulation, blockchain law, securities law, technology law*

JEL Classifications: *K20, K22, K23, K24, O31, O38, G28*

Despite the vast opportunities distributed ledger technologies (DLT) offer, they suffer from challenges and limitations such as security and privacy, compliance, and governance issues that have not yet been thoroughly explored and addressed. There are many threats and numerous attack vectors, such as phishing, malware, implementation, and technology. While there are some studies on the security and privacy issues of DLT, they lack a systematic examination of the security of these systems at the fundamental level of digital signatures and public key infrastructure (PKI) vulnerabilities. Vulnerabilities and weaknesses lead to the execution of various security threats to the standard functionality of the distributed ledger (DL) platforms. The rapid development and progress of quantum computing technology are not considerations that CEOs and CIOs are correctly figuring in as a risk factor. Quantum computing poses global security concerns because the technology will be able to hack into and disrupt nearly all current information technologies. In this paper, the author explores the attack surfaces in the open-source-permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. The attacks considered are insider threats, certificate authority (CA) attacks, and private-key attacks from quantum computers (QCs). The author will examine single points of failure in Hyperledger Fabric's membership service provider (MSP), or PKI, which proves to be a centralizing aspect of a decentralized system and a significant weakness of the permissioned blockchain network. Also, the author presents a cyber-resilient framework as possible use in a hybrid post-quantum-resistant enterprise PKI. Cyber resiliency is a feature that must be in systems of the future, which, when implemented, will enable the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, and/or attacks. Both the global security risks and the economic benefits necessitate building in cyber resilience.

Digital Currency and Blockchains under Attack

In 2018 alone, $1 billion in cryptocurrency was hacked from exchanges,[4] approximately $2.7 million stolen per day, or $1,860 each minute. Upbit is the seventh major crypto exchange hack of 2019 so far.[5] Upbit is the largest victim of hacking to date, after losing $49 million at 9:00 UTC on November 26, 2019. The exchange stated that an "abnormal transaction" resulted in a 342,000 ether loss in a few minutes. Some of the most notable attacks occurred in June 2011, when a hacker was able to exfiltrate Mt. Gox's auditor's credentials and transferred 2,609 bitcoins (BTCs) to an address for which Mt. Gox had no keys. The second attack occurred in 2014, resulting in 750,000 BTCs ($350 million) stolen from the exchange, and Mt. Gox halted operations and filed for bankruptcy. The Bitfloor bitcoin exchange was hacked in 2012 when hackers were able to retrieve unencrypted private keys that were kept online for backups. The amount stolen was 24,000 BTCs. Poloniex was hacked in 2014 and only stated it "has lost 12.3% of its total bitcoin supply in an attack." The exchange also explained that "the hacker found a flaw in his site's code that processes withdrawals, and made multiple simultaneous withdrawals," and the system did not respond to this error. The major problem was a coding error, and "the auditing and security features were not explicitly looking for negative balances."[6] On January 4, 2015, Bitstamp announced that an anonymous hacker hacked it, and 19,000 BTCs (worth $5 million) were lost. In 2016, Bitfinex breached and claimed 120,000 BTCs (worth $72 million) hacked.

The attackers exploited a vulnerability in the multi-sig wallet architecture of Bitfinex and BitGo.[7] On May 7, 2019, Binance was hacked, losing more than 7,000 BTCs ($40 million). Binance announced that they discovered a large-scale security breach on May 7, 2019. The attackers were able to obtain user Application Orograming Interface (API) keys and 2FA codes. The attackers used techniques such as phishing, viruses, and other attacks, and the hackers were able to withdraw 7,000 BTCs from this one transaction.

Distributed Ledger Growth in Critical Infrastructure

Recent forecasts indicate that global blockchain technology revenues will experience rapid growth in the coming years, with the market expected to rise to over $60 billion worldwide in size by 2024. The financial sector is currently the largest investor in blockchain, with over 60% of the technology's market value concentrated in this field.[8] However, global enterprises are increasingly adopting DLT and are hosting critical assets and critical infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. As an example, the Energy Web Foundation (EWF) is a global organization that uses blockchain technology in the energy sector, with offices in Switzerland, Germany, and the United States. EWF launched the Energy Web Chain, in June 2019, and advertised "the world's first public, open-source, enterprise-grade blockchain tailored to the energy sector."[9] On December 12, 2019, the U.S. President's National Infrastructure Advisory Council published draft findings on the urgent cyber risks in the most critical and highly targeted private infrastructures and called for bold action.[10] The report indicated that escalating cyber risks to critical infrastructures present an existential threat to the continuity of government, economic stability, social order, and national security. Global governments and enterprises adopting DL are on the front lines of a cyberwar; they are ill-equipped to win against organized cybercriminals and nation-states intent on hacking, robbing, disrupting or destroying critical assets.

DLT Complexity

There are more than 30 known DL attack vectors in the categories of network, wallet, mining, double spending, and smart contracts and these attack can be phishing and social engineering, DNS hijacking, exchange hacks, 51% attacks, software flaws, and other types that can be malware and crypotjacking, and other traditional attacks that affect systems that connect to a blockchain [3]. The zero-day vulnerabilities cannot be quantified but must be considered as potential vulnerabilities that will be discovered and exploited. DLT consist of the integration of networked cryptography, fault-tolerance, and distributed consensus. Each of these topics is complicated, intricate and has many known vulnerabilities and weaknesses that are not well-understood by those who lack the technical background in these topics. Also, as with any complicated technology, there are always zero-day vulnerabilities yet to be discovered and made public. The combined technologies used to form DLT dramatically increase the vulnerabilities, threats, and weaknesses. This complexity, along with the intricacies of its ecosystem (wallets, exchanges, sidechains, mining pools, enterprise consortiums), requires a formal and logical framework to address issues systematically and mitigate them to make DLT resilient.

The Quantum Computer Threat

Google's "quantum supremacy" announcement means that QCs can process and solve massive computational problems that exceed the capabilities of current supercomputers and threatens DL cryptography. Complex mathematical problems are the foundation in which much of today's cryptography is based, including PKI and DL. DLT and PKI use asymmetric digital signature schemes for private and public-key generation, signing, verification of digital signatures, and QCs break and all of these functions. This public-key cryptography is in email, web browsing, encrypted storage, banking, virtual private networks, communications, critical infrastructures, and much of the Internet [2]. It would be exceptionally naive to think that covert research and development in "quantum supremacy" is not among the highest priorities of organized groups and nation-states around the planet. Further, it would follow that classified programs seek to protect actual capabilities, or there would not be a need for secrecy. Also, a QC attack could be difficult to detect because the attacker would derive the private key from the available public key, and with the private key, a hacker will have free and absolute access [4].

Impact of Compromised PKI Private Keys

PKI is the backbone of today's enterprise blockchain, DL, network, and internet security. Figure 1 is a depiction of Hyperledger Fabric's Managed Service Provider (MSP) services, which is essentially an abstraction of PKI for enterprise blockchains. Cyber resilience is methods and procedures that aid in preventing adversarial access to systems housing critical data while ensuring the integrity of data, despite the presence of the adversary on the network and being resilient to the adversary's efforts to manipulate data. DL must assume the existence of adversaries in the network and be capable of nullifying adversarial strategies by harnessing the computational capabilities of the honest nodes, and the information exchanged is resilient to manipulation and destruction [5].

Network DL private keys are the credentials and the means of authorizing transactions, which, if compromised, will make all assets controlled or secured by the keys freely available to an adversary. The private keys enable and allow the attacker(s) to capture information, passwords, compromise CAs, certificate forgeries, obtain other private keys, derive other private keys, hijack private keys, and forge validations. The attacks and risks associated with these malicious acts allow forged documents and emails, signed malware, unauthorized clients, eavesdropping, and man-in-the-middle (MITM) attacks. The impact of these activities can result in the loss of personally identifiable information (PII), protected health information (PHI), intellectual property (IP), reputation, assets, crippled operations, and human life.

Each MSP is in a folder with various subfolders containing the administrator certificate(s), root CA certificates, the node's private key, the node's X.509 certificate, and other optional inclusions. An X.509 PKI infrastructure is a security architecture or format used in intranets, networks, and the Internet. Its cryptographic mechanisms support functions such as email, server authentication, signature generation, and validation. Specifications such as the secure multipurpose internet mail extensions (S/MIME) and transport layer security (TLS) also rely on this standard. The MSP is used to link identities, public-keys, and CAs; it acts as the primary trusted authority and uses digital signature algorithms to sign certificates of trust. Key security considerations include the ability of untrusted or unauthorized persons to participate in the network and the strength of the bit security of the encryption protocols [2]. Administrative duties include providing access and permissions for the entire blockchain network and are thus a single point of centralization. Each participant on the network is assigned a digital certificate that assures they are whom they say they are and defines the levels of access and permissions. These administrators set the permissions along with a digital certificate; each participant is assigned what Fabric labels a digital signature or the private key half of a public-/private-key pair. These keys sign off on transactions and endorsements to ensure and retain the integrity of the blockchain [6].

In the case of an insider threat such as a rogue administrator, the holder of the administrator certificate(s) is not to be trusted and has free rein over the blockchain. Administrative controls such as adding or revoking access, adding identities to the Certificate Revocation List (CRL), MSP validation of CAs, and manipulating the access a given identity has to the blockchain network are all managed solely by the administrator. Digital certificates and identities are crucial to the operation of the MSP. Cryptogen, a utility for generating Hyperledger Fabric key material, provides a means of preconfiguring a network for testing, and produces all private keys in one

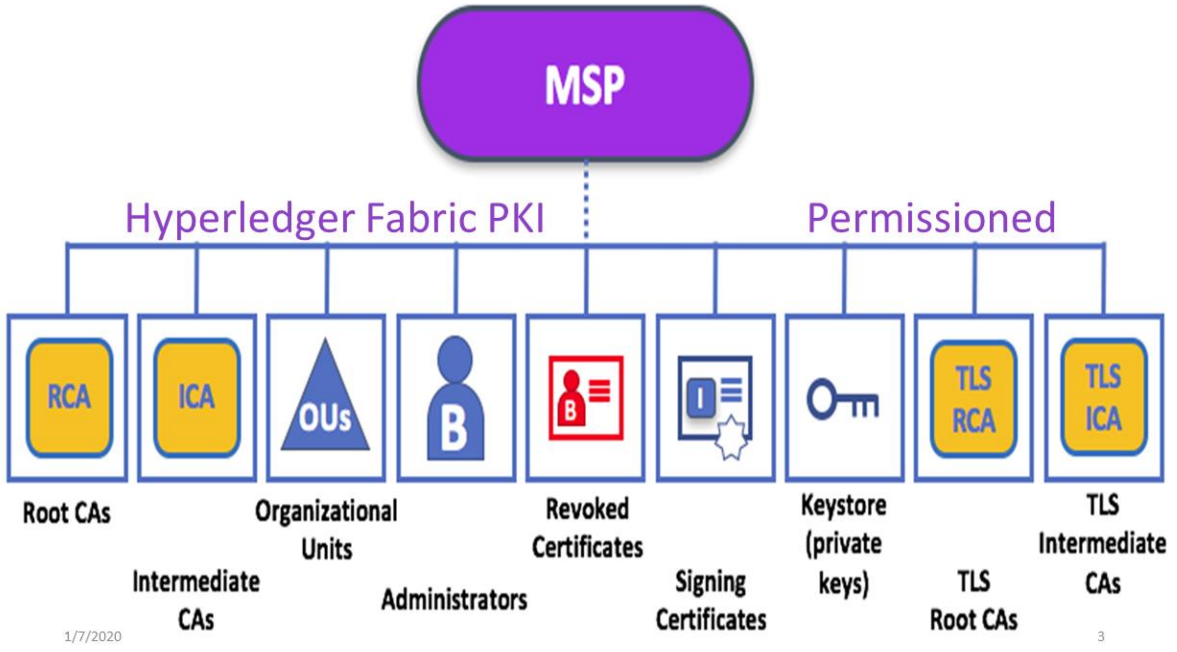
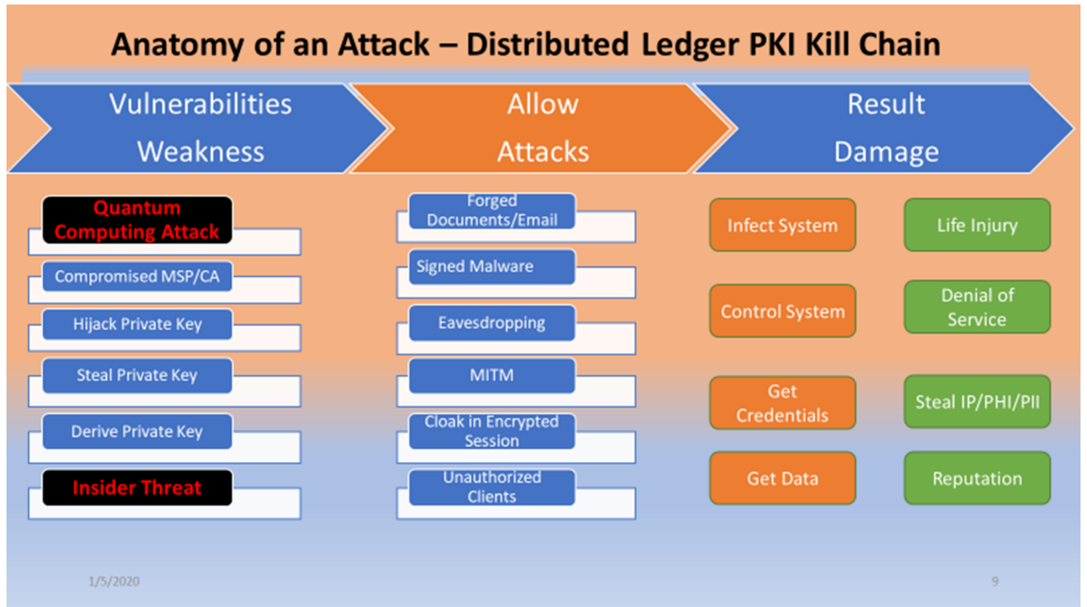


Figure 1. MSP Architecture. Source: Hyperledger Fabric.

centralized location, and it is then up to the user to adequately and safely copy them to appropriate hosts and containers. Allowing new users to decide key management best practices and the lack of standard procedures can easily lead to private-key leakage attacks. Private-key leakage is possible because each participant can choose to store and protect their private key in any way the member determines; there need to be key management best practices for all members [6].

An outside attacker obtaining private key(s) could lead to any number of attacks. As private-key leakage attacks provide potential unlimited access to the blockchain and open the possibility for any number of secondary attacks, they are one of the greatest threats to the MSP. The leakage of private keys or a successful quantum computing attack could further lead to more severe attacks, such as MITM attacks, replay attacks, message tampering attacks, and identity leakage attacks [6]. Figure 2 illustrates the weaknesses, threats, and risks of a compromised MSP or PKI in enterprise blockchains. A further shortcoming of CAs in Hyperledger Fabric is in the way it is implemented in the MSP. The MSP requires at least one root CA and can support as many root and intermediate CAs as desired. If the root CA certificate or implementation were attacked, all certificates leading back to the root certificate are compromised. Successful attacks on the MSP, which controls the membership of the blockchain runs on, would be detrimental to the security of the entire enterprise, resulting in falsified identities and more.


Anatomy of an Attack – Distributed Ledger PKI Kill Chain

Vulnerabilities Weakness

Allow Attacks

Result Damage

Quantum Computing Attack
Compromised MSP/CA
Hijack Private Key
Steal Private Key
Derive Private Key
Insider Threat

Forged Documents/Email
Signed Malware
Eavesdropping
MITM
Cloak in Encrypted Session
Unauthorized Clients

Infect System
Life Injury
Control System
Denial of Service
Get Credentials
Steal IP/PHI/PII
Get Data
Reputation

1/5/2020
9

Figure 2. Distributed Ledger Kill Chain.

Anatomy of a Critical Infrastructure Attack Scenario Using Hyperledger Fabric

The following is a hypothetical critical infrastructure attack scenario on an energy plant X using enterprise blockchains such as Hyperledger Fabric and the newly discovered Russian-linked malware, which infects safety instrumented systems (SIS), called Triton. The SIS are automated safety defense systems for industrial facilities, responsible for stopping plant operations in the event of an emergency and are designed to prevent equipment failure and catastrophic incidents such as explosions or fire. FireEye has linked Triton to the Russian state-sponsored hackers.[11]

Quantum Computing Attack Scenario

The hackers are equipped with QCs capable of cracking today's standard PKI cryptography started by researching and gathering information about energy plant X. They looked for network ranges, IP addresses, and domain names. Furthermore, the hackers also searched for email addresses of key players in the organization, such as CFOs, IT professionals, and CTOs. After getting access to the network, the hackers proceeded to infiltrate the organization's network. Once the private keys were derived or obtained, the hackers accessed the entire network and went through the system silently. The attackers, armed with private keys, quickly gained remote access to an SIS engineering workstation and deployed the Triton attack framework. Immediately they started to reprogram the SIS controllers as the infection entered the SIS workstation and system via remote access. Also, the malware compromised the target system's logic controllers, exploiting "zero-day" vulnerabilities and software weaknesses that have not been identified by security experts.

The attackers reprogrammed the SIS to allow an unsafe condition while using the distributed control system (DCS), which allows attackers the ability to monitor and control an industrial process remotely and to cause fires and explosions. The result is that the attackers manipulated the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately and giving false feedback to panel safety controls until it is too late to react. The attackers were able to exploit the weaknesses, vulnerabilities, and risks contained in the current enterprise architecture PKI technology and caused explosions and fires that destroyed the plant and caused the release of lethal gas and radioactive clouds causing massive injuries and loss of human life.

During the incident, none of the SIS controllers entered a visible failed safe state, which provided false safety readings and allowed the industrial process to continue under unsafe and dangerous conditions. The false readings prevented any investigation that would have alerted authorities and initiated an investigation. The attackers employed multiple techniques to conceal their activities and to deter digital forensic investigation of their tools and activities. They renamed the most typical and useful files to make them look legitimate like Microsoft update files or a legitimate Schneider Electric application; they also used hacker tools to mimic legitimate administrator activities.[12] The attackers were able to derive the private keys of critical personnel, including safety monitors, and took total control of energy plant X. They gained complete control of SIS and caused dangerous processes to go unnoticed by sending false data to the safety control panels. The panels showed normal readings when the actual condition was increasingly hazardous. This control of the SIS and the extreme safety condition continued until it was too late, and it caused many explosions and the destruction of the plant and release of lethal and toxic clouds.

Urgent Need for Risk Management Framework for Distributed Ledger Systems

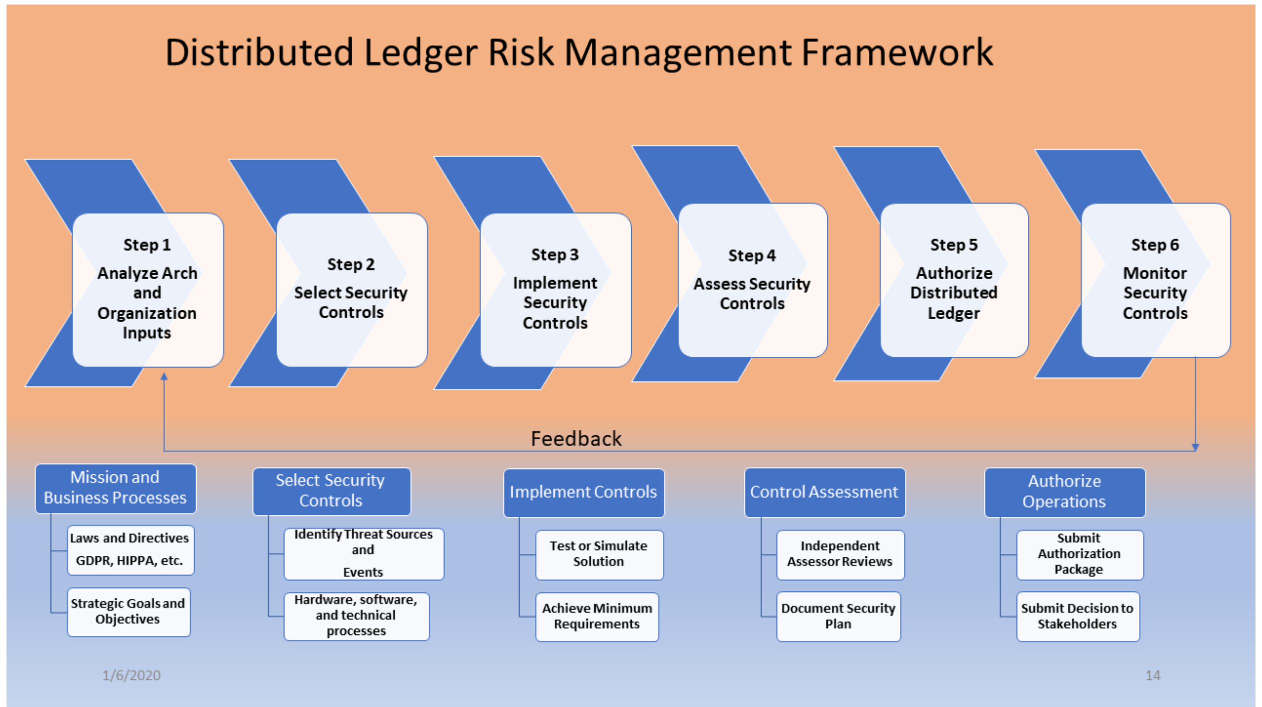
There is a pressing need to strengthen further the DL information systems, component products, and adopted services in critical infrastructures and enterprise sectors. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise. Cyber resiliency can be for system elements, systems, missions or business functions, and the system-of-systems which support those functions, organizations, sectors, or transnational missions/business functions. Nation-states and other well-resourced adversaries have intensified their efforts to infiltrate and gain control of enterprise networks and critical infrastructures, such as financial services and energy and if successful, these could impact the continuity of government, public safety, economic stability, and national security. Global enterprises are on the front lines of a cyberwar; they are ill-equipped to fully understand, thwart, or counter against nation-states' intent upon disrupting and destroying critical infrastructure. Cyber resilient DL systems require developing an integrated approach to building trustworthy systems. The author has modified SP 800-37 Rev. 2 guidelines and recommended steps to help build a more defensible information technology infrastructure, including the component products, systems, and services [7]. Systems security engineers must apply the necessary security measures that assure the system can withstand cyber faults, failures, and attacks.

Mitigating Cyberattacks on Permissioned DLTs

While no known technology, method, or procedure can categorically prevent cyberattacks, some steps and procedures can be put in place to mitigate attacks. The architecture, deployment, and operation impact the network's cybersecurity risks and determine the controls that are best able to reduce those risks. Mitigating considerations include the number and types of participants in the system; unauthorized persons to access the network; the design and sturdiness of the consensus validation rules and processes; the strength of the encryption protocols and the sensitivity of the data or transactions recorded in the ledger; and the ability to correct fraudulent, malicious, or erroneous files or data. At a high level, Figure 3 represents cybersecurity principles and controls of best practices that can be implemented on compromised CA, MSP, public keys, or private keys. These principles and controls include access controls, threat modeling, systems, and procedures to detect actual and attempted attacks or intrusions and risk management practices. The most important contribution this modified framework offers is the ability to adapt, survive, and continue operations with minimum disruption and loss. This framework can be used in building, deploying, and operating DL systems and outlines logical step-by-step procedures needed for cyber resiliency.

Resources Needed for Incident Response

Cyber resilient DL systems must have a business continuity planning (BCP) that delineates the organization's use of strategies, procedures, technical measures, and plans necessary for the recovery of lost data, operations, and systems in the event of a business disruption. The BCP includes a management plan, data backup plan, disaster recovery plan, and an emergency mode operation plan. The plans must consist of roles, responsibilities, and communication strategies in the event of a compromise or disaster, including notification of relevant external partners. Data backup plan is required to establish necessary procedures to ensure the maintenance and retrieval of exact copies of stored regulated data. The disaster recovery plan creates procedures and processes that will assist the restoration of any lost data in case of disaster, system failure, or cyberattacks. This plan is crucial, especially in the case of a cyberattack that may disrupt access to such data for an extended period. This will also require creating an inventory of all the sensitive data and systems that will be necessary for the restoration of an enterprise's activities. The emergency mode operation plan is used to ensure the continuity of an enterprise's operations while protecting critical assets and regulated data. This operation plan assists an organization in resuming its normal operations in the event of a disaster, emergency, system failure, or cyberattack. The plans should be tested and revised as necessary to ensure that the procedures put in place are effective. The main goal should be periodic testing of written contingency plans to identify weaknesses and making necessary revisions on the documentation. Figure 3 outlines the primary phase in the Distributed Ledger Risk Management Framework.



Distributed Ledger Risk Management Framework

Step 1
Analyze Arch and Organization Inputs

Step 2
Select Security Controls

Step 3
Implement Security Controls

Step 4
Assess Security Controls

Step 5
Authorize Distributed Ledger

Step 6
Monitor Security Controls

Feedback

Mission and Business Processes
- Laws and Directives GDPR, HIPPA, etc.
- Strategic Goals and Objectives

Select Security Controls
- Identify Threat Sources and Events
- Hardware, software, and technical processes

Implement Controls
- Test or Simulate Solution
- Achieve Minimum Requirements

Control Assessment
- Independent Assessor Reviews
- Document Security Plan

Authorize Operations
- Submit Authorization Package
- Submit Decision to Stakeholders

1/6/2020

14

Figure 3. Distributed Ledger Risk Management Framework.

The Distributed Ledger Risk Management Framework starts with Step 1, analyzing the organizational architecture documents and reference materials external to the enterprise. This step is in the context of determining the criticality of the information and system according to potential worst-case, adverse impact on the organization, mission/business functions, and the system. These documents include policy and procedures, data regulating requirements, and laws for protected data such as the General Data Protection Regulation (GDPR) Health Insurance Portability and Accountability Act (HIPAA), Financial Industry Regulatory Authority (FINRA). In this phase, the business processes, objectives, and goals must align with the overall platform design and performance. Selecting security controls in Step 2 is based upon the output of Step 1, which builds the baseline using categorization. Step 2 specifies a minimum baseline of security controls for countermeasures prescribed for the system designed to ensure the integrity, confidentiality, and availability of its information and to meet a set of defined requirements. Step 3 implements security controls within the enterprise architecture and systems using solid system security engineering practices. Step 4 determines security effectiveness—assessing whether the controls are implemented correctly, operating as intended, and meeting the security requirements for the system and environment of operation. Step 5 involves a documented independent assessment of security controls, and this information is promulgated to all stakeholders to ensure everyone understands the configuration changes and its potential impact on operations and business. The authorizing official (AO) examines the output of the security controls evaluation to determine whether or not the risk is acceptable. Step 6 monitors security controls for effectiveness and includes a communication or feedback loop that goes back to Step 1. Continually monitoring the controls applied for the system and its ecosystem of operation for changes, indications of attack, and so on may affect regulation and reassess control effectiveness.

Cyber Resilient Distributed Ledger Systems and NIST Post-quantum Project

Google's surprise announcement of quantum supremacy is a warning to all that quantum computing advances are not predictable. Cyber resiliency requires the ability to react quickly to cryptographic threats by implementing alternative methods of encryption. Specifically, it requires the ability to respond to incidents, has an inventory of all certification and cryptographic keys from all issuing authorities, and is capable of quickly migrating the PKI to new post-quantum resistant PKI algorithms. National Institute of Standards and Technology (NIST) is in the process of choosing one or more public-key cryptographic algorithms through a public competition-like process. The latest public-key cryptography standards will specify one or more additional digital signature and public-key encryption algorithms. These algorithms will likely be capable of protecting sensitive information well into the foreseeable future, including after the advent of QCs. NIST has down-selected a group of potential cryptographic algorithms—down to a bracket of 26. These algorithms are the ones that NIST mathematicians and computer scientists consider to be the strongest candidates. The 9 second round candidates for digital signatures are CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, and SPHINCS+[13]. While NIST does not expect to formalize new post-quantum cryptography (PQC) standards until the 2022–2024 time frame,[14] the enterprises cannot afford to wait. The time is now to begin independent testing and evaluation of the most promising NIST candidate algorithms toward migration and replacement. The path to a successful migration is lengthy and complicated.

Recommendations

It is of note that this research does not specify any of the NIST second-round candidate algorithms will be a straightforward "drop-in replacement"; it may need additional NIST rounds and years of follow-on research, analysis, and testing for a suitable "drop-in replacement" to be identified or developed. Therefore, the author believes that now is the time to test possible near-term "Hybrid Quantum Resistant Classical

Public Key Infrastructure," a solution with an aim of seeking reductions in public-key size as one of the most significant parameters. It is the public key that is exposed and used the most in today's PKI systems, and it is possible to modify the X.509 certificate standard to accommodate new PQC algorithms, which would only provide the public key that would be much more resistant to implementation and quantum computing attacks. Additional research is needed on approaches to introducing new PQC algorithms (e.g., hybrids) within live systems that must remain interoperable with other systems during the period of industry migration. This includes such areas as penetration testing, formal testing, formal modeling, automated tools, and approaching transition in complex infrastructures. There is a critical need for research to understand and quantify the implications of replacing today's public cryptography algorithms.

Conclusion

Google's surprise announcement of quantum supremacy is a notice to all that quantum computing advances cannot be perfectly projected. Quantum computing attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. PQC-safe algorithms generally have higher computation, memory, storage, and communication requirements; research and prototyping are needed to understand performance, security, and implementation. In this paper, the author explored the attack surfaces in open-source permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. Despite the vast opportunities DLT offer, they suffer from challenges and limitations such as security and privacy, compliance and governance issues. The author examined single points of failure in Hyperledger Fabric's MSP, or PKI, which prove to be a centralizing aspect of a decentralized system and a significant weakness of the permissioned blockchain network. Further research is required on policy, process, and people. Global enterprises are increasingly adopting DLT and are hosting critical assets and infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. As an example, EWF is a global organization that uses open-source blockchain technology in the energy sector without clear or public plans and strategies to migrate safely and timely to PQC. There is a pressing need to further strengthen the critical infrastructures and enterprise sectors and adopted DL information systems, component products, and services. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise.

References

[1] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," 2019. [Online]. Available: https://jbba.scholasticahq.com/article/7679-evaluation-of-post-quantum-distributed-ledger-cryptography. [Accessed 21 9 2019].
[2] R. Campbell, "Transitioning to a Hyperledger Fabric Quantum-Resistant Classical Hybrid Public Key Infrastructure," 31 July 2019. [Online]. Available: https://jbba.scholasticahq.com/article/9902-transitioning-to-a-hyperledger-fabric-quantum-resistant-classical-hybrid-public-key-infrastructure. [Accessed 21 September 2019].
[3] H. Chen, M. Pendleton, L. Njilla and S. Xu, "A Survey on Ethereum Systems Security" 13 August 2019. [Online]. Available: https://arxiv.org/pdf/1908.04507. [Accessed 7 1 2020].
[4] A. Majot and R. V. Yampolskiy, "Global catastrophic risk and security implications of quantum computers," Futures, vol. 72, no., pp. 17–26, 2015.
[5] S. Bagheri and G. Ridley, "Organisational cyber resilience: research opportunities," 2017. [Online]. Available: https://eprints.utas.edu.au/25820. [Accessed 7 9 2019].
[6] A. Davenport, X. Liang, and S. Shetty, "Attack Surface Analysis of Permissioned Blockchain Platforms," September 2018. [Online]. Available: https://par.nsf.gov/servlets/purl/10083311. [Accessed 8 1 2020].
[7] J. T. Force, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. [Accessed 8 1 2020].
[8] V. Lyubashevsky, T. Güneysu, T. Poppelmann, and D. Stehlé, "Post-Quantum Cryptography - Round 2 Submissions," 30 March 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. [Accessed 14 January 2020].

[1] Gartner Reveals Seven Digital Disruptions CIOs May Not See Coming: https://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-reveals-seven-digital-disruptions-cios-may-not-see-coming

[2] IBM's new 53-qubit quantum computer is the most powerful machine you can use: https://www.technologyreview.com/f/614346/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/

[3] Quantum Supremacy Using a Programmable Superconducting Processor: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

[4] How Hackers Stole $1B From Cryptocurrency Exchanges In 2018: https://www.forbes.com/sites/daveywinder/2018/12/31/how-hackers-stole-1b-from-cryptocurrency-exchanges-in-2018/#7066025e4d87

[5] Upbit Is the Seventh Major Crypto Exchange Hack of 2019: https://www.coindesk.com/upbit-is-the-sixth-major-crypto-exchange-hack-of-2019

[6] Yet another exchange hacked: Poloniex loses around $50,000 in bitcoin: https://arstechnica.com/information-technology/2014/03/yet-another-exchange-hacked-poloniex-loses-around-50000-in-bitcoin/

[7] The Binance Hack: https://medium.com/coinmonks/the-attack-on-binance-eba46700eef6

[8] Blockchain Market Shares, Market Strategies, and Market Forecasts, 2018–2024: https://www.ibm.com/downloads/cas/PPRR983X

[9] The Energy Web is unleashing blockchain's potential in the energy sector: https://www.energyweb.org/

[10] NIAC TRANSFORMING THE U.S. CYBER THREAT PARTNERSHIP DRAFT REPORT: https://www.cisa.gov/publication/niac-transforming-us-cyber-threat-partnership-draft-report

[11] TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers: https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

[12] SAS 2019: Triton ICS Malware Hits A Second Victim: https://threatpost.com/triton-ics-malware-second-victim/143658/

[13] PQC Standardization Process: Second Round Candidate Announcement: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

[14] Post-Quantum Cryptography: Workshops and Timeline: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Robert E. Campbell, Sr. designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Robert E. Campbell, Sr. would like to thank Dr. Ian McAndrew,
Dean of Doctoral Programs.

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(4)2020

Crypto Governance: Analysing and Comparing Crypto Assets Trading Platforms

Sabino Correa
London Business School, London, UK
Correspondence: scorrea.sln2019@london.edu

Received: 30 October 2019 **Accepted:** 24 January 2020 **Published:** 18 February 2020

Abstract

The annualised volume of Crypto Exchange markets reaches the trillion dollars threshold. Due to the dispersed and decentralised nature of this market, in which each Crypto Asset trading platform works as an independent dark pool, official statistics is unavailable and there is little private research data. The objective of this paper is to present a brief overview of the global Crypto Exchange market, providing an inventory of the available Crypto Exchanges as of the end of 2018, and compare the most relevant in both quantitative and qualitative terms. From a sample representing 99% of a daily global market share, measured by trading volume, a Key Performance Indicator system is proposed and tested to evaluate the level of corporate governance (or 'crypto governance') observed at each Crypto Exchange. The outputs are compared with average fees and individual market shares. The results obtained from market data provide evidence that most of the volume is traded at Crypto Exchanges with lower governance scores, while those ranked with higher governance scores charge, on average, higher trading fees.

Keywords: *Crypto Exchanges, Crypto Governance, Crypto Currencies, Blockchain, Crypto Finance, Crypto Assets*

JEL Classifications: *D04, F02, F03, F04, F06, G01, G02, G03, O03, P02, P04*

1. Introduction

The market structure of Crypto Assets operates through, mostly unregulated, private trading platforms. These enterprises are predominantly run by tech entrepreneurs, although there are also some Venture Capital and Private Equity initiatives in the sector. Despite the controversy regarding the use of the term 'Exchange' [1], this terminology is widely used by participants in this market. Therefore, the term 'Crypto Exchange' will be adopted by this paper to refer to any kind of business, whether locally regulated or unregulated, that trades, or promotes the trading of, Crypto Assets. Currently, a comprehensive regulation framework for Crypto Exchanges does not exist, which means that only a small fraction of participants in the market are able to present accurate information about being licensed by local financial authorities.

1.1. Sources of information

Normally, consolidated reports from local authorities provide an updated list of active institutions or market statistics, for instance this information on banks and brokers is available through each country's central bank and the local securities' commission database, respectively. Due to the decentralised nature of the Crypto Exchange market, there are no comparable information services. Nor is there an international institution similar to the Bank of International Settlements (BIS), which compiles data from countries worldwide into periodic reports or online services, opening a window on traditional worldwide banking activity. Thus, the assessment of global crypto market data requires an independent research on its own, a task which falls within the scope and aims of this paper. Therefore, information must be compiled from independent sources and overlaps purged, yet this exercise does present challenges. The deficiency of standardised information in this sector is reflected in the many different providers of information who use similar denominations but produce diverse results.

At the end of 2018, the website bitcoin.org, which is the closest available equivalent of an official source of information, listed 72 exchanges, by contrast, bitcoinwiki.org listed 219, Wikipedia listed 49 and List.Wiki listed 136. Major private resources also display inconsistent findings, for example, at the end of 2018, Howtobuybitcoin.info listed 110 exchanges, the CryptoCompare platform listed 185 exchanges and CoinMarketCap listed 229. These numbers are summarised in Table 1, and, after purging overlaps, the total number of Crypto Exchanges amounts to 473 worldwide.

Table 1. Summary of Global Crypto Exchanges Information Sources

Source	Nr.	URL:
Bitcoin.org	72	https://bitcoin.org/en/exchanges
Bitcoin.org wiki	219	https://en.bitcoinwiki.org/wiki/Cryptocurrency_exchanges_list
Wikipedia	49	https://en.wikipedia.org/wiki/List_of_bitcoin_companies
list.wiki	136	https://list.wiki/Cryptocurrency_Exchanges
How to Buy Bitcoin	110	https://howtobuybitcoins.info/#!/
CryptoCompare	185	https://www.cryptocompare.com/
Coinmarketcap .com	229	https://coinmarketcap.com/rankings/exchanges/
Net Number	473	(Total after purging overlaps)

As the market matures over the following years, consolidation of the vast number of exchanges is expected. Signals for this trend are already evident. Amongst the gross data set there were 81 extinct Crypto Exchanges and 8 that have undergone M&A processes.

A proper comparison of the substantial number of members would require some prior level of categorisation, which is a proposal examined in Section 1.2.

1.2. Categories of Exchanges

Although a taxonomic definition is beyond the scope of this paper, some conceptual aspects regarding the different structures of Crypto Exchanges should be highlighted. A formal definition would be difficult to achieve in an innovative and constantly mutating environment, but there is latitude to recognise the main concepts and qualities within the market. Therefore, four main types of Crypto Exchanges are proposed:

- **Regular Crypto Exchanges:** These exchanges resemble the traditional stocks of FX brokers, receiving Fiat currencies (money), or the tradable asset itself (Crypto Assets), allowing individuals to trade and withdraw as Fiat or Crypto afterward. The first kind of transaction is usually known as 'Crypto to Fiat', and the second as 'Crypto to Crypto'. Those exchanges work as a traditional business, having a controller, administrator, registry, physical office and jurisdiction.

Examples of this type of regular Crypto Exchanges include OKEx, Binance, Coinbase and Bitstamp.

- **Decentralised Crypto Exchanges:** These are exchanges which the transactions are not performed at a single place – just like the very concept of blockchain, the transactions are distributed along the internet. In contrast to regular Crypto Exchanges, decentralised Crypto Exchanges can work without a traditional business framework because it is possible to implement them with neither formal registry, physical office nor jurisdiction.

Examples of this type of decentralised Crypto Exchanges include IDEX, Alcoin.io and Bisq.

- Peer-to-Peer (P2P) Crypto Exchanges: These are platforms that provide the information and means for two parties (the seller and the buyer) to transact directly with each other. A parallel can be drawn with the role that eBay plays between individuals trading goods.

Examples of this type of P2P Crypto Exchanges include Localbitcoins.com and Paxful.

- Conversion Platforms: These are available as apps that provide a similar service to that offered by regular 'Crypto to Crypto' Exchanges and perform the same task, while converting one digital asset into another. In spite of that, they are not formally actual regular Crypto Exchanges as they use much straightforward processes, without the requirement of opening an account prior to engaging into the first transaction. Some of those conversion platforms allow customers to use their services directly from and into their digital wallets.

Examples of conversion platforms include Shapeshift and Conswitch.io.

The scope of this work is limited to the assessment of regular Crypto Exchanges, as defined here. The portal coinmarketcap.com acts as the source of information for trading volumes and market share. The information used was downloaded January 1, 2019, and represents worldwide transactions recorded during the preceding 24-hour trading. All the quantitative analysis in this work only uses data for spot transactions. It avoids markets with no fees or transaction mining because they are more susceptible to irregular price support and price manipulation practices using US dollar proxies (e.g. USDT) [2].

The assessment of data for each Crypto Exchange cites the source of information as the one available on the website of each Crypto Exchange. Collateral or indirect sources of information (e.g. Wikipedia, Press or independent reviews) are not considered.

2. Academic Overview of Crypto Markets

Academic interest in cryptocurrency governance has increased. Studies range from the market structure [4], to financial networks [5] and legal aspects [6] or risks [7]. Yet, there is a scarcity of research regarding the assessment of Crypto Exchange governance. Academic evidence suggests that a significant portion of users approach digital currencies because they want to participate in an alternative investment vehicle [3]. As pointed out by Böhme et al., Crypto Exchange trading activities work much like traditional financial markets [8].

Nevertheless, most of the crypto adopters do not seem to exercise the same level of caution found in other types of commercial dealing.

Many of the top ranked exchanges (by trading volume activity) do not fulfil the most basic governance requirements for safeguarding the interests of consumers and investors, such as the identification of company name, address or the country where it is based. This paper proposes and tests the use of a crypto governance KPI to measure and compare each Crypto Exchange governance levels. The proposed scoring system addresses some key points to provide better security for users.

The adopted criterion for selecting the exchanges that will compose the study sample was to pick top-down Crypto Exchanges, representing 99% of the total market share, measured by a daily, 24-hour global trading volume, obtained from coinmarketcap.com portal, comprising data from 00:00 to 23:59 on 31 December 2018. The 99% threshold is adopted ad hoc.

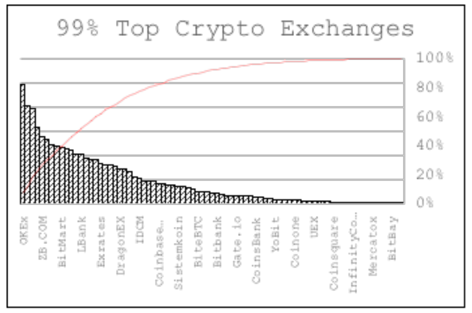


Chart 1: 99% Representative Sample Selection

The outcome of this assortment results in 78 Crypto Exchanges, which are each measured according to the crypto governance Key Performance Indicators (KPI) described in Section 3. In addition to the governance assessment, the levels of fees for a 'taker' trading transaction for each of the evaluated Crypto Exchanges are also measured and compared. For Crypto Exchanges that have different fees depending on the transaction value, the adopted criterion considers a standard transaction of US$ 10,000.00.

The governance score results are framed according to the market share of each exchange and market fees, providing some evidence on the Crypto Assets consumer's or investor's preferences.

3. Comparing Crypto Exchanges

In this section the proposed governance KPI criteria are described in subsection 3.1 and individual results are presented in subsection 3.2. The trading fees for each of the Crypto Exchanges are also evaluated and compared in subsection 3.3, and the cross results are displayed and analysed in subsection 3.4.

3.1. Crypto Exchanges Governance KPI

The proposed crypto governance qualitative measurement criteria are based on seven basic key questions regarding aspects of the following areas: legal compliance, years of activity in the market, jurisdiction clarity and authority regulation, as summarised in Table 2.

The KPI questions, their type and the logic of required answer are described below.

i. Does the Crypto Exchange provide clear information about the company's name and registry identification?
Type of Variable: Boolean (True/Yes=1 or False/No=0);

ii. Does the Crypto Exchange provide clear information about its key personnel and management team identification?
Type of Variable: Boolean (True/Yes=1 or False/No=0);

iii. Does the Crypto Exchange provide clear information about its controllers and investors' identification?
Type of Variable: Boolean (True/Yes=1 or False/No=0);

iv. Does the Crypto Exchange provide clear information about its number of years of activity in the market?
Type of Variable: Scale/Range ("No" and Less or equal to 1 year = 0; from 1 year up to less than 2 Years = 1; from 2 years up to less than 3 years = 2; more than 3 years = 3);

v. Does the Crypto Exchange provide clear information about its jurisdiction of incorporation?
Type of Variable: Boolean (True/Yes=1 or False/No=0);

vi. Does the Crypto Exchange present obscurity on its jurisdiction of control?
Type of Variable: Boolean (True/Yes=0 or False/No=1);

vii. Is the Crypto Exchange authority regulated?
Type of Variable: Boolean (True/Yes=3 or False/No=0);

The KPI questions and scores are summarised in Table 2.

Table 2. KPI Score Summary

Crypto Exchanges Governance Proposed Key Performance Indicators (KPI)		
Topic	**Minimum Points**	**Maximum Points**
Legal Compliance		
Company name and Registry Identification	0	1
Key personnel and Management identification	0	1
Controllers and investors identification	0	1
Years of Activity		
Number of Years	0	3
Jurisdiction of Incorporation		
Clear Jurisdiction of Incorporation	0	1
Clarity about Controller Jurisdiction	0	1
Authority Regulation		
Clearly presents as Authority regulated	0	3
Number of Points	**0**	**11**

A more straightforward measure can be obtained using a simplified Overall Level attribution by ranges:

Table 3. Overall Governance Level

Score Range	0 to 3	4 to 6	7 and above
Overall Governance Level	Poor	Fair	Good

3.2. Comparing Crypto Exchanges Governance Scoring Results

Chart 2 summarises the distribution of results for the KPI governance evaluation for the top 78 Crypto Exchanges measured. The data provide evidence that, using the proposed criteria, most of the Crypto Exchanges currently present low governance scores.

It is remarkable that most of the KPI topics are seamlessly achieved, and (except from the 'Authority Regulated' question) they could easily be accomplished by many ordinary non-crypto businesses. Conversely, Crypto Exchanges that handle enormous volumes of monetary transactions do not offer the minimum acceptable levels of governance; some of them do not even inform properly the jurisdiction where they are located.
As shown in Chart 3, from the overall level perspective, more than two-thirds of the exchanges are in the 'Poor' level of governance range, 22% are within the 'Fair' level range, while only 10% can be classified as 'Good'.

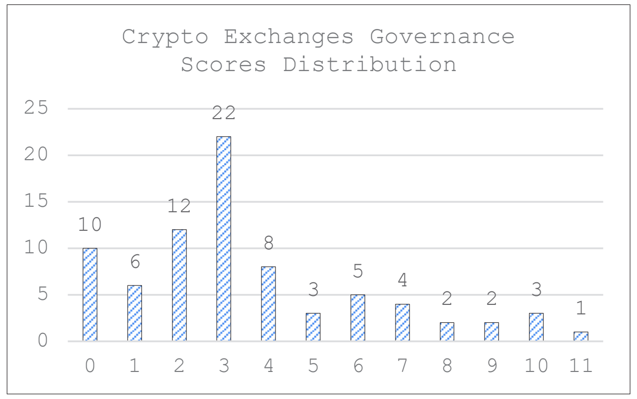


Chart 2: KPI Governance Scores Distribution

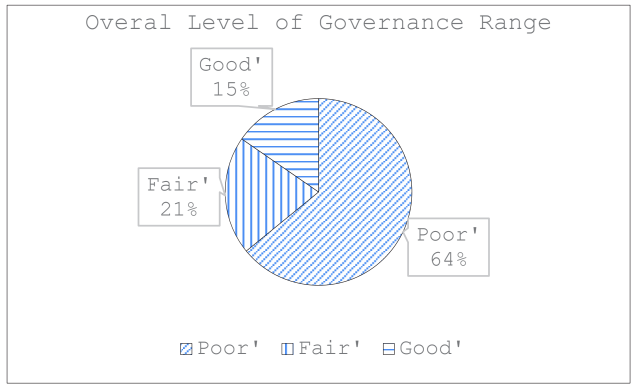


Chart 3: KPI Governance Scores Distribution

3.3. Comparing Trading Fees

To ensure a fair comparison, data regarding the trading fee at each Crypto Exchange was obtained using the same type of transaction. The adopted standard computes the fee for a 'Taker' order, which is a type of fee that can be found in all 78 components of the sample and maintains the same meaning across all the different researched exchanges. The minimum fee found for a 'Taker' order was 0.00% (which might raise questions regarding the bid/ask booking transparency, as none of the analysed exchanges present themselves as a non-profit organisation). The maximum fee currently being charged among the sampled exchanges is 1.00%. For 11 Crypto Exchanges it was not possible to find clear information about the fees, and the overall simple average fee for the group is 0.19%. The distribution of results is presented in Chart 4.

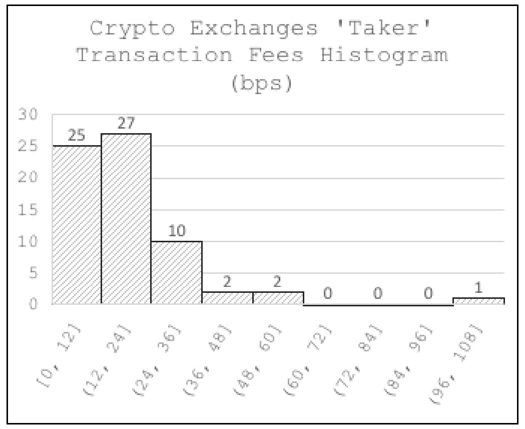


Chart 4: Frequency of Fees Histogram

3.4. Cross Results

3.4.1. Comparing Fees and Governance Scores

The cross results between Crypto Exchange governance scores, market share and fees offer a better comparison of the macro aspects of the Crypto Assets Exchanges' market. The breakdown of the simple average of the trading market fees found in this research, as illustrated in Chart 5, provides evidence that the Crypto Exchanges practicing higher levels of governance (according to this paper's criteria) are able to charge higher fees as their customers seem to be willing to pay a 'premium' for more reliable services. The cross results for crypto governance scores and average fees suggest that better governance in Crypto Exchange markets can be converted into more added value to the business. A more detailed overview on the distribution of fees per each Crypto Exchange governance score is portrayed in Chart 6. All fees are presented here in basis points (10-4).

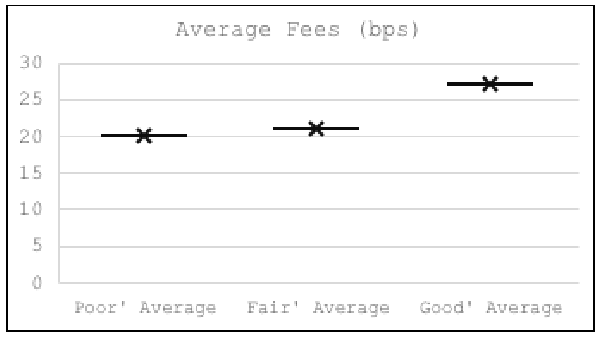


Chart 5: Average Fees by Governance Range

The individual fees chart below gives a better vision of the distribution with more accuracy about the behaviour of outliers.

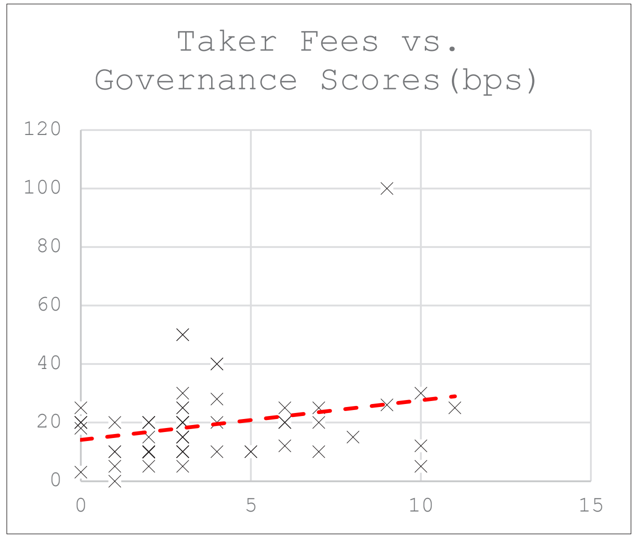


Chart 6: Fees (bps) per Exchange per Governance Score

Both average, aggregate results and individual data indicate that the well-governed Crypto Exchanges are able to charge higher fees on average. To better illustrate this point, Chart 6 highlights a linear tendency line (dashed).

3.4.2. Comparing Market Share and Governance Scores

The cross results between Crypto Exchanges' governance scores and Crypto Exchanges' market shares indicate that the major share of the global Crypto Assets Exchanges' market is currently being traded by entities with lower levels of governance (measured with this paper's criteria).

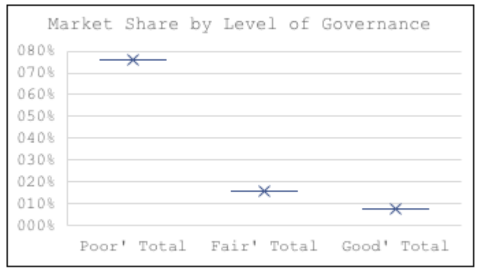


Chart 7: Market Share by Level of Governance

When individual results are observed, as shown in Chart 8, the linear tendency turns into a negative sloped line, indicating a diminished average market share for the highest governance levels (according to this paper's proposed measurement criteria).

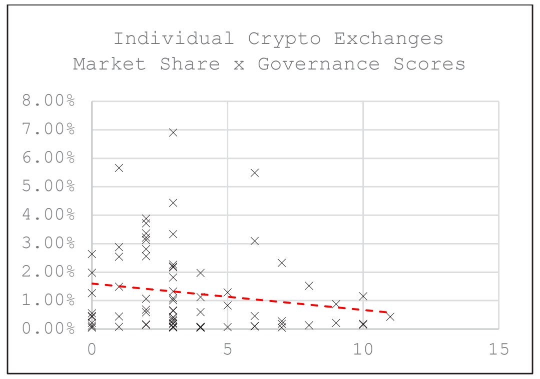


Chart 8: Individual Exchange's Market Share by Score

4. Conclusion

4.1. Summary

The research in this paper identified, from various sources of information, a large number of Crypto Exchanges (517), and from this number, a sample of 78 Crypto Exchanges was categorised and extracted that represents a 99% market share of the global Crypto Assets market, measured by the last 24-hour trading volume for the end of December 2018.

The proposed qualitative criteria applied KPI methodology to measure and compare the governance level of each sample component. The KPI provided an objective governance scale that allowed cross comparison of results with the market share and fees in individual and aggregate terms.

The cross results provided evidence that the majority of today's market share is traded at exchanges with lower levels of governance scores, according to this paper's proposed criteria. Additionally, the results also suggest that the Crypto Exchanges with better governance scores are able to charge higher fees from their customers for better quality services.

4.2. Limitations

Research that utilises a longer time series for the market share data would produce more reliable data. Yet, due to the scope limits of this work, the only plausible data available was for a short 24-hour period offered by coinmarketcap.com portal. Although the reasonably large size of the sample (n = 78) does offer some stability to the set, a more profound study over the matter would certainly demand a wider time series in order to improve the consistency of the results.

The absence of auditing by third parties over the trading volumes remains an important caveat for the Crypto Exchanges, especially for those categorised here as "Regular" Crypto Exchanges, although many exchanges have already adopted third-party audits for its reserves. The challenges associated to traded volume auditing are highlighted by the Canadian Public Accountability Board [10] which reported: *"When crypto-assets are commingled, a crypto-exchange reflects transactions between buyers and sellers of the same crypto-asset in its records but not on the applicable blockchain ledger (i.e., off-chain transactions). This makes it impracticable for auditors to verify the occurrence of an entity's crypto-asset transactions by referring to the applicable blockchain record."* Those practical limitations for independent auditing over reported volumes by Crypto Exchanges might explain why questioning over the actual traded volume is still in place [11].

4.3. Next Steps

Finally, I would like to suggest a possible direction for further studies advancing Crypto Exchanges' governance research:

Advancing on KPI evaluation criteria, the proposed KPI criteria presented in this paper encompasses the most basic levels of governance and compliance. A deeper assessment, including auditing, KYC, AML, data security, trading volumes transparency and other key factors should be added for a better qualitative evaluation of the market components of Crypto Exchange. Additionally, a geographical breakdown that verifies preferences by countries, or global regions, would also contribute to a better understanding of the preferences of crypto investors.

References:

[1] Financial Stability Board - FSB, "Crypto-asset markets - Potential channels for future financial stability implications," FSB Press Releases, Basel, Switzerland, 2018.

[2] J. M. G. a. A. Shams, "Is Bitcoin Really Un-Tethered?," SSRN, p. 66, 13 October 2018.

[3] F. a. Z. K. a. H. M. a. W. M. C. a. S. M. Glaser, "Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions," ECIS 2014 (Tel Aviv), p. 14, 16 April 2014.

[4] K. P. K. R. S.-H. Octavian Nica, "Cryptocurrencies: Concept and Current Market Structure," University of Manchester, FinTech working paper no. 1, p. 66, 25 October 2017.

[5] P. Paech, "The Governance of Blockchain Financial Networks," LSE Legal Studies Working Paper No. 16/2017, p. 45, 30 November 2016.

[6] P. D. F. Aaron Wright, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," Yeshiva University, Université Paris II - Panthéon-Assas, p. 58, 10 March 2015.

[7] J. Lee, "Distributed Ledger Technologies (Blockchain) in Capital Markets: Risk and Governance," School of Law, University of Exeter, p. 25, 29 May 2018.

[8] N. C. B. G. E. a. T. M. Rainer Böhme, "Bitcoin: Economics, Technology, and Governance," Journal of Economic Perspectives, Vol. 29, Issue 2 - Spring 2015, p. 26, 14 September 2014.

[9] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," University College of London - Center for Blockchain Technologies, p. 37, December 2015.

[10] CBBA – Canadian Public Authority Board, "Auditing in The Crypto-Asset Sector", December 2019.

[11] SEC Memorandum – "Bitwise Presentation to the U.S. Securities and Exchange Commission", March, 2019.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
SC would like to thank Prof. Dr. Philipp Sandner at Frankfurt School Blockchain Center.

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(8)2020

Blockchain Governance: What We Can Learn from the Economics of Corporate Governance

Darcy W. E. Allen and Chris Berg
RMIT Blockchain Innovation Hub, RMIT University, Australia
Correspondence: darcy.allen@rmit.edu.au

Received: 20 February 2020 **Accepted:** 16 March 2020 **Published:** 30 March 2020

Abstract

Understanding the complexities of blockchain governance is urgent. The aim of this paper is to draw on other theories of governance to provide insight into the design of blockchain governance mechanisms. We define blockchain governance as the process by which stakeholders (those who are affected by and can affect the network) exercise bargaining powers over the network. Major considerations include the definition of stakeholders, how the consensus mechanism distributes endogenous bargaining power between those stakeholders, the interaction of exogenous governance mechanisms and institutional frameworks, and the needs for bootstrapping networks. We propose that on-chain governance models can only be partially utilised because of the existence of implicit contracts that embed expectations of return among diverse stakeholders.

Keywords: *Blockchain Governance, Institutional Cryptoeconomics, Economics of Blockchain, Corporate Governance*

1. Introduction

Blockchains are decentralised digital network protocols whose governance is characterised by a complex interplay between stakeholders. An incomplete list of these stakeholders includes token holders, network validators (such as Bitcoin's miners and economic full nodes), core and application developers, and founders. Each of these stakeholder groups have a stake in the protocol and each face sharply different incentives when considering whether and how the protocol should be modified. Many other stakeholders don't actively participate in the network but have interests in its structure and modification. These groups include government regulators, activists, media and social media, participants in competing and complementary blockchains, and other parts of the technology stack. The blockchain governance challenge is how to design and build systems that balance the interests of each of these stakeholders and ensure the success of the network, however that success is defined [1].

Social organisations such as corporate firms are made up of individuals that have diverse ends seeking to make exchanges and modify or sustain the environment in which they make those exchanges. They seek to make decisions, implement those decisions, and monitor their implementation and outcomes. These decisions are necessary because not all future states of the world can be identified at the exact moment of organisational formation. Organisations need to adapt to survive [2]. Governance describes the processes by which individuals and groups with ongoing relationships bargain about how to adapt to changes within an institutional environment—such as a firm, a political or community organisation, or in market contracting [3–6].

Whether the institutions of governance have been designed explicitly or not, all blockchains have governance. While those governance systems vary in their effectiveness [7], governance itself is a descriptive, rather than a normative, attribute. Blockchains can be thought of as competing constitutional rule sets, where they compete on rules for making rules [8]. In this way, blockchain governance relates to the way decisions are made, not the decisions themselves—who chooses and how choices are made, rather than what is chosen [9, 10].

Since the whitepaper by Nakamoto [11], which groups should be considered stakeholders in blockchain governance—as well as the formal and informal structures for decision-making—has been highly contested. Owing to their past decisions—such as investing in tokens in the early stages of a network—bargaining power is asymmetric between stakeholders. Stakeholders, and the groups they form, face distinct set of costs in past and future investments in the network—that is, they have made asset-specific investments that constrain future decision-making. On public blockchains such as Bitcoin that allow for open entry and exit (holding and transacting coins, as well as observing the chain and validating new transactions), bargaining power is relevant when modifications to the underlying protocol or core software are proposed. Initial decisions about the governance of the Bitcoin protocol were made by the founder(s) directly or in consultation with a small online community. Later, decisions about protocol modifications to facilitate network scaling were subject to intense bargaining between stakeholder groups—dominated by miners—and led to some uncertainty about the future of the network [a detailed exploration of this scaling debate is provided by 12]. In a user-activated soft fork in 2017, token holders and economic nodes demonstrated that non-mining stakeholders could also exercise bargaining power within Bitcoin's governance structure.

Governance disputes surrounding blockchain protocols have extended beyond Bitcoin (including, for instance, the DAO hack on Ethereum) and have raised important questions on how blockchains should be governed. It is common to distinguish between "on-chain" or "off-chain" governance [see 13, 14, 15]. On-chain governance describes the project of explicitly building governance arrangements within the protocol itself, such as the implementations of EOS, Tezos, and Dash that allow certain categories of stakeholders to vote on modification proposals. Off-chain governance typically describes governance structures external to the protocol, particularly the role and management of foundations or firms funded by token sales or other token distributions (for example, Zcash's Electric Coin Company and Zcash Foundation), or community meeting places such as Reddit, Telegram, Slack, dedicated forums, and Twitter.

In this paper we aim to provide a descriptive framework for understanding blockchain governance, from which we draw some normative implications.

Our goal is to contribute to a deeper understanding that blockchain entrepreneurs can draw from when designing governance systems. "Blockchain" is a generic term for a prominent subclass of distributed ledger technologies, "multi-party systems that operate in an environment with no central operator or authority, despite parties who may be unreliable or malicious"; see Rauchs et al. [16]. We limit our investigation to public blockchains, rather than permissioned or private blockchains (while recognising that the difference between the two is not clear at the margin). While our insights have relevance to permissioned blockchains (including, for instance, defining who should be permissioning), there are some clear differences particularly relating to the definition of stakeholders (and thus control) in permissioned networks, the different needs of bootstrapping, and the problem of forming and governing consortia. We leave these important questions to future research.

We draw on a coherent body of theory around institutional economics—a body of thought structured around the governance of contractual relationships. This body of thought, including transaction cost economics, brings together economics, law, and organisation theory to make the transaction as the basic unit of analysis and includes contributions by Ronald Coase (on why firms exit), James Buchanan (on club goods and constitutional rules), Oliver Williamson (on the economic institutions of capitalism), Oliver Hart (on incomplete contracting and make-or-buy decisions), and Elinor Ostrom (on commons) [17–25]. This coherent body of thought has been applied specifically to blockchain networks through institutional cryptoeconomics [26–30].

While much of the institutional cryptoeconomics has focussed on the effect of blockchain as an institutional technology, in this paper we focus on what institutional economics can teach us about the governance of blockchains themselves. We explore several questions regarding blockchain governance. Who is a stakeholder in blockchain governance? To what extent are blockchain governance systems unique? How can effective long-term blockchain governance be consistent with the needs of bootstrapping—the process of building a blockchain network from the ground up [28]?

We start from corporate governance rather than network governance [31], technology ecosystem governance [32], or nodal governance [33] for two reasons. First, blockchains have algorithmically specified structures that deterministically distribute bargaining power within the network. While this distribution is not hierarchical, as in a firm, neither does it meet traditional understanding of informal reciprocal and social network governance, in that a blockchain network is a domain of formal (smart) contractual exchange. (We discuss the differences between blockchain governance and another network governance—the internet—in Section 5.) Second, attempts by the blockchain industry to design formal on-chain governance systems suggest to us that it is most valuable for researchers to start with the formal governance of the corporation and work their way out from there. At the first instance, a blockchain is a platform for n-sided market contractual exchange [34], around which a technology ecosystem is built.

This paper makes several contributions to the literature on blockchain governance. Blockchain governance is the process by which stakeholders—all those that are affected by and can affect the network—exercise bargaining power over the network itself. This includes token holders, miners, and founders. But blockchains interact with, and are shaped by, external institutional frameworks, such as the firms that act as institutional investors for tokens or other organisations up and down the stack, the firms that provide exchange services, and government regulators who impose requirements (such as know-your-customer and anti-money laundering regulations) on the on-ramps to the network. We draw on the literature on corporate governance with a focus on implicit and explicit contracts, and how management and governance deals with those complexities.

We introduce three distinct elements that shape our understanding of blockchain governance: endogenous governance, exogenous governance, and the need for bootstrapping. We offer a new distinction between the distribution of bargaining power endogenous to the consensus mechanism and the exogenous governance structures that are built on top. Endogenous governance describes the bargaining power that is directly derived from instrumental features of the consensus mechanism. That is, elements of the protocol that are minimally necessary for achieving consensus. In a proof-of-work protocol like Bitcoin, bargaining power is determined by the instrumental roles of miners and full economic nodes. Endogenous governance is the distribution of power between stakeholders directly involved in the consensus mechanism. We also discuss the needs of bootstrapping in the early stages of the network and how this affects the distribution of bargaining power. These elements provide, sometimes, contradictory pressures towards and against decentralisation.

2. Who is a stakeholder in blockchain governance?

Blockchain governance faces a boundary problem. Before we can determine how a governance mechanism is structured, we need to define the boundaries of who is doing the governing—that is, who are the stakeholders. Whether a blockchain governance system is implicit (that is, the allocation of bargaining power comes from the instrumental design of the consensus mechanism) or planned (where the protocol has been designed specifically with a governance mechanism in mind), we need some guidance about which stakeholders are analytically relevant for the assessment and design of governance mechanisms.

We can look to our understanding of how we define corporations and their governance—from the responsibility to deliver profit to broader conceptions of corporate social responsibility—to understand stakeholders in blockchains. Milton Friedman [35] famously wrote that the sole responsibility of a firm is to generate profits to its shareholders. A formal model of this describes the firm as a nexus of contracts between investors, managers, and their subordinates, where the residual income accrues to shareholders [25, 36]. Thus, corporate governance under this framework describes the process by which shareholders ensure that profits for their investments are returned—that managers do not abscond with money already invested [37].

The transaction cost approach to the firm emphasises how the inevitably incomplete contracts that make up firms shape institutional choices [21, 22]. This tradition of framework can be described as a contracting-first approach to corporate governance, and pivots around the ownership and use of property rights in the organisation.

The corporate social responsibility movement has challenged the shareholder-first framework [38], arguing that a wider variety of groups and interests should be taken into consideration by the management. Rather than being simply responsible towards shareholders, firms ought to be responsible towards "stakeholders." In many ways, corporate social responsibility is the process of stakeholder management [39]. But as Janita Vos [40] asks, who is a stakeholder? A stakeholder can be any group or individual who can affect the governance or an operation of an organisation or is affected by it [41, 42]. The first true list of stakeholders for the management was that attributed to the vision of General Electric in 1931: shareholders, employees, customers, and the general public [43, 44]. But other groups could, of course, be affected, or could affect the organisation.

Governance discussions around blockchains have typically narrowly defined the categories of a stakeholder, either implicitly or explicitly. Disputes around the scaling of Bitcoin, for instance, have sometimes been seen as a narrow bilateral dispute between Bitcoin core developers—those who work on the reference implementation of the Bitcoin software—and miners who validate the chain and compete to mint new tokens [45, 46]. Explicitly designed governance mechanisms are likewise constrained. EOS and Tezos, two blockchain protocols with such explicit governance, give token holders voting rights over delegated validators and modification proposals, respectively. But token holders are not the only potential stakeholders who might be affected (and can affect) governance decisions. It is worth noting that in EOS and Tezos, validators and core developers are not explicitly identified as stakeholders for formal on-chain governance except insofar they may also hold tokens (whether to maintain a stake in the system or as part of receiving and disposing of block rewards). In this way, different stakeholder groups may be highly correlated.

We can identify a wide range of separate stakeholder groups. Even in Bitcoin, token holders are not a homogenous group. Governance analysis might distinguish between token holders who intend to use their holdings primarily as a medium of exchange, and those who are holding them as speculative assets (HODLers). Founders and founding foundations can affect the decisions of the protocol. Developers can be divided into core developers (with or without repo access) and developers who are building applications that use the protocol as an infrastructure layer. Economic full nodes, such as large, over-the-counter traders, token holders, and miners can have distinct stakeholder interests. The producers of hardware that support the chain (ASIC or GPU producers, cold storage wallets, etc.) are also stakeholders.

We can expand the stakeholder groups further when considering individuals or groups who are affected by the blockchain but do not directly interact with it. Bitcoin provides a medium of exchange and unit of account for holders of other cryptocurrency tokens. A typical exchange denominates cryptocurrency in units of Bitcoin. Initial coin offerings on EC20 tokens typically involve an initial acquisition of the Ethereum token, Ether. Bitcoin and Ethereum stakeholders can be said to have the power to affect holders of other cryptocurrencies. In this sense, the financial system itself can affect cryptocurrencies through its interaction with blockchain on-ramps (exchanges, payment networks, etc.) or through competition or even simply through the price level. Furthermore, industries which are disrupted by specific blockchain (supply chains, logistics, data science, health, etc.) might also be said to be stakeholders. Government authorities that have regulatory responsibility for fields in which blockchain applications operate are also stakeholders. In some circumstances, social groups can be described as stakeholders. The significant electricity use of proof-of-work consensus mechanisms, and its potential impact on the global energy use, means that environmentalists, of their representative non-government organisations, could be stakeholders, insofar as they are affected by the operation of the protocol.

Given the potentially wide range of stakeholders, and the complexities in identifying them, which groups should be considered stakeholders while maintaining workable governance structures? Too many stakeholders exercising control rights over an organisation can privilege the interests of groups with little stake above those who are most directly affected, or alternatively, where delegation has been given to authorities to weigh interests, allowing managers to hide self-interested behaviour [47]. Responding to this challenge, the corporate social responsibility tradition has sought to distinguish between different groups of stakeholders. Fassin [48] and Fassin [49] propose a division between "real" stakeholders, whose influence over the firm is the organisation (insofar as they have control rights over the organisation, the organisation has control rights over them), "stakewatchers," who represent the interests of real stakeholders (such as unions, consumer groups, environmental groups, and investor associations), and "statekeepers," who have no stake in the firm but impose constraints (such as government agencies and regulators).

By contrast, the contract approach structures its answer to who is a stakeholder around property rights as residual rights to income [36] or residual control rights [50]. In this approach, stakeholders are "all investors who create transaction- and/or firm-specific property under the reasonable expectation of a return on investment through interaction with the firm" [51]. Here, the legitimate group of stakeholders encompasses those who have both explicit and implicit contracts with the firm. Explicit contracts are those contracts not directly stated but understood by both parties for the contract to exist. Implicit contracts recognise the existence of the co-creation of value and the expectation of a real return for such investments. Such informal quid pro quos are pervasive within the firm, and even explicit contracts are hard to navigate without some understanding of the implicit agreements that underpin them [52, 53]. Incorporating this understanding of implicit contracts for the co-production of economic value considerably narrows the otherwise infinite space of stakeholders.

Implicit contracts are contracts which are obscure to outside observers. Indeed, because implicit contracts are not written down and are based in norm rather than a clear agreement, they obscure the ultimate economic value of an organisation and the search for general principles that might apply across organisations. In a firm, some "outputs"—such as the training of employees—are neither priced nor explicitly documented.

Implicit contracts exist in blockchain networks, most obviously through the roles played by founders, foundations, and developers. But in a firm, it is the job of the management to weigh and balance the implicit contracts [54, 55]. Stakeholders can implore the management to weigh their interests more heavily, and penalise the firm through (a) reputation loss and (b) a choice not to make further investments if they are not satisfied. Firm managers have the discretion to distribute income to stakeholder groups, identifying and responding to implicit contracts as necessary. They are constrained from doing so in their interests to the extent that the explicit contracts with shareholders prevent such opportunistic behaviour [47]. By design, decentralised organisations have no "management." No single class of stakeholder is empowered to coordinate implicit contracts. This obviously protects against a category of rent-seeking behaviour caused by agency losses between the owners and the management. But it leaves uncertainty as to how the distribution of value-derived implicit contracts can be negotiated between stakeholders.

3. Endogenous and exogenous governance

In this section, we examine the mechanisms through which governance decisions over implicit and explicit contracts are made. We distinguish between two forms of governance of blockchain networks: endogenous and exogenous. Blockchains have endogenous governance systems that create the relative bargaining power instrumentally determined by the consensus mechanism. We argue that the initial design of a blockchain consensus protocol maps to a different distribution of bargaining power over the network itself. Furthermore, blockchains also have exogenous governance systems that are the formal and informal governance processes that exist outside of the instrumental needs of distributed consensus over the state of the ledger. Our analysis is distinct from the endogenous-exogenous split presented by de Filippi and Mcmullen [56] because it pivots on whether governance is determined by the consensus mechanism, which Rauchs et al. [16] describe as the characteristic that makes distributed ledger systems unique.

The distribution of bargaining power over blockchain governance, at the first instance, is *endogenously governed* by the consensus mechanism. Bitcoin is a three-sided market between miners, buyers, and sellers [34]. The dominant players are economic full nodes—those who keep a complete copy of the chain, broadcast transactions, and validate the shared ledger [57, 58]. Their decision of whether to adopt software amendments produced by core developers depends on whether they believe that other economic full nodes will accept new blocks produced by the software. In other words, it is the economic full nodes that enforce the rules. Their ability to accept or reject blocks following different rules gives them endogenous bargaining power and, therefore, the governance control over the network. How precisely this distribution manifests itself in decisions depends, of course, on the interests of the economic full nodes as individual agents, but structurally the consensus mechanism gives them the governing power over the network.

Our focus here is not on whether blockchains have designed or not designed governance processes, or between blockchains with or without governance. Rather, we emphasise that the structure of the consensus protocol determines the bargaining power. Stakeholders in endogenous governance have been given formal bargaining power over the network by the design of the consensus protocol. A parallel here is with the formal institutions of a firm—shareholders, management, and employees—that forms the "machine" for profit-seeking economic activity. Endogenous governance can be intentionally designed. While Bitcoin was built without governance in mind, in EOS a "governance" system has been built into the consensus mechanism which allows token holders to vote for block validators. This produces an alternative distribution of bargaining power, where token holders (and their proxies) exercise a significant amount of power (relative to the Bitcoin network).

By contrast, *exogenous governance* describes the formal and informal governance processes that exist outside the instrumental needs of distributed consensus over the state of the ledger. These can be formally designed or evolved in response to a perceived need for legitimacy. Exogenous governance can be "on-chain" or "off-chain", "formal" or "informal," as described by Buterin [59], Buterin [60], Zamfir [61], and Ehrsam [62]. At Coindesk's Consensus conference in 2017, an agreement (the "New York Agreement") was brokered between 56 separate mining and Bitcoin application firms for two modifications of the protocol: segregated witness and larger block sizes [63]. The exogenous governance mechanism here is provided by the opportunity for coordination presented by the Consensus conference itself. De Filippi and Loveluck [1] describe this process as the "invisible politics" of Bitcoin. In the wake of the hack of The DAO, a voting mechanism was created to vote on whether to hard fork Ethereum to reverse the hack. The hard fork was triggered in July 2016. On-chain mechanisms for voting on protocol modifications (such as the ones offered in EOS, Tezos, and Dash) are exogenous insofar as they do not form an instrumental part of the consensus function.

Endogenous and exogenous governance mechanisms co-exist, providing mutual restraints against each other. Where governance has been explicitly designed, it is still subject to endogenous governance processes. The creation of Ethereum Classic after The DAO hard fork underlines the persistence of endogenous bargaining power after the creation of exogenous governance, albeit with the result being a split in the network. In EOS, the delegated proof-of-stake consensus mechanism allows token holders to vote for validators (block producers), and also to vote on decisions about the protocol (referendum proposals). The distribution of bargaining power determined by the former voting system is endogenous and the latter exogenous. Both endogenous and exogenous governance processes are subject to evolutionary pressure as technical developments (such as ASICs) and entrepreneurial innovation (such as mining pools) reshape the relative bargaining power of stakeholder groups [8, 64].

We can see here how the co-existence of implicit contracts between diverse stakeholders and blockchain governance systems creates challenges. Implicit contracts in decentralised systems have to be constantly negotiated, in the same way that corporate culture as a tool for the negotiation of implicit contracts is subject to constant evolution and evaluation. Particular on-chain exogenous governance systems that provide a formal mechanism for token holders (weighted by token holdings) to vote on protocol-level changes elide these complex multi-party negotiations by identifying a singular distinct category of stakeholders whose preferences are most convenient to collate.

4. Governance and the needs of bootstrapping

The distribution of bargaining power of endogenous governance is set instrumentally by the consensus mechanism. The domains of exogenous governance, on the other hand, is more diverse. Exogenous governance can be built into the protocol as a referendum process (as in EOS and Tezos) or revolve around over the norms and cultural structures of the community of users. Those norms and cultures vary significantly [65] and determine whether exogenous governance decisions are seen as legitimate by all stakeholders.

One obvious illustration of the role of legitimacy around exogenous governance norms is the governance role of Satoshi Nakamoto in the early days of Bitcoin, and the subsequent function played by the Bitcoin Foundation. Satoshi's "vision," as outlined in the Bitcoin whitepaper [11] and subsequent mailing list and forum posts, has played an outsized role in shaping governance choices over the network. Likewise, core developers have a governance role that does not simply reflect their instrumental function within the consensus mechanism. In parallel to democratic governance, some exogenous governance mechanisms rely on leaders and key players to provide guidance and heuristics for people to make decisions about blockchain governance. Some relatively informal exogenous governance mechanisms—such as leaders and early adopters—might ameliorate the costs of making more formal governance decisions.

A fruitful but extensive task would be to audit blockchain communities looking for commonalities in these norms and cultures [one early attempt to do so is 10]. Here, however, we start from the question: how do those norms evolve? There is at least one consistent feature of all blockchain networks. They must start from somewhere. They must all be bootstrapped.

Blockchain protocols are the result of entrepreneurial creative discovery [66]. They come from specific environments—from the mind of entrepreneurs and their relationship with other idea producers. In this Kirznerian tradition, Allen [67] and Potts [68] explore how ideas are governed as they are combined and recombed in the proto-entrepreneurial stage. To bring ideas to market, organisational structures are created so that the property rights over those ideas can be allocated [27, 69]. The organisational creation need not be a firm. It can be as simple as writing a white paper that describes the protocol for a new business model, marking that code as open source, and posting it on a websit. Alternatively, many blockchain networks have undertaken initial coin offerings that have raised substantial funds for development and to subsidise development work within their communities [29, 70-72]. For blockchain networks, these two stages—the proto-entrepreneurial and the organisational—leave their mark on the later governance and shape the distribution of bargaining power by later stakeholders.

Blockchains are not born decentralised. Catalini and Gans [28] describe Bitcoin as the first digital platform to be bootstrapped without the need for investment from a planner or other intermediaries. But bootstrapping still requires work. Whether Satoshi was an individual or group of individuals, specific individuals had to design the software and write the Bitcoin white paper. New innovations need hype to facilitate early-stage cooperation, and the hype is an economic good that has to be produced [73]. Even if Bitcoin emerged fully formed from the mind of a single "Satoshi Nakamoto," in the early stages of Bitcoin, decisions as to the design of the protocol were negotiated between different stakeholders through Bitcoin talk forums, newsgroups, and email lists. One prominent picture of the governance of Bitcoin around the needs of bootstrapping is the December 2010 debate of whether Wikileaks should be encouraged to use Bitcoin for donations, which was at the time resolved in favour of an appeal from Satoshi to Wikileaks not to adopt the fledgling cryptocurrency [74, 75].

The process of bootstrapping exerts an influence on the norms around governance and the implicit contracts that are negotiated long after an initial bootstrapping phase. For example, De Filippi and Loveluck [1] describe a belief implicit in Bitcoin governance processes that "the Bitcoin core developers (together with a small number of technical experts) are—by virtue of their technical expertise—the most likely to come up with the right decision as to the specific set of technical features that should be implemented in the platform." Recent work on the economics of corporate

culture underpins the role that culture plays in coordinating expectations between the management and the employees who have made specific investments in the firm [76–78]. We can understand these relationships within the network as subject to implicit contracts that enhance the network's economic value.

These implicit contracts have a clear origin—the entrepreneurial creation of the protocol and the need for bootstrapping a network—but by their nature are hard to be pinned down with any formality and are highly contextual. They explain the role played by Satoshi in Bitcoin's early days, and the shifts in governance since Satoshi's disappearance. Disputes over the Satoshi legacy and the increasing contestability of the role of the Bitcoin core developers are a form of renegotiation of this implicit contract. Satoshi's absence from the Bitcoin community since December 2010 is an unusual case. Founders and their founding organisations play a key role in the creation and bootstrapping processes. Their structural roles (for instance, as core developers or block validators) and the implicit contracts that have been built around them tend to be controversial. Examples include the role of Vitalik Buterin and the Ethereum Foundation, the position of Block.One as the developers of the EOS network, and the Zcash founders' reward. These founders and organisations do not have any endogenous role in blockchain governance as determined by the consensus mechanism. But their role as exogenously determined stakeholders and the implicit contracts that support that role create a dilemma for blockchain governance, given political beliefs about decentralisation within many blockchain communities.

5. The ends of blockchain governance

Corporations are treated in law as intentional systems [79, 80]—that is, corporations are an entity, even a moral entity, in and of themselves. Alchian and Demsetz [36] argue that firms are units of team production, where the possibility of teamwork is limited by the costs of disciplining/shirking—that is, corporations are the aggregation of a nexus of contracts [81]. These views are typically seen as contrasting [82] but each imputes to the corporation a particular—if not quite a singular—purpose. While each contractor to the firm (employee, management, and shareholder) seeks their own ends, the team is organised in the pursuit of a singular end. The governance of a firm consists in coordinating around that singular end, whether it is profit-maximisation in the Friedman sense or ends determined by an assessment of the corporation's social responsibilities.

So, what are the ends of blockchain governance? An implicit end common to the blockchain community is that the network survives—that is, it maintains its immutability through distributed consensus while accepting new transactions—and is adopted more widely. The Bitcoin governance crisis described by De Filippi and Loveluck [1] concerned these two ends. Of course, the ends of different categories of stakeholder groups are heterogeneous between and within those categories. Token holders who hold tokens as an investment might want the value of their holdings to increase relative to fiat currency, while application developers who wish to use tokens as a utility in their applications often want price stability. While each stakeholder group shares a distributed network, they pursue different final ends.

These stakeholders use blockchain as a shared economic resource with which they pursue different ends—that is, blockchain is an infrastructure [83]. Frischmann [84] offers a set of characteristics that make a resource infrastructural: its consumption is non-rivalrous within certain demand bounds, its demand is a function of downstream production, and it is an input into a wide array of goods and services. A given blockchain offers generic public capabilities that allow for diverse productive ends to be pursued. The shared interest is in the maintenance of that infrastructure and its increased utility of the infrastructure, which exploits possible network effects.

We might compare blockchain governance then with internet governance, another shared digital infrastructure. The United Nations Working Group on Internet Governance [85] describes governance as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet." Nonetheless, as Van Eeten and Mueller [86] note, debates over internet governance have tended to focus disproportionately on a small number of formal institutions and quasi-government stakeholders (such as the Internet Corporation for Assigned Names and Numbers) while downplaying the role of (for instance) internet service providers, telecommunications regulators, operating system developers, and mobile phone device manufacturers who fit within that definition.

Likewise, using the expansive approach to stakeholder identification described in Section 2, the active participants in exogenous blockchain governance include stakeholders all the way through the stack, from the telecommunications providers who host the distributed network, the GPU and ASIC manufacturers who produce mining equipment, application developers, chains launching their native tokens on other chains, venture capital firms investing in application developments, to government standard bodies and financial sector regulatory agencies. Importantly, these governance stakeholders do not all share the same ends—not all of them have the shared interest in the maintenance and increased utility of the blockchain—yet all can exercise a degree of control about the future of the blockchain network. The parallel between internet governance and blockchain governance should encourage researchers to cast their net wide for stakeholder identification.

Nonetheless, the differences between internet governance and blockchain governance are substantial and relevant. Putting aside possible balkanisation of the internet [87], the internet is a singular shared protocol. By contrast, there are many competing blockchain protocols. They compete on different margins and evolve and fork at different speeds. Furthermore, the use of one blockchain does not preclude the use of others, partly because they each operate on internet infrastructure.

A more fundamental difference between the internet and blockchain governance is the role that blockchain tokens play in coordinating maintenance of the network. Tokens align incentives by endogenising the capital formation necessary for bootstrapping [28]. While the internet has a variety of institutional governance frameworks—such as corporate, government, and commons [84]—blockchains can be understood as a self-contained institutional technology [27]. Yet the managers of corporations are constrained by fiduciary duties specified in law that require them to act both in the interest of shareholders and the company. As an institutional innovation, stakeholders in blockchains lack these legal constraints. Neither token holders, miners, nor full economic nodes are required to act in others' interests. To the extent that they do, it is because the consensus mechanism and native token coordinate self-interested behaviour to maintain and protect the network.

6. Conclusion

In this paper we have drawn on the theory of corporate governance to better understand the complexities of blockchain governance. We have offered insights into defining stakeholders, the distribution of bargaining power endogenous to the consensus mechanism, the role of exogenous governance structures, and the need to bootstrap networks.

While we have aimed to be descriptive here, our analysis has normative implications. Current on-chain governance models can only be partial because of the existence of implicit contracts that embed expectations of return among diverse stakeholders. Alternatively put, governance can be on-chain to the extent that control rights can be made explicit. Implicit contracts are unavoidable in public blockchains, given the open, repeated interactions between participants in the n-sided market and technology ecosystem and the entrepreneurial needs of network bootstrapping. Protocols concerned with blockchain governance ought to frame their thinking around the need to recognise the coordinating of consensus around the existence and persistence of these implicit contracts.

These considerations raise a further research agenda on blockchain governance. The blockchain industry lacks an extensive understanding of governance that corporate governance relies upon, and which in turn informs regulatory policy. Yet regulatory dilemmas around whether tokens represent ownership in a network (that is, are tokens shares) or where control over a network is vested (which speaks to the OECD's [88] concern with tacit collusion on blockchain networks) are already on-going. The proposal by Pierce [89] for a regulatory safe harbour that allows a bootstrapped network to be decentralised will pivot on better understanding than we have now of what constitutes decentralisation of control. A deeper understanding of how the interaction between bootstrapping and decentralised consensus has evolved will offer a guide for blockchain developers who seek to achieve long-run decentralisation.

References:

[1] P. De Filippi and B. Loveluck, "The invisible politics of bitcoin: governance crisis of a decentralized infrastructure," Internet Policy Review, vol. 5, no. 3, 2016.
[2] P. G. Klein, J. T. Mahoney, A. M. McGahan, and C. N. Pitelis, "Organizational governance adaptation: Who is in, who is out, and who gets what," Academy of Management Review, vol. 44, no. 1, pp. 6–27, 2019.
[3] O. E. Williamson, The Mechanisms of Governance. Oxford University Press, 1999.
[4] O. E. Williamson, "The institutions of governance," The American Economic Review, vol. 88, no. 2, pp. 75–79, 1998.
[5] D. C. North, "Institutions," Journal of Economic Perspectives, vol. 5, no. 1, pp. 97–112, 1991.
[6] O. E. Williamson, "The theory of the firm as governance structure: from choice to contract," Journal of Economic Perspectives, vol. 16, no. 3, pp. 171–195, 2002.
[7] K. Yeung and D. Galindo, "Why do public blockchains need formal and effective internal governance mechanisms?," European Journal of Risk Regulation, vol. 10, no. 2, pp. 359–375, 2019.
[8] E. Alston, "Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets," Center for Growth and Opportunity at Utah State University Working Paper Series, vol. 3, 2019.
[9] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
[10] Y.-Y. Hsieh, J.-P. Vergne, and S. Wang, "The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies," in Bitcoin and Beyond: Blockchains and Global Governance, vol. 48–68, M. Campbell-Verduyn, Ed. London and New York: Routledge, 2018.
[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[12] R. Nyffenegger, "Scaling Bitcoin," Master's, Universität Basel, 2018.
[13] W. Reijers et al., "Now the code runs itself: On-chain and off-chain governance of blockchain technologies," Topoi, pp. 1–11, 2018.
[14] P. Honkanen, M. Westerlund, and M. Nylund, "Governance in Decentralized Ecosystems," CLOUD COMPUTING 2019, p. 59, 2019.
[15] L. Mosley, H. Pham, and Y. Bansal, "Towards a Systematic Understanding of Blockchain Governance in Proposal Voting: A Dash Case Study," Available at SSRN 3416564, 2019.
[16] M. Rauchs et al., "Distributed Ledger Technology Systems: A Conceptual Framework," SSRN, 2018.
[17] R. H. Coase, "The Nature of the Firm," Economica, vol. 4, no. 16, pp. 386–405, 1937.
[18] J. M. Buchanan and G. Tullock, The Calculus of Consent. Ann Arbor: University of Michigan Press 1962.
[19] J. M. Buchanan, "An Economic Theory of Clubs," Economica, vol. 32, no. 125, pp. 1–14, 1965.
[20] O. D. Hart, Firms, Contracts, and Financial Structure. Oxford and New York: Clarendon Press, 1995.
[21] O. D. Hart, "Incomplete Contracts and the Theory of the Firm," Journal of Law, Economics, & Organization, vol. 4, no. 1, pp. 119–139, 1988.
[22] O. E. Williamson, The Economic Institutions of Capitalism. NY: Free Press, 1985.
[23] E. Ostrom, Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge: Cambridge University Press, 1990.
[24] J. R. Commons, "Institutional economics," The American Economic Review, pp. 648–657, 1931.
[25] R. H. Coase, "The problem of social cost," The Journal of Law and Economics, vol. 56, no. 4, pp. 837–877, 1960.
[26] 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, 2018.
[27] C. Berg, S. Davidson, and J. Potts, Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics. Edward Elgar Publishing, 2019.
[28] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," National Bureau of Economic Research, 2016.
[29] D. W. E. Allen, C. Berg, B. Markey-Towler, M. Novak, and J. Potts, "Blockchain and the Evolution of Institutional Technologies: Implications for Innovation Policy," Research Policy, 7 August 2019.
[30] 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 Journal of the British Blockchain Association, vol. 2, no. 1, pp. 57–65, 2019.
[31] W. W. Powell, "Neither Market Nor Hierarchy: Network forms of organization," Research in Organizational Behavior, vol. 12, pp. 295–336, 1990.
[32] J. Wareham, P. B. Fox, and J. L. Cano Giner, "Technology ecosystem governance," Organization science, vol. 25, no. 4, pp. 1195–1215, 2014.
[33] S. Burris, P. Drahos, and C. Shearing, "Nodal governance," Australian Journal of Legal Philosophy, vol. 30, p. 30, 2005.
[34] C. Berg, S. Davidson, and J. Potts, "Proof of work as a three-sided market," Frontiers in Blockchain, 31 January 2020.
[35] M. Friedman, "The social responsibility of business is to increase its profits," in New York Times Magazine, ed, 1970.
[36] A. A. Alchian and H. Demsetz, "Production, Information Costs, and Economic Organization," The American Economic Review, vol. 62, no. 5, pp. 777–795, 1972.
[37] A. Shleifer and R. W. Vishny, "A Survey of Corporate Governance," The Journal of Finance, vol. 52, no. 2, pp. 737–783, 1997.
[38] H. R. Bowen, Social Responsibilities of the Businessman. University of Iowa Press, 1953.
[39] T. Donaldson and L. E. Preston, "The stakeholder theory of the corporation: Concepts, evidence, and implications," Academy of management Review, vol. 20, no. 1, pp. 65–91, 1995.
[40] J. F. Vos, "Corporate social responsibility and the identification of stakeholders," Corporate Social Responsibility and Environmental Management, vol. 10, no. 3, pp. 141–152, 2003.
[41] R. E. Freeman, Strategic Management: A Stakeholder Approach. Pitman, 1984.
[42] M. E. Clarkson, "A stakeholder framework for analyzing and evaluating corporate social performance," Academy of management review, vol. 20, no. 1, pp. 92–117, 1995.
[43] E. M. Dodd Jr, "For whom are corporate managers trustees," Harv. L. Rev., vol. 45, p. 1145, 1931.
[44] L. E. Preston and H. J. Sapienza, "Stakeholder management and corporate performance," Journal of behavioral Economics, vol. 19, no. 4, pp. 361–375, 1990.
[45] S. DiRose and M. Mansouri, "Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations," in 2018 13th Annual Conference on System of Systems Engineering (SoSE), 2018, pp. 195–202: IEEE.
[46] N. Carter, "A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors," 2016.
[47] M. J. Roe, "The shareholder wealth maximization norm and industrial organization," University of Pennsylvania Law Review, vol. 149, p. 2063, 2000.
[48] Y. Fassin, "A dynamic perspective in Freeman's stakeholder model," Journal of Business Ethics, vol. 96, no. 1, p. 39, 2010.

[49] Y. Fassin, "The stakeholder model refined," Journal of Business Ethics, vol. 84, no. 1, pp. 113–135, 2009.
[50] S. J. Grossman and O. D. Hart, "The costs and benefits of ownership: A theory of vertical and lateral integration," Journal of Political Economy, vol. 94, no. 4, pp. 691–719, 1986.
[51] P. G. Klein, J. T. Mahoney, A. M. McGahan, and C. N. Pitelis, "Who is in charge? A property rights perspective on stakeholder governance," Strategic Organization, vol. 10, no. 3, pp. 304–315, 2012.
[52] G. Baker, R. Gibbons, and K. J. Murphy, "Relational contracts and the theory of the firm," The Quarterly Journal of Economics, vol. 117, no. 1, pp. 39–84, 2002.
[53] C. I. Barnard, The Functions of the Executive. Harvard University Press, 1938.
[54] J. S. Harrison, D. A. Bosse, and R. A. Phillips, "Managing for stakeholders, stakeholder utility functions, and competitive advantage," Strategic management journal, vol. 31, no. 1, pp. 58–74, 2010.
[55] C. Eesley and M. J. Lenox, "Firm responses to secondary stakeholder action," Strategic Management Journal, vol. 27, no. 8, pp. 765–781, 2006.
[56] P. de Filippi and G. Mcmullen, "Governance of blockchain systems: Governance of and by Distributed Infrastructure," Blockchain Research Institute and COALA, 2018.
[57] J. Song, "Bitcoin, UASF and Skin in the Game," in Medium, ed, 2017.
[58] E. G. Sirer, "Time for Bitcoin Users to Reclaim Their Voice," ed, 2016.
[59] V. Buterin, "Governance, Part 2: Plutocracy Is Still Bad," in Vitalik Buterin's website, ed, 2018.
[60] V. Buterin, "Notes on Blockchain Governance," in Vitalik Buterin's website, ed, 2017.
[61] V. Zamfir, "Against on-chain governance," in Medium, ed, 2017.
[62] F. Ehrsam, "Blockchain Governance: Programming Our Future," in Medium, ed, 2017.
[63] Digital Currency Group, "Bitcoin Scaling Agreement at Consensus 2017," 23 May 2017, Available: https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77.
[64] A. Berg, C. Berg, and M. Novak, "Blockchains and constitutional catallaxy," Constitutional Political Economy, forthcoming.
[65] M. Prewitt and S. McKie, "Blockchain communities and their emergent governance," in Amentum blog, ed: Medium, 2018.
[66] I. M. Kirzner, Discovery and the Capitalist Process. University of Chicago Press, 1985.
[67] D. W. E. Allen, "The Private Governance of Entrepreneurship: An Institutional Approach to Entrepreneurial Discovery," PhD (Economics), School of Economics, Finance and Marketing, RMIT University, Melbourne, 2017.
[68] J. Potts, Innovation Commons: The Origin of Economic Growth. Oxford University Press, 2019.
[69] K. Dopfer and J. Potts, The general theory of economic evolution. Routledge, 2015.
[70] Y. Chen, "Blockchain tokens and the potential democratization of entrepreneurship and innovation," Business horizons, vol. 61, no. 4, pp. 567–575, 2018.
[71] J. M. Woodside, F. K. Augustine Jr, and W. Giberson, "Blockchain technology adoption status and strategies," Journal of International Technology and Information Management, vol. 26, no. 2, pp. 65–93, 2017.
[72] D. W. E. Allen, "Governing the Entrepreneurial Discovery of Blockchain Applications," Journal of Entrepreneurship and Public Policy, forthcoming.
[73] J. Potts, "Hype as a public good for innovation," Available at SSRN 2934675, 2017.
[74] J. Assange, When Google Met Wikileaks. OR Books, 2016.
[75] S. Nakamoto. (2010). Re: Wikileaks contact info? Available: https://bitcointalk.org/index.php?topic=1735.msg26999#msg26999
[76] D. M. Kreps, "Corporate culture and economic theory," in Firms, Organizations and Contracts, Oxford University Press, Oxford, J. E. Alt and K. A. Shepsle, Eds., 1996, pp. 221–275.
[77] J. Jeffers and M. Lee, "Corporate Culture as an Implicit Contract," presented at the ASSA Annual Meeting, Atlanta, Georgia, 5 January 2019. Available: https://www.aeaweb.org/conference/2019/preliminary/902?q=eNqrVipOLS7OzM8LqSxIVbKqhnGVrJQMlWp1lBKLi_OTgRwlHaWS1KJcXAirLDO1HKQ2JbUkMTNcJzUFrFhHqaigXDDEMlwwAZDelMRKqM7M3FQQqxZcMIhcIiBv
[78] C. Camerer and A. Vepsalainen, "The economic efficiency of corporate culture," Strategic Management Journal, vol. 9, no. S1, pp. 115–126, 1988.
[79] P. A. French, "The corporation as a moral person," American Philosophical Quarterly, vol. 16, no. 3, pp. 207–215, 1979.
[80] W. G. Weaver, "Corporations as intentional systems," Journal of Business Ethics, vol. 17, no. 1, pp. 87–97, 1998.
[81] M. C. Jensen and W. H. Meckling, "Theory of the firm: Managerial behavior, agency costs and ownership structure," Journal of financial economics, vol. 3, no. 4, pp. 305–360, 1976.
[82] G. G. Sollars, "The corporation: Genesis, identity, agency," in The Routledge Companion to Business Ethics: Routledge, 2018, pp. 239–256.
[83] C. Berg, S. Davidson, and J. Potts, "Blockchain technology as economic infrastructure: Revisiting the electronic markets hypothesis," Frontiers in Blockchain, vol. 2, p. 22, 2019.
[84] B. M. Frischmann, Infrastructure: The Social Value of Shared Resources. Oxford University Press, USA, 2012.
[85] United Nations Working Group on Internet Governance, "Report of the Working Group on Internet Governance," United Nations, June 2005, Available: http://www.wgig.org/docs/WGIGREPORT.pdf.
[86] M. J. Van Eeten and M. Mueller, "Where is the governance in Internet governance?," New media & society, vol. 15, no. 5, pp. 720–736, 2013.
[87] M. Mueller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. Wiley, 2017.
[88] Organisation for Economic Co-operation and Development, "Blockchain Technology and Competition Policy – Issues paper by the Secretariat," 8 June 2018, Available: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf.
[89] H. M. Pierce, "Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization," Chicago, Illinois, 2020.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
DA and CB designed and wrote the manuscript jointly and in its entirety.

Funding:
None declared.

Acknowledgements:
The authors would like to acknowledge participants at the Wharton Cryptogovernance Workshop (July 2019) and the British Blockchain Association's International Scientific Conference (March 2020).

PEER-REVIEWED RESEARCH

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

What is in It for Me? Identifying Drivers of Blockchain Acceptance among German Consumers

Florian O. Knauer and Andreas Mann
Institute of Management and Business Studies, University of Kassel, Germany
Correspondence: knauer@wirtschaft.uni-kassel.de

Received: 17 July 2019 **Accepted:** 11 September 2019 **Published:** 8 October 2019

Abstract

From a consumers' perspective, Blockchain Technology (BCT) holds the potential to decrease transaction costs, improve privacy and redesign social interactions, which potentially leads to enhanced consumer power in transactional relationships. Nevertheless, only a few consumers use Blockchain-based applications consciously. By combining earlier research about BCT acceptance with different conceptualisations in the technology acceptance field (i.e. the Technology Acceptance Model and Rogers' Diffusion Theory), a Blockchain-specific model to explain the usage intention has been developed and validated by conducting an online survey among 157 German consumers. While most of them have recognised the technology's existence and confirmed its general relevance, many consumers do not know how to access and profit from BCT. Integrating the results of a Structural Equation Model and Pairwise Comparisons between typical attributes of Blockchain-based applications, specific beliefs about BCT usage are found to have a remarkable impact on consumers' acceptance. Based on the results, strategies to promote the acceptance of BCT among consumers are discussed from a marketer's, developer's and researcher's point of view.

Keywords: *Blockchain, Distributed Ledger Technology, Technology Acceptance, Technology Diffusion, Consumer, Germany*

1. Introduction

More than ten years after Satoshi Nakamoto (pseudonym) released his More than ten years after Satoshi Nakamoto (pseudonym) released his famous white paper [1] leading the way for the Bitcoin Blockchain and several follow-up applications based on distributed ledgers, the technology [i] has recently been recognised by the "business world" and is in ongoing exploitation [2]. However, only about 4% of consumers are already using Blockchain technology (BCT) consciously [3].[ii] This is particularly surprising, because consumers could already profit from a wide range of Blockchain based applications[iii] in terms of improvements in security, availability of applications or cost reductions and thereby increase their independence from banks, technology groups or individual states [4, 5, 6]. Furthermore, it is often advocated that BCT could reinforce consumers' data sovereignty by allowing them to share their data anonymously or for specific purposes only [7]. Beyond these specific functionalities, BCT offers consumers new opportunities to select favourable social systems for their interaction with others by "configuring" or choosing Blockchain-based solutions on the basis of their preferred set of assets, rules, norms or social coordination mechanisms [for this and below: 8]. In consequence, the technology probably changes economical structure not only by lowering transactio costs, but by lowering transaction costs, but by enforcing rules based on algorithms that are only partly asserted by trustworthy institutions so far and thereby constitutes new ways to build consensus (e.g. about what is of value) in the digital space. Concretely, BCT might enable consumers to take more active positions in transactions (e.g. by selecting "smart contracts") [6] or to foster their influence on prices and conditions on many markets due to increased market transparency [9].

The question now is why despite this potential the majority of consumers still hesitates to use Blockchain-based applications: maybe they are not aware of the technology's properties, perceive a lack of well-designed applications or are well-informed, but not convinced by the technology. Anyhow, when aiming at pushing the diffusion of Blockchain-based applications, it is essential to identify the reasons for consumers' current lack of acceptance concerning the underlying technology, especially because it is expected to strongly affect developers' risk of market introduction [10].

To do so, it is worth defining what is actually meant by "acceptance": starting at verbal definitions of the term, it refers to an attitudinal degree of affirmation regarding an object, e.g. a technology [11]. Nevertheless, the construct is often measured by actual usage or adoption, which is a possible, but not an inevitable consequence[iv] of a positive attitude towards usage that typically constitutes the intention to use a technology [12]. Anyhow, a usage intention, which we consider as "acceptance" in this paper in accordance with common acceptance theories and models,[v] can be regarded as a preliminary step for actual usage [13]. Therefore, it is very important to understand the attitudinal dimensions that drive the intention to use BCT, which will be the focus of this paper. In particular, it targets at identifying perceptions of BCT that are critical for its acceptance by consumers and further analyses their quantitative influence on usage intention to derive strategies for enhancing acceptance.

After discussing earlier publications that deal with acceptance aspects in the Blockchain field (part 2), common theories and models addressing technology acceptance are integrated and combined with Blockchain-specific beliefs into a novel research model that aims at explaining the acceptance of BCT among consumers (part 3). The methodology to empirically check the model's validity is presented in part 4. Therefore, an online survey among 157 German participants was conducted to test the research model. Survey's results are described in part 5. Conclusions are drawn and reflected in part 6.

2. Acceptance Research in the Blockchain Field

Different surveys from 2015-2018 report that about 50% of all consumers are aware of Bitcoin [4, 14, 15] and about 30% of BCT [3, 15]. In consequence, a lack of awareness does not explain low adoption rates. Henry et al. [14] further investigated the knowledge of central BCT characteristics among US-Americans in 2017, which was very low and thus

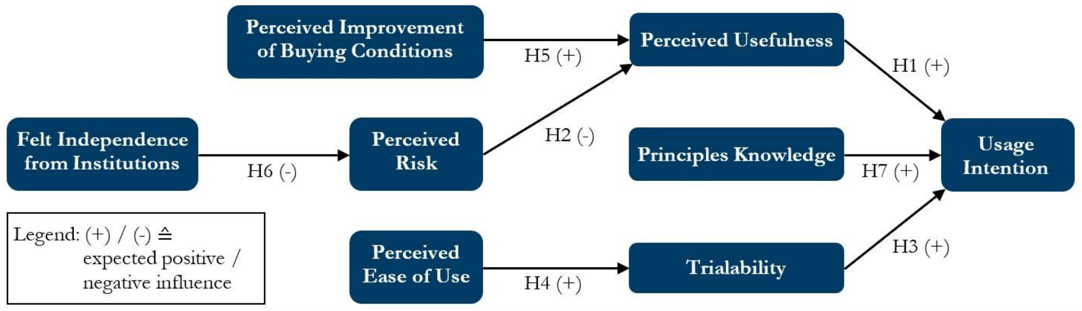


Figure 1. Research Model.

might be critical for further adoption.

Qualitatively, Folkinshteyn and Lennon [for this and below: 17] combine case studies and an interview with a Blockchain expert (Lasha Antadze) for identifying acceptance determinants of the Bitcoin and the Blockchain technology used as a financial software platform from developers' and end users' perspective. Their analysis results in a roughly structured accumulation of (potential) acceptance drivers. Baur et al. [18] follow a comparable approach by interpreting interviews with consumers and professionals to find usage determinants of cryptocurrencies, but furthermore assess the current state of perception concerning common acceptance determinants, in particular with regard to the Bitcoin. Woodside et al. [for this and below: 19] discuss BCT's status of adoption among firms from a management perspective by combining secondary data. For the purpose of this paper, in particular their discussion of drivers (e.g. transparency, costs, user control) and drawbacks (e.g. regulatory status, privacy and security) of BCT's adoption is addressed in addition to consumer-focused investigations, whereby it should be noted that adoption motives of firms probably differ from consumers' ones. On the level of applications, Francisco and Swanson [20] develop a conceptual model to explain the use of Blockchain-based Supply Chains that particularly puts a spot on the relevance of a system's transparency.

Quantitatively, Queiroz and Fosso Wamba [for this and below: 21] consider the level of transparency as a direct determinant of the intention to adopt BCT among US-American and Indian Supply Chain professionals. Surprisingly, their survey does not reveal a significant effect of the transparency on the usage intention and only partly confirms the relevance of some common acceptance constructs (in particular of "Facilitating conditions" and "Social influence") as well as of the trust among the stakeholders of a Blockchain for the adoption intention. Authors provide low awareness of BCT and cultural differences as possible explanations for their results. Abramova and Böhme [for this and below: 4] estimate a Structural Equation Model to explain Bitcoin usage of consumers. In particular, they specify risks and carve out the level of decentralisation, perceived security and control as well as characteristics regarding transaction processing as Blockchain-specific acceptance determinants. However, it remains open to discussion if these beliefs are also relevant for the acceptance of the underlying BCT and which additional perceptions might be crucial in this context. Kumpajaya and Dhewanto [22] further empirically validate a more generic model explaining Bitcoin-usage in Indonesia that explicitly incorporates "knowledge" as relevant acceptance predictor.

To sum it up, most of the few publications addressing Blockchain acceptance among consumers identify and structure (potential) acceptance drivers, but forego the empirical examination of their actual effect on usage (intention) or predominantly focus single applications only, in particular the Bitcoin Blockchain or Supply Chain solutions. This paper helps to close the resulting research gap by developing and empirically testing an acceptance model on BCT layer. Some of the earlier publications thereby serve to identify Blockchain-specific beliefs that are expected to influence consumers' usage intention. These beliefs are either incorporated by specifying more generic beliefs for a BCT context (cf. Table 1; all tables in the appendix) or represent newly developed Blockchain-specific variables in the research model (cf. Table 2).

3. Conceptual Framework and Research Model

This part is concerned with deriving the research model and its hypothesis, displayed in Figure 1. At the basic level, the research model is grounded on the "Theory of Reasoned Action" (TRA) developed by Martin Fishbein. The theory offers an empirically confirmed [23] framework for explaining the execution of behaviours that can be considered as a result of predominantly cognitive consideration[vi] and thus appears to be suitable for the initial or enduring usage of BCT due to the appreciable consequences and efforts technology changes imply [24].

The TRA distinguishes different types of beliefs to be crucial for forming a behavioural intention: "Behavioural Beliefs" are defined as the perceived probability that a behaviour (e.g. technology usage) leads to a specific outcome, e.g. privacy [for this and below: 13]. By forming Behavioural Beliefs, an overall "Attitude Toward the Behaviour" (ATB) is formed spontaneously. In addition to ATB, the TRA incorporates "Normative Beliefs", referring to the extent that others appreciate a behaviour or are likely to perform it, as influencing factor. Although Blockchain-based applications are "social" by design, these beliefs are not considered in the following, because most consumers are not expected to know many reference persons already using BCT or to feel social pressure to do so [20]. The "Theory of Planned Behaviour", an extension of TRA, further adds "Control Beliefs", which describe the felt control over performing a behaviour that might be restricted by factual or perceived barriers (e.g. lacking confidence). But due to many freely accessible Blockchain based applications, factual barriers should not be of notable relevance for BCT and perceived barriers will be captured by another variable ("Trialability", details later) to some extent.

Based on TRA, Davis specified Behavioural Beliefs determining the usage of technological innovations and integrated them into the "Technology Acceptance Model" (TAM) [25, 26], which has already been validated in a Blockchain context [22]. According to the TAM, one can assume that the "Perceived Usefulness" (PU), defined here as "the perceived likelihood that the technology will benefit the person in performance of some task" [26, p. 1063], has a direct positive influence on the usage intention of BCT:

H1: Perceived Usefulness positively influences the intention to use

Blockchain technology

It is noteworthy that PU should be considered relative to other technologies, because individuals continuously compare the functional benefits of currently used technology to technological alternatives [27]. The same holds for "Perceived Ease of Use" (PEOU), capturing expected mental and physical efforts necessary to learn and use a technology that lead to a general perception of a technology's "simplicity" [25, 26, 27] PEOU is especially relevant for the initial use of a technology and therefore, due to the low percentage of actual BCT users, expected to have a remarkable impact on overall acceptance of BCT [26]. Inside the TAM, it has a direct as well as an indirect positive effect on usage intention mediated by PU [28], but will be incorporated into the research model otherwise (cf. H4).

Over time, several modifications of the TAM emerged: Pavlou in particular added "Perceived Risk" (PR), defined as "consumer's subjective belief of suffering a loss in pursuit of a desired outcome" [29, p. 77], which has a direct negative impact on the intention to force an online transaction [for this and below: 29]. This "outcome" can refer to costs, performance, security or privacy. Following Pavlou, PR is particularly important in the context of online transactions due to the impersonality, the limited possibilities to check the quality of goods and services in advance and potential interventions by third parties and thus appears to be indispensable in a BCT context. Because the reduction of risks in a transactional context is an essential idea of BCT constituting its usefulness [30], PR probably should be interpreted as a determinant of PU:

H2: Perceived Risk negatively influences Perceived Usefulness

Because of its confirmed validity for strongly differing applications (for meta-analysis, see [31]), the TAM is considered to be an appropriate model for gathering general information about perceptions associated with or for figuring out a general level of satisfaction regarding a technology [for this and below: 32]. However, whenever aiming at collecting information about specific perceptions that promote or impede a technology's acceptance, the quite generic TAM should be combined with other conceptualisations that allow a theory-based enrichment with context-specific constructs. To do so, further beliefs are derived in the following.

Firstly, "Trialability" is introduced, referring to the (perceived) extent to which possibilities to experiment with an innovation are available [33]. Thus, it can be considered as expression of a Control Belief inside the TRA [34].[vii] The variable is included, because it is especially important at early stages of diffusion, which is the case if only a few, very "innovative" consumers are using an innovation [33, 34]. As introductorily mentioned, this holds for BCT. The variable stems from the so-called "Diffusion Theory" by Rogers [for this and below: 33]. In contrast to the TAM, it explicitly models the dynamic process of technology adoption every individual passes through as part of a social system, before, while and after adopting a (technological) innovation [34], thus allowing acceptance determinants[viii] to vary in importance over time. According to Rogers, Trialability fosters adoption (respectively usage):

H3: Trialability positively influences the intention to use Blockchain technology

Trialability is furthermore used as a "bridge" to incorporate PEOU into the research model: the easier learning and using of a technology is perceived, the easier it is to try and the more likely consumers are expected to confidently state that they know possibilities to initially use it, i.e. expressing a higher Trialability [33]:

H4: Perceived Ease of Use positively influences Trialability

All theory-based beliefs discussed correspond to more specific beliefs in the context of Blockchain-based applications, which are repeatedly mentioned in earlier Blockchain-related research and called "subordinate beliefs" in Table 1. The perception of these subordinate beliefs is strongly related to actual (technical) characteristics of Blockchain-based applications. Table 1 schedules some of these relations that make clear how important certain (technical) properties are for the formation of certain beliefs and thus that perceptions cannot be detached from technical specifications and vice versa. In the following, Blockchain-specific Behavioural Beliefs in the sense of TRA are introduced that are constituted by typical characteristics of Blockchain-based applications (cf. Table 2).

Stemming from increased efficiency [4] and the introductorily mentioned possible enhancement of consumers' position in many markets, BCT might improve their buying conditions in the internet (including price, terms of delivery/return, etc.). Because these improvements are not expected for all applications, the variable is not incorporated in PU. However, the more consumers believe that BCT provides improved outcome, the higher PU should be:

H5: Perceived Improvement of Buying Conditions positively influences Perceived Usefulness

Felt Independence from Institutions is designed to capture a consumer's perceived ability to take decisions independent from the influence of existing institutions [35][ix]. This independence is potentially empowered by BCT use, because peer-to-peer transactions become possible without any bank involved [4, 17], centrally offered services of technology groups (e.g. search engines) are challenged by Blockchain-based solutions [36] and if participants, respectively servers, of a Blockchain are widely distributed over multiple states, their consensus is beyond the control of single states [4, 17]. This independence is not only part of the ideology many Blockchain-based solutions (e.g. the Bitcoin system) are based on [37]. It can also be considered from a risk perspective: because dependency gives institutions the possibility to intervene or to exploit consumers' vulnerability, it entails uncertainty and perceived risks [29]. H6 follows:

H6: Felt Independence from Institutions reduces the Perceived Risk

Besides beliefs, earlier Blockchain-related research extracted a lack of actual knowledge of the technology as acceptance predictor [22]. This evidence is supported by the TRA considering knowledge as "background factor" [13]. The Diffusion Theory even describes an "Awareness stage" that is critical for the decision to even form an attitude towards a technology later on [for this and below: 33]. In this stage, having heard of an innovation, individuals seek for further information about it if they realise a potential need satisfaction by using it. Thereby, consumers acquire different types of knowledge: while "How-to-Knowledge" (HTK) refers to ways an innovation can be used, "Principles Knowledge" (PRK) is about underlying functional principles. This differentiation can be applied to BCT: beyond knowing how to come in touch with the technology, which is strongly addicted to Trialability, HTK should, in a BCT context, predominantly be about coming along with interfaces, which is widely captured by PEOU. But the functional principles (decentralisation, etc.) of BCT are not just background information, because their understanding can be regarded as necessary to understand the technology's potential to satisfy needs and to reason its existence. Thus, PRK is explicitly considered as direct antecedent of the usage intention, leading to:

H7: The level of Principles Knowledge positively influences the intention to use Blockchain technology

4. Methodology

To validate the research model, an online survey was conducted in July 2018. A link was sent to e-mail distribution lists of student organisations as well as sport clubs and was distributed on Social Media (convenience sample). Due to the chosen channels, participants were relatively young

(in average 33 years old) measured against the German population.[x] The survey was named "future technologies in everyday life" to avoid self-selection, i.e. that mainly people who are interested in BCT participate in the survey and thus bias in particular the awareness and knowledge measurement.

The survey is structured as follows (cf. Table 3): after some general questions concerning the use, intention to use and perceived relevance of BCT and selected reference technologies[xii], the participants were asked to state, how clearly they know the functional principles of BCT. Only participants who expressed a vague understanding of the technology's functioning were exposed to questions measuring general beliefs regarding the BCT and a "relatively clear" perceived understanding was required to reveal specific beliefs. This adaptive design was chosen, because those claiming not to have any understanding of the technology will presumably not be able to state stable beliefs about BCT and thus were asked to rate attributes of a new app for automatic online shopping that are typical for many Blockchain-based applications (e.g. Protection against subsequent manipulations) instead. For each pair of attributes participants needed to decide which is more important for them (full profile measurement). By applying a Bradley-Terry-Luce-Test [38, 39], the relative importance of these attributes was analysed. In consequence, the research model was tested directly by Structural Equation Modeling and indirectly by considering the Pairwise Comparisons.

The latent variables of the Structural Equation Model (SEM) are designed by applying the C-OAR-SE procedure for scale development [40]. In consequence, the variables "Usage Intention", "Trialability" and "Perceived Improvement of Buying Conditions" are classified as concrete attributes leading to a single-item-measure. All other constructs besides PEOU and PRK are formed by beliefs regarding the BCT. Thereby, technology's characteristics serve to reason subordinate beliefs and thus specify the formative measurement of theory-based constructs (cf. Table 1). In contrast, PEOU, although also affected by the technology's characteristics, usually is not formed by different, widely independent attributes, but more of general disposition reflected in multiple, highly correlated beliefs and therefore measured in a reflective manner. Because specific beliefs regarding the BCT and its applications are supposed to be perceived relative to the status quo, these are measured "compared to existing IT applications" (cf. Table 7). In consequence of the adaptive survey design, only 32 participants expressed these specific beliefs, which still is a sufficient number to get meaningful results for the SEM [41].

In general, constructs were measured relying on validated scales, if possible (see Table 4 for details), and backward-translation was executed for the survey's presentation inside this paper. To calculate the SEM, path-based weighting is used and a Bootstrapping including 5000 random subsamples performed using the software "Smart PLS". Thereby, actual users are assumed to also have an intention to use BCT.

Finally, to motivate the presumably already exhausted participants to reveal their knowledge of BCT, "Gamification" elements have been integrated [42] in form of a "Blockchain-Quiz" consisting of ten true/false questions whereby the first five have been designed to measure How-to-Knowledge and the other five for measuring Principles Knowledge (for details, see Table 5).

The questions have been designed to capture Blockchain-based applications most commonly used by consumers (and thus have a focus on public (permissionless) Blockchains) and to be as easy to understand while maintaining as much precision as possible. To further differentiate the participants' knowledge, they were asked to state their confidence for every answer to calculate "Confidence Ratings" that weight correct answers with strong confidence higher than correct answers with low confidence. Incorrect answers are handled contrariwise. This approach is especially used to calculate a Principles Knowledge Score for each participant which is called "Principles Knowledge" in the following.

Therefore, the calculation scheme by Hassmen and Hunt [43] is used. Due to the fact that the quiz has been designed as an appendix after the primary survey, results should be generalised carefully with respect to average knowledge levels (presumably they are overestimated), because the decision to take part in the quiz might actually be a knowledge predictor [14]. But to distinguish between participants having comparably high and low knowledge levels, which is the main purpose of the quiz, this is not a problem.

5. Results

5.1. Descriptive Statistics on Usage, Knowledge and Perception of the Blockchain Technology

Looking at Figure 2, a majority of 61.1% has already heard of BCT, which is the lowest percentage of all tested technologies, but higher than earlier surveys [3, 16] indicated. Comparatively high awareness might be a consequence of the relatively young and educated participants[xii] or technology's high media coverage prior to the survey [30]. Nevertheless, only five (3.2%) respondents state to use BCT and 19 (12.1%) more to have the intention to do so in the future.[xiii]

As discussed earlier, limited knowledge might be an adoption barrier. Results of the Blockchain Quiz, displayed in Table 5, reveal that only 59% of all true/false-questions are answered correctly. In total, HTK seems to be very low, it is even not possible to show that in average, the amount of correct answers (2.55 of 5) is different from random guessing ($p > 0.1$ (t-test)). Regarding PRK, 3.36 of 5 answers are correct, which is definitively a higher number than expected by random guessing ($p < 0.01$ (t-test)), but also capable of improvement.

Asking for associations to the stimulus "Blockchain" (cf. Figure 3) many of the 61 participants who entered an answer think of cryptocurrencies (n = 9) or Bitcoin in particular (n = 14) or refer to essential ideas of BCT like "Decentralisation" (n = 11) or "Linkage/chaining of data" (n = 7). Also noteworthy is the repeated mentioning of the high energy consumption (n = 5).

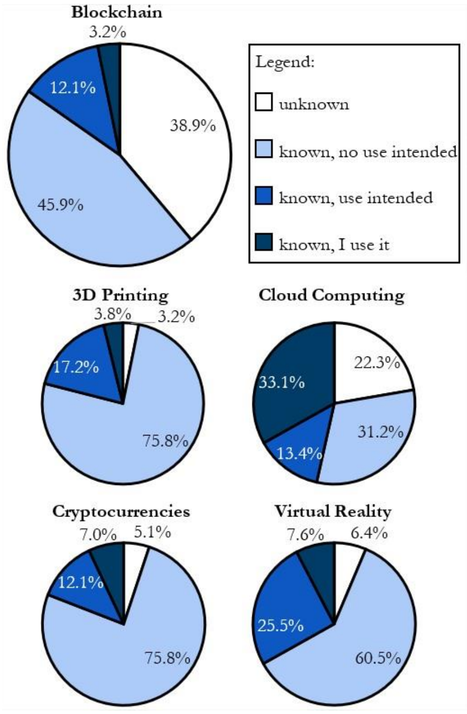


Figure 2 : Awareness and usage of selected technologies.

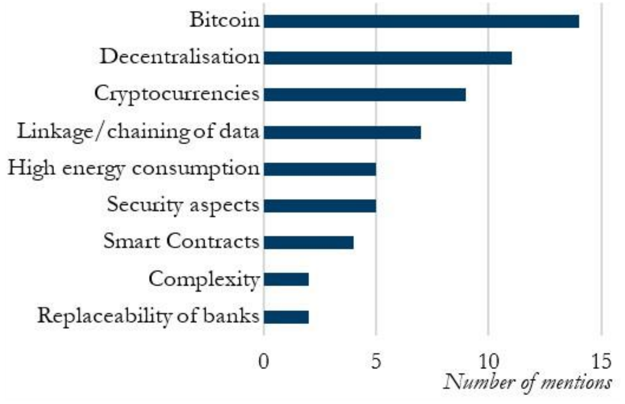


Figure 3. Associations to the stimulus "Blockchain".

Referring to the general perception of BCT, participants think that it is generally useful, but are not convinced that it delivers value to them personally (cf. Table 6, items 1 and 2). Generally, the technology is perceived as complex and hard to understand, leading to a low PEOU. A notable risk perception can be observed, which however is not extraordinarily high. Trialability is basically very low, but perceived very differently as the high variance indicates. As anticipated, social norms currently are negligible.

Regarding specific beliefs (cf. Table 7), the answers' general proximity to the scale centre indicates that participants evaluate specific attributes of Blockchain-based applications similar to those of currently used IT applications. This holds in particular for the independence from technology groups as well as for perceived transaction costs and buying conditions. Independence from individual states or banks and privacy protection are only perceived slightly better. In contrast, transparent process documentation, the protection against transactions' manipulation and the perception of legal risks positively stand out.

5.2. Pairwise Comparisons (PC) (Indirect Proof of the Research Model)

As Figure 4 reveals, security aspects, especially the protection of personal data and against fraud, seem to be very important in the context of automated online transactions compared to other properties. The possibility to specify further criteria (e.g. the delivery date) in combination with an option to refuse the app's recommendation, called "Freedom of decision (customisable attributes)", and the additional consideration of manufacturers' stores for price comparison, called "Independence from ordering platforms", are also relevant. In contrast, the app's permanent availability and low costs of payment execution appear to be relatively unimportant. However, this result should not be misinterpreted, because the importance of availability might only be realised if problems occur and referring to costs, these might have become elusive, because no concrete values were introduced.

5.3. Structural Equation Model (SEM) (Direct Proof of the Research Model)

Figure 5 (on the next page) displays the estimated SEM. Evaluating model's quality, the coefficients of determination (R^2) can be interpreted as "satisfying" regarding Usage Intention ($R^2 = 0.294$) and PR ($R^2 = 0.327$) and as "substantial" for PU ($R^2 = 0.513$) due to the many potential determinants [41]. Considering multicollinearity between constructs and the items in case of formative variables, variance inflation factors should be regarded [44]: all range from 1.0 to 1.8 (for details, see Table 8), which is far below widely accepted maximum values of 5 or 10. For addressing PEOU, factor loadings indicate sufficient internal consistency (all above 0.7) [41]. Bootstrapping reveals that all hypothesis can be confirmed at 10% significance level and besides H5 all even at 5%. In consequence, validity of the SEM can be assumed.

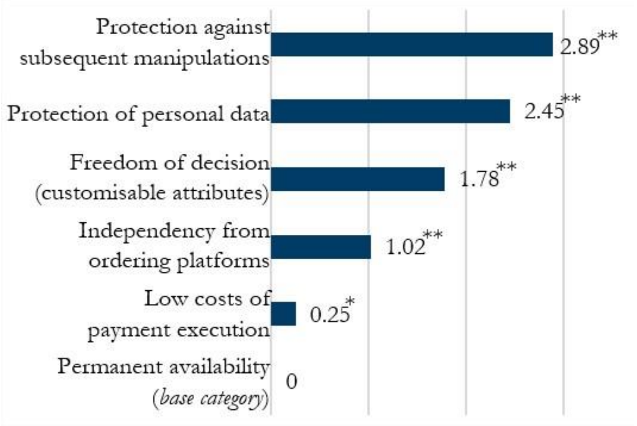


Figure 4. Pairwise Comparisons.

Legend:
values represent parameters of a Bradley-Terry-Luce-Test with "Permanent availability" as pre-defined base category.
* / ** - significantly different from base category at 10% / 1% level

In addition to path coefficients (cf. Figure 5), that already allow a first indication of effect sizes, F^2 is calculated for each relationship (cf. Table 9). Considering direct determinants of Usage Intention, Trialability, which clearly depends on PEOU ($F^2 = 0.200$), emerges as strongest ($F^2 = 0.192$), while PU ($F^2 = 0.111$) and PRK ($F^2 = 0.059$) have a comparatively small, but unambiguous effect on it. Perceived Improvement of Buying Conditions has a remarkable influence on PU ($F^2 = 0.723$) and the Felt Independence from Institutions reduces PR strongly ($F^2 = 0.485$). Finally, it appears suitable to model PR as a determinant of PU having an indirect effect on Usage Intention only ($F^2 = 0.137$). Looking at items' weighting factors to form latent variables, summarised in Table 8, indirect conclusions can be drawn [44]:[xiv] Felt Independence from Institutions is surprisingly dominated by perceived independence from individual states ($\gamma = 0.435$) and technology groups ($\gamma = 0.660$), whereby it should be noted that the latter's effect might be affected by privacy improvements addicted to independence from technology groups [9]. PR extensively consists of the perception, that predominantly criminals use BCT ($\gamma = 0.505$), but obviously other influence factors also contribute to BCT's application being perceived as generally "risky" ($\gamma = 0.485$) and associated to potential losses ($\gamma = 0.330$). Lastly, PU strongly depends on the expected transaction costs ($\gamma = 0.322$), which is in line with findings regarding Perceived Improvement of Buying Conditions, as well as on perceived privacy protection ($\gamma = 0.341$) and a general value perception of BCT usage ($\gamma = 0.536$).

5.4. Integration of Results

To sum it up, consumers miss possibilities to try out BCT which they perceive to be very complex. Maybe because of their low knowledge of the disrupting ideas or principles the technology is based on, they do not realise how they can personally benefit from it. Finally, the following four beliefs regarding BCT are found to be specifically critical for stimulating acceptance:

- Expected Improvement of Transaction Conditions (derived from SEM)
- Perceived Privacy Protection (derived from PC and SEM)
- Felt Independence from Institutions (derived from SEM and indicated by PC)
- Perceived Fraud Protection (derived from PC and SEM)

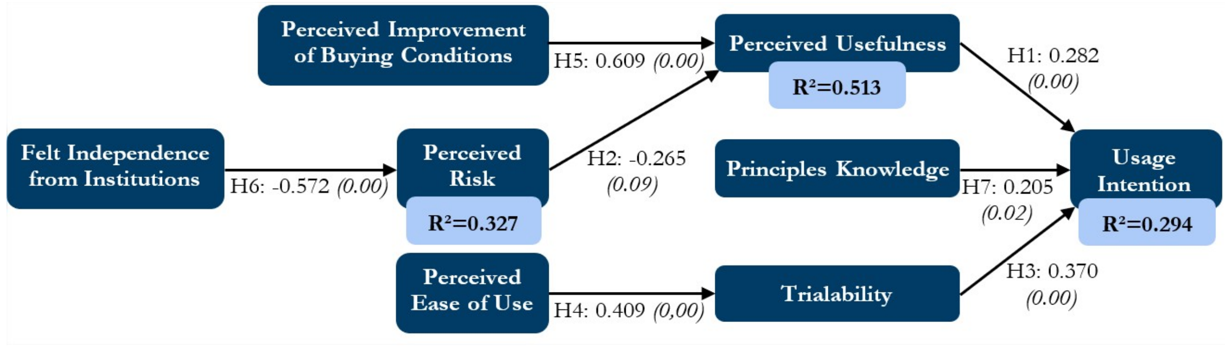


Figure 5. Structural Equation Model.

Legend: hypothesis (cf. part 3) → H6: -0.572 *(0.00)* ← error term (calculated by Bootstrapping-procedure)
↑
standardised path coefficient

6. Discussion

The results allow for concluding implications from the perspective of multiple stakeholders. The stated lack of legal certainty, for example, emphasises the importance of closing gaps in the law, e.g. in Data Protection Law [45] or Contract Law [46]. But in the following, the focus will be on suitable communication strategies to form desirable beliefs about BCT and on recommendable directions of the technology's further (technical) development. Final remarks, moreover, discuss conclusions for future research.

6.1. Communication Strategies Towards Consumers

(Persuasive) communication is a well-established instrument to form desirable beliefs [13]. The following recommendations are relevant for all institutions that might be interested in stimulating the diffusion of BCT (e.g. governmental ministries) or of applications based on BCT (e.g. start-up companies), because the general attitude towards the technology's usage profits from application's image whenever referring to BCT (e.g. in advertising) and vice versa ("image transfer"). Although target groups for communication should be defined context- and application-specific, general recommendations can be derived from the results by applying the already introduced Diffusion Theory (cf. part 3), which differentiates human stereotypes, called "Adopter Types", by their innovativeness [for this and below: 33]. The first to adopt are "Innovators", typically interacting with other Innovators, who are adventuresome, risk-seeking and have the ability to understand complex innovations. They serve as "gatekeepers" for a technology's diffusion and inspire "Early Adopters", who regularly catch up on new trends and enjoy to be local opinion leaders. Members of the "Early Majority" carefully weigh up innovations' usage and thereby refer to Early Adopters, who in consequence are crucial for reaching a critical mass.

Now comparing the percentage of actual BCT users (3.2%) with the estimated percentage of innovators in the population (ca. 2.5%[xv]) [for this and below: 33], one can conclude that the Innovators already use BCT by a majority. In contrast, Early Adopters (ca. 13.5% of the population) typically have already formed an intention to use the technology, but hesitate to use it (which is true for 12.1% of respondents) and thus are critical for the technology's further adoption, especially considering their influence on later Adopters. Early Adopters, for example, could be targeted by using methods discussed in the context of "Influencer Marketing" due to their increased use of Social Media, reasoned by their intense need for social participation. As regards content, possibilities to use BCT might be communicated (increasing Trialability) by emphasising improvements through the technology with respect to critical beliefs carved out in part 5 (Expected Improvement of Transaction Conditions, etc.). Thereby, it might be advisable to refer to technical characteristics for enhancing Principles Knowledge, which entails the challenge to explain complex principles as comprehensibly as possible. However, most crucial for communication success might be the derivation of tangible benefits and additional possibilities through the use of BCT from technical characteristics. Early Adopters, for example, possibly need to realise that BCT enables them to choose the way and rules of social interaction independent of technology groups or states.

6.2. Further Development of Blockchain-Based Applications

General recommendations for further development address business model creators just as frontend- and backend developers of Blockchain-based applications. First of all, a focus on usability to increase PEOU and to enhance the user experience [47] as well as the passing-on of savings due to Blockchain usage to consumers to some extent (leading to improvements of transaction conditions for them) is generally advisable. The relevance of "Independence from Institutions" further invites small providers of Blockchain-based applications to use the technology to communicate increased Independence from Institutions to gain competitive advantage. Privacy protection can be ensured by anonymity, which, however, is not guaranteed only because pseudonyms are used [17] and might be opposed to legal certainty. Anyway, only putting data "on-chain" that are necessary for the functionality of an application and informing users about (reasons for) use of data [48] could also increase perceived privacy protection. To counter consumers' perceived risk to be defrauded, certifications for Blockchain solutions offered by trustworthy organisations based on transparent criteria [49] and insurances covering overestimated risks [4] are promising options. Continuing the development of solutions for the protection of private keys could further contribute to perceived risk reduction [50].

6.3. Research Implications and Final Remarks

From a researcher's perspective, a new, Blockchain-specific acceptance model has been developed, which delivers an explorative starting point for further acceptance research addressing BCT and some interesting findings for technology acceptance research in general. In particular, the interpretation of PEOU as an essential determinant of Trialability in the context of emerging technologies that has only occasionally been applied in the past [34] and the consideration of PR as influencing factor of PU whenever risk reduction is a constituting idea behind a technology's usage might inspire future research.

Of course, this paper faces many limitations: first of all, only usage intention and not actual usage is explained and no representativeness for the German population ensured. Furthermore, it leaves the explicit consideration of hedonic usage motives and expected changes of the interaction in social systems to future research. Although many of the indicated effects are probably valid for consumers from other countries than Germany, cultural differences, in particular in terms of technology usage habits, as well as country-specific requirements depending on legal circumstances and the technical infrastructure [21] might restrict international transferability. Moreover, technical trade-offs in Blockchain designs (e.g. between usability and security) leading to limits in evoking desirable perceptions at the same time have not been regarded [51]. Finally, some might argue that it only makes sense to research the acceptance of specific applications and not of the underlying technology because of the diversity of applications and designs. However, even for acceptance research on the application level, which is expected to increasingly follow in the future, this paper provides indications for research designs as well as for critical beliefs determining consumers' acceptance that is considered to be of outstanding importance to help the Blockchain technology fulfil its potential.

Appendix:

Table 1. Derivation of theory-based beliefs.

Theory-based belief	**Corresponding theory**	**Subordinate beliefs relevant in Blockchain context (selection)**	**Corresponding characteristics of Blockchain applications (selection)** [51]
Perceived Usefulness	TAM	Perceived increase of transparency [17, 18, 19, 22]	Availability (+) Consistency (+) Vulnerability Resistance (+)
		Expected reduction in transaction costs* [4, 17, 18, 19, 22]	(low) direct, monetary transaction costs (+) (low) indirect transaction costs (+) (e.g. required time depending on transaction validation speed and the effort that is necessary to find a transaction partner)
		Perceived improvement of privacy protection* [4, 17]	Confidentiality (+) (e.g. enabled by pseudonymity, applied encryption methods or user-managed data exchange) Integrity (+)
Perceived Ease of Use	TAM	Usability perception [17, 18]	Interoperability between applications (+) Exchangeability of cryptocurrencies (+) Response time (-) Support for constrained devices (+)
Perceived Risk	TAM, extended	Perception of fraud risks [4, 17, 18, 19, 22]	Confidentiality (-) Consistency (-) Integrity (-) (especially tamper-resistant logging) Decentralisation (-) Vulnerability resistance (-)
		For more detailed discussion of risks associated with BCT usage, see [4]	
Trialability	Diffusion Theory	Accessibility [4, 17, 18, 19, 22]	Availability (+) Interoperability between applications (+) Required bandwidth (-) Support for constrained devices (+)

Table 2. Derivation of technology-based beliefs.

Technology-based belief	**Subordinate beliefs relevant in Blockchain context (selection)**	**Constituting characteristics of Blockchain applications** [51] For argumentation regarding independence, compare [4]
Felt Independence from Institutions	Independence from technology groups*	Possible consequence of disintermediation and… …decentralisation by taking over services of technology groups or banks enabled by BCT (independence from technology groups and banks) *or respectively* …the international distribution of power to change consensus (independence from states) These processes are enabled by BCT's characteristics, especially by Availability, Confidentiality, Consistency, Integrity, Encryption, Resilience, Vulnerability resistance, (low) costs (of transactions), Ease of Node Adoption, Support for constrained devices
	Independence from banks*	
	Independence from states*	
Perceived Improvement of Buying Conditions	Expected price	*Directly* based on (low) monetary costs (of transactions), (high) transaction validation speed *and indirectly* by transparency-induced (potential) gain of power in transactional relations as a consequence of market transparency and disintermediation [9]
	Expected terms and conditions	

Table 3. Adaptive design of the online questionnaire.

Part of the online questionnaire	**Abbreviation**	**Number of participants**	**Understanding of functional principles (of BCT)** (referring to "Perceptual Awareness Scale" [55])			
			none	vague	relatively clear	clear
General technology use	GT	157	🟩	🟩	🟩	🟩
BCT: general beliefs	BG	73	🟥	🟩	🟩	🟩
BCT: specific beliefs	BS	32	🟥	🟥	🟩	🟩
Pairwise Comparisons (attributes of a new app)	PC	102	🟩	🟩	🟥	🟥
Personal data	PD	128	🟩	🟩	🟩	🟩
Blockhain-Quiz (appendix)	QU	49	🟩	🟩	🟩	🟩

Legend: 🟩 displayed 🟥 not displayed BCT = Blockchain technology
The number of participants includes all who answered at least one question of the part.

Table 4. Measurement models in the Structural Equation Model.

Latent variable	**Type of measure-ment**	**Item's description** (cf. Table 6 and Table 7)	**Questionnaire part** (cf. Table 3)	**Origin of item's scale** (BC = measured in a Blockchain context)
Perceived Usefulness	Formative	BCT use valuable	BG	[29] [22 (BC)]
		Privacy protection	BS	
		Low transaction costs	BS	
		BCT useful	BG	
Perceived Ease of Use	Reflective	BCT easy to understand	BG	[26, 29, 56] [20 (BC)]
		BCT use easy to learn	BG	
Perceived Risk	Formative	BCT use risky	BG	~ [29] [22 (BC)]
		Damage from BCT use	BG	
		Criminal users of BCT	BG	
Felt Independence from Institutions	Formative	Independence from technology groups	BS	/
		Independence from banks	BS	
		Independence from states	BS	
Perceived Improvement of Buying Conditions			BS	/
Trialability			BG	[56]
Principles Knowledge			QU	[43]
Usage Intention			GT	/ (dichotomous)

Legend: BCT = Blockchain technology All scales used were translated into German and thereby partially slightly modified.

Table 5. Blockchain-quiz – questions and results.

	Question Nr.	**Question text**	**Correct answer**	**Share of correct answers**	**Ø Confidence rating**	**Score** (Ø = average / SD = standard deviation)
How-to-Knowledge (HTK)	1	Recipient's public key is needed to initiate a transaction	true	49%	1,77	Ø = + 6,3/SD = 31,0
	2	Recipient's private key is needed to initiate a transaction	false	27%	1,98	Ø = - 2,8/SD = 31,7
	3	Private and public keys consist of numbers and letters	true*	84%	2,27	Ø + 30,9/SD = 21,4
	4	On prevalent Blockchains, transactions are approved by an authorised participant (central authority)	false	63%	2,06	Ø = + 19,6/SD = 28,0
	5	New transactions are immediately incorporated into the Blockchain	false	33%	2,06	Ø = - 6,1/SD = 33,5
	Total			**51%**	**2,03**	**Ø = + 9,57/SD = 68,1**
Principles Knowledge (PRK)	6	Each block has one specific predecessor	true	79%	1,91	Ø = + 21,6/SD = 26,2
	7	Usually, multiple transactions are assigned to a block	true	62%	1,72	Ø = + 18,0/SD = 25,5
	8	Usually, a transaction is distributed to multiple blocks	false	60%	1,60	Ø = + 15,0/SD = 24,7
	9	On public (permissionless) Blockchains, all transactions are typically visible for all participants	true	79%	1,64	Ø = + 24,8/SD = 20,6
	10	If "proof-of-stake" consensus mechanism is applied, a miner's asset influences his chance to create an upcoming block	true	57%	1,34	Ø = + 9,4/SD = 24,5
			Total	**67%**	**1,64**	**Ø = + 88,8/SD = 67,5**
			Total HTK + PRK	**59%**	**1,84**	**Ø = +136,5/SD = 107,7**

Legend: *if displayed in conventional hexadecimal system. Questions partly inspired by Henry et al. [14].
n = 49 (varies due to drop outs for each question; 46 participants answered all ten questions).
"Confidence Rating" is scaled from 0 (very unconfident) to 4 (very confident). Score ranges from -60 to +50 for each question, in consequence from -300 to +250 for HTK and PRK and from -600 to +500 in total.

Table 6. Beliefs about Blockchain technology (BCT).

Item Nr.	**Item Text**	**Item description**	**Average (ranges from 0 to 4)**	**Standard deviation** (in scale points)
1	The use of Blockchain technology is valuable for me	BCT use valuable	1.98	1.09
2	The technology is useful	BCT useful	3.25	0.70
3	Blockchain technology is easy to understand	BCT easy to understand	1.24	0.90
4	Technology's application is easy to learn	BCT use easy to learn	1.69	1.09
5	The application of Blockchain technology is risky	BCT use risky	1.57	1.16
6	Using the technology can cause substantial damage for me	Damage from BCT use	1.64	0.98
7	Blockchain technology is predominately used by criminals	Criminal users of BCT	1.23	0.81
8	I know how to try out Blockchain applications	Trialability	1.77	1.42
9	Others expect me to use Blockchain technology	Social Norm *(not part of SEM)*	0.80	1.06

Legend: items were measured in questionnaire part "BG" (cf. Table 3).
SEM = Structural Equation Model. Corresponding question: how strongly do you agree with the following statements concerning the Blockchain technology?
n = 70; participants stating "cannot judge" were filtered out. In consequence, actually considered responses for each item range from 45 to 64. Scale points are named the following:
0 (minimum) – fully disagree | 1 – rather disagree | 2 – neither agree nor disagree | 3 – rather agree | 4 (maximum) – fully agree

Table 7. Specific beliefs about Blockchain technology (BCT).

Item Nr.	**Item text "Blockchain applications…"**	**Item description**	**Average (ranges from 0 to 4)**	**Standard deviation** (scale points)
10	"…make me independent from technology groups"	Independence from technology groups	2.32	1.06
11	"…make me independent from banks"	Independence from banks	2.76	1.02
12	"…make me independent from individual states"	Independence from states	2.42	1.07
13	"…are characterised by low costs per transaction"	Low transaction costs	2.04	1.34
14	"…protect my privacy"	Privacy protection	2.46	1.07
15	"…improve the conditions at which I can buy goods and services"	Perceived Improvement of Buying Conditions	1.91	1.24
	Perception of selected functionalities			
16	"…can record processes transparently"	Transparent process documentation	3.03	0.87
17	"…preclude the manipulation of transactions"	Manipulation resistance	2.71	1.21
18	"…preclude the execution of transactions in the name of someone else"	No identity fraud	1.58	1.10
	Risk perception			
19	"…hold legal risks"	Legal risk	2.60	1.00
20	"…hold the risk to loose money due to fraud"	Fraud risk	2.10	1.15
21	"…lack maturity and thus their usage could cause substantial damage to me"	Maturity risk	1.86	1.11

Legend: items were measured in questionnaire part "BS" (cf. Table 3).
n = 32; participants stating "cannot judge" were filtered out. In consequence, actually considered responses for each item range from 23 to 29.
Corresponding question: how do you evaluate Blockchain applications generally regarding the following characteristics compared to currently used IT applications?
Scale points are named the following: 0 (minimum) - much less pronounced | 1 – little less pronounced | 2 – equally pronounced 3 – little more pronounced |4 (maximum) – much more pronounced

Table 8. Accuracy of the Structural Equation Model.

Latent variable	**Item description** (cf. Table 6 and Table 7)	**Coefficient β** (formative) **/ factor loading r** (reflective)	**VIF** (formative) **/ reliability coefficient ϱ** (reflective/1-item)
Perceived Usefulness (PU)	BCT use valuable	β = 0.536	VIF = 1.372
	Privacy protection	β = 0.341	VIF = 1.238
	Low transaction costs	β = 0.322	VIF = 1.174
	BCT useful	β = 0.217	VIF = 1.444
Perceived Ease of Use (PEOU)	BCT easy to understand	r = 0.873	ϱ = 0.843
	BCT use easy to learn	r = 0.833	
Perceived Risk (PR)	BCT use risky	β = 0.485	VIF = 1.365
	Damage from BCT use	β = 0.330	VIF = 1.425
	Criminal users of BCT	β = 0.505	VIF = 1.140
Felt Independence from Institutions	Independence from technology groups	β = 0.660	VIF = 1.079
	Independence from banks	β = 0.254	VIF = 1.783
	Independence from states	β = 0.435	VIF = 1.689
	Perceived Improvement of Buying Conditions	r = 1.000 (single item)	/
	Trialability	r = 1.000 (single item)	/
	Principles Knowledge	r = 1.000 (single item)	/
	Usage Intention	r = 1.000 (single item)	/

Legend: VIF = variance inflation factor.

Table 9. Effect sizes of the Structural Equation Model.

Hypothesis	Relation	F² | effect strength	Hypothesis	Relation	F² |effect strength
H1	PU→Intention	F² = 0.111|small	H5	Conditions→PU	F² = 0.723|strong
H2	PR→PU	F² = 0.137|small	H6	Independence→PR	F² = 0.485|strong
H3	Trialability→Intention	F² = 0.192|medium	H7	Principles Knowledge → Intention	F² = 0.059|small
H4	PEOU→Trialability	F² = 0.200|medium	Legend: evaluation of effect strength based on Hair et al. [41]		

Legend: PU = Perceived Usefulness PEOU = Perceived Ease of Use PR = Perceived Risk

References:

[1] S. Nakamoto, "Bitcoin: A peer-to-peer Electronic cash system", 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: June 04, 2019].

[2] V. Morabito, "Business innovation through blockchain", Cham: Springer International Publishing, 2017.

[3] YouGov Deutschland GmbH, "Blockchain Revolution: How Blockchain-Technology will change the Financial Sector from a Consumer's Perspective". [Original title] "Blockchain-Revolution: Wie die Blockchain-Technologie die Finanzwelt aus Verbrauchersicht ändern wird", 2017. [Online]. Available: https://yougov.de/news/2017/09/04/blockchain-als-nachste-stufe-des-internets/. [Accessed: June 07, 2019].

[4] S. Abramova and R. Böhme, "Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study", in Proceedings of the 37th International Conference on Information Systems (ICIS), Dublin, Ireland, pp. 1–20, 2016.

[5] S. Davidson, P. De Filippi and J. Potts, "Economics of Blockchain", SSRN Journal, 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751. [Accessed: June 07, 2019].

[6] C. R. Harvey, C. Moorman and M. Toledo, "How Blockchain Will Change Marketing As We Know It", SSRN Journal, 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3257511. [Accessed: June 26, 2019].

[7] G. Zyskind, O. Nathan and A. 'S.' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", in 2015 IEEE Security and Privacy Workshops, San Jose, California, USA, pp. 180–184, 2015.

[8] A. Hayes, "The Socio-Technological Lives of Bitcoin", Theory, Culture & Society, vol. 36, no. 4, pp. 49–72, 2019.

[9] L. W. Cong and Z. He, "Blockchain disruption and smart contracts", The Review of Financial Studies, vol. 32, no. 5, pp. 1754–1797, 2019.

[10] N. Jonker, "What Drives Bitcoin Adoption by Retailers", SSRN Journal, 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3134404. [Accessed: June 07, 2019].

[11] A. Schwarz and W. Chin, "Looking forward: Toward an understanding of the nature and definition of IT acceptance", Journal of the Association for Information Systems, vol. 8, no. 4, pp. 230–243, 2007.

[12] V. Venkatesh, M. G. Morris and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View", MIS Quarterly, vol. 27, no. 3, pp. 425–478, 2003.

[13] M. Fishbein and I. Ajzen, "Predicting and changing behavior: The reasoned action approach", New York: Psychology Press, 2010.

[14] C. S. Henry, K. P. Huynh and G. Nicholls, "Bitcoin Awareness and Usage in Canada", in Bank of Canada Staff Working Paper, no. 56, 2017. [Online]. Available: https://www.bankofcanada.ca/wp-content/uploads/2017/12/swp2017-56.pdf. [Accessed: June 07, 2019].

[15] S. Schuh and O. Shy, "U.S. Consumers' Adoption and Use of Bitcoin and other Virtual Currencies", 2015. [Online]. Available: https://www.bankofcanada.ca/wp-content/uploads/2015/12/us-consumers-adoption.pdf. [Accessed: June 07, 2019].

[16] Hongkong & Shanghai Banking Corporation Holdings PLC, "Trust in Technology", 2017. [Online]. Available: http://www.hsbc.com/trust-in-technology-report. [Accessed: June 07, 2019].

[17] D. Folkinshteyn and M. Lennon, "Braving Bitcoin: A technology acceptance model (TAM) analysis", Journal of Information Technology Case and Application Research, vol. 18, no. 4, pp. 220–249, 2016.

[18] A. W. Baur, J. Bühler, M. Bick and C. S. Bonorden, "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co", in Lecture notes in computer science, Open and Big Data Management and Innovation, M. Janssen, M. Mäntymäki, J. Hidders, B. Klievink, W. Lamersdorf, B. van Loenen and A. Zuiderwijk, Eds., Cham: Springer International Publishing, pp. 63–80, 2015.

[19] J. M. Woodside, F. K. Augustine Jr. and W. Giberson, "Blockchain Technology Adoption Status and Strategies", Journal of International Technology and Information Management, vol. 26, no. 2, pp. 65–93, 2017.

[20] K. Francisco and D. Swanson, "The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency", Logistics, vol. 2, no. 1, 2018.

[21] M. M. Queiroz and S. Fosso Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA", International Journal of Information Management, vol. 46, pp. 70–82, 2019.

[22] A. Kumpajaya and W. Dhewanto, "The acceptance of Bitcoin in Indonesia: Extending TAM with IDT," Journal of Business and Management, vol. 4, no. 1, pp. 28–38, 2015.

[23] D. Montaño and D. Kasprzyk, "Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model", in Health behavior and health education: Theory, research, and practice, K. Glanz, B. K. Rimer, K. Viswanath and C. T. Orleans, Eds., 4th ed. San Francisco: Jossey-Bass, pp. 67–96, 2008.

[24] R. H. Fazio and T. Towles-Schwen, "The MODE model of attitude-behavior processes", in Dual-process theories in social psychology, S. Chaiken and Y. Trope, Eds., New York: Guilford Press, pp. 97–116, 1999.

[25] F. D. Davis, "A Technology Acceptance Model for Empirically Testing New End-User Information Systems". PhD [Dissertation]. Cambridge: Massachusetts Institute of Technology, 1985. [Online]. Available: https://www.researchgate.net/publication/35465050_A_Technology_Acceptance_Model_for_Empirically_Testing_New_End-User_Information_Systems. [Accessed: June 07, 2019].

[26] S. Kulviwat, G. C. Bruner II, A. Kumar, S. A. Nasco and T. Clark, "Toward a unified theory of consumer acceptance technology", Psychology & Marketing, vol. 24, no. 12, pp. 1059–1084, 2007.

[27] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989.

[28] V. Venkatesh and F. D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies", Management Science, vol. 46, no. 2, pp. 186–204, 2000.

[29] P. A. Pavlou, "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model", International Journal of Electronic Commerce, vol. 7, no. 3, pp. 101–134, 2003.

[30] K. Nærland, C. Müller-Bloch, R. Beck and S. Palmund, "Blockchain to Rule the Waves-Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments", in Proceedings of the 38th International Conference on Information Systems (ICIS), Seoul, South Korea, pp. 3885–3990, 2017.

[31] P. Legris, J. Ingham and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model", Information & Management, vol. 40, no. 3, pp. 191–204, 2003.

[32] K. Mathieson, "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior", Information Systems Research, vol. 2, no. 3, pp. 173–191, 1991.

[33] E. M. Rogers, "Diffusion of innovations", 5th ed., New York, London, Toronto, Sydney: Free Press, 2003.

[34] K. K. Kapoor, Y. K. Dwivedi and M. D. Williams, "Rogers' Innovation Adoption Attributes: A Systematic Review and Synthesis of Existing Research", Information Systems Management, vol. 31, no. 1, pp. 74–91, 2014.

[35] S. Chakrabarty, G. Brown and R. E. Widing, "The Effects of Perceived Customer Dependence on Salesperson Influence Strategies", Journal of Personal Selling & Sales Management, vol. 30, no. 4, pp. 327–341, 2010.

[36] R. Frey, D. Wörner and A. Ilic, "Collaborative Filtering on the Blockchain: A Secure Recommender System for e-Commerce", in Surfing the IT innovation wave: 22nd Americas Conference on Information Systems (AMCIS), San Diego, USA, pp. 1734–1738, 2016.

[37] N. Dodd, "The Social Life of Bitcoin", Theory, Culture & Society, vol. 35, no. 3, pp. 35–56, 2018.

[38] R. A. Bradley and M. E. Terry, "Rank Analysis of Incomplete Block Designs: I. The Method of Paired Comparisons", Biometrika, vol. 39, no. 3/4, pp. 324–345, 1952.

[39] R. D. Luce, "Individual choice behavior: A theoretical analysis", Mineola: Dover Publications, 2005.

[40] J. R. Rossiter, "The C-OAR-SE procedure for scale development in marketing", International Journal of Research in Marketing, vol. 19, no. 4, pp. 305–335, 2002.

[41] J. F. Hair, G. T. M. Hult, C. M. Ringle and M. Sarstedt, "A primer on partial least squares structural equation modeling (PLS-SEM)", 2nd ed., Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: Sage, 2017.

[42] K. Seaborn and D. I. Fels, "Gamification in theory and action: A survey", International Journal of Human-Computer Studies, vol. 74, pp. 14–31, 2015.

[43] P. Hassmen and D. P. Hunt, "Human Self-Assessment in Multiple-Choice Testing", Journal of Educational Measurement, vol. 31, no. 2, pp. 149–160, 1994.

[44] S. B. MacKenzie, P. M. Podsakoff and C. B. Jarvis, "The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions", The Journal of applied psychology, vol. 90, no. 4, pp. 710–730, 2005.

[45] J. Erbguth and G. Fasching, "Who is the Responsible Person of a Bitcoin Transaction? Applicability of the GDPR to the Bitcoin Blockchain". [Original title] "Wer ist Verantwortlicher einer Bitcoin-Transaktion? Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain", Zeitschrift für Datenschutz, vol. 7, no. 12, pp. 560–564, 2017.

[46] R. Böhme, N. Christin, B. Edelman and T. Moore, "Bitcoin: Economics, Technology, and Governance", Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–238, 2015.

[47] V. Venkatesh, "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model", Information Systems Research, vol. 11, no. 4, pp. 342–365, 2000.

[48] E. Aguirre, A. L. Roggeveen, D. Grewal and M. Wetzels, "The personalization-privacy paradox: implications for new media", Journal of Consumer Marketing, vol. 33, no. 2, pp. 98–110, 2016.

[49] O. Labazova, T. Dehling and A. Sunyaev, "From Hype to Reality: A Taxonomy of Blockchain Applications", in Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019), Wailea, USA, 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3250648. [Accessed: June 07, 2019].

[50] M. A. Khan and K. Salah, "IoT security: Review, Blockchain Solutions, and Open Challenges", Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[51] N. Kannengießer, S. Lins, T. Dehling and A. Sunyaev, "What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs", in Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019), Wailea, USA, 2018. [Online]. Available: https://www.researchgate.net/publication/327793246_What_Does_Not_Fit_Can_be_Made_to_Fit_Trade-Offs_in_Distributed_Ledger_Technology_Designs [Accessed: June 07, 2019].

[52] [Cited in the endnotes]. J. Kolla, "Decoding the evolution of Blockchain 3.0", 2018. [Online]. Available: https://www.livemint.com/Technology/OIb3LaLJ2pdwAGMRCiGLhI/Decoding-the-evolution-of-Blockchain-30.html. [Accessed: June 07, 2019].

[53] [Cited in the endnotes]. Federal Statistical Offices, "Welcome to the census database of the Census 2011. Dynamic and individual results", 2011. [Online]. Available: https://ergebnisse.zensus2011.de/?locale=en. [Accessed: July 04, 2019].

[54] [Cited in the endnotes]. K. Panetta, "5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies", 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/. [Accessed: June 07, 2019].

[55] [Cited in the appendix]. K. Sandberg and M. Overgaard, "Using the perceptual awareness scale (PAS)", in Behavioral Methods in Consciousness Research, M. Overgaard, Ed., Oxford: Oxford University Press, pp. 181–196, 2015.

[56] [Cited in the appendix]. G. C. Moore and I. Benbasat, "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation", Information Systems Research, vol. 2, no. 3, pp. 192–222, 1991

[i] This paper refers to "Blockchain technology", because most consumers are expected to be more familiar with the commonly used term "Blockchain" than with the more broadly defined, but much more abstract concept of "distributed ledgers". Anyhow, results might also be relevant for applications based on distributed ledgers that are not built on Blockchains.

[ii] Referring to a survey among German consumers by Yougov Deutschland GmbH, only 4% of consumers use the Internet to deal with cryptocurrencies like Bitcoin as the most commonly used Blockchain-based application among consumers [3]. The low percentage of users is replicated in the present study (3.2%, cf. part 5).

[iii] Besides payments based on cryptocurrencies, consumer-oriented apps relying on BCT already offer a wide range of services, for example, cloud or messaging services [52].

[iv] This evidence, which is discussed regularly under the heading of "Intention-Behaviour-Gap", can be traced back to various causes, e.g. unexpected problems or emotions occurring in real situations that have not been anticipated when hypothetically forming an intention [13].

[v] Many well-known acceptance theories and models like the "Unified Theory of Adoption and Usage of Technologies" (UTAUT) or the "Technical Acceptance Model" (TAM) use intention as an acceptance variable.

[vi] This does not imply that these processes need to be conscious or cannot include spontaneous components or emotions [13]. Anyhow, to explain spontaneously initiated and predominantly affective decisions to perform a behaviour of interest, the theory should not be used [24].

[vii] Alternatively, it can be interpreted as further Behavioural Belief, addicted to the expected outcome of trying out BCT.

[viii] The theory specifies four more beliefs ("Relative advantage", "Compatibility", "Complexity" and "Observability") that determine overall evaluation of an innovation that show analogies to PEOU (Complexity) or PU (Relative Advantage) and have been used for investigations until today, but are not significant in all applications [34]. In consequence, only Trialability is explicitly taken into account.

[ix] Authors discuss "Perceived customer dependence" from a sales perspective [35].

[x] 93.4% of the participants had a graduation qualifying for university entrance (for comparison with the German population, see [53]).

[xi] Reference technologies were selected comparing the "Hype Cycle for Emerging Technologies" of the consulting company "Gartner, Inc." from the years 2015 to 2017. The aim was to select emerging technologies in different stages of diffusion [54].

[xii] Earlier surveys focussing the Bitcoin Blockchain yield a negative correlation between age and awareness as well as between age and usage (intention) [14, 15], which can broadly be replicated by the present data (r (Spearman rank coefficient) of age and awareness = 0,24, $p < 0.05$; r (rank coefficient) of age and usage intention = -0,16 ($p < 0.1$)).

[xiii] But interestingly eleven declare to actually own or have owned

cryptocurrencies (and only four of these eleven seem to be aware of the fact that they thereby use BCT), which indicates that cryptocurrencies and BCT are not necessarily connected in consumers' perception. Because respondents were further asked to specify the cryptocurrencies they own and all stating to own some have Bitcoin or Ether as Blockchain-based cryptocurrencies in their portfolio, this can definitely not be a sophisticated statement based on the fact that not all cryptocurrencies are based on Blockchains. Anyhow, a generalisation of this incident is not possible due to the low numbers of users participating in the survey.

[xiv] The higher an item's weighting factor, that can be interpreted as regression coefficient [44], the more it determines the influence of the corresponding latent variable on others (and ultimately on Usage Intention).

[xv] The classification assumes a normal distribution based on earlier research and is not completely sharp because of "innovativeness" being a continuous variable [33]. Anyhow, it allows a rough estimation of the percentage that different Adopter Types represent in the population.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
None declared.

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(7)2020

Distributed Ledger Technologies and the Internet of Things: A Devices Attestation System for Smart Cities

Evandro Pioli Moro and Alistair Keith Duke
Department of Applied Research, British Telecommunications, UK
Correspondence: evandro.moro@bt.com

Received: 15 January 2020 **Accepted:** 16 March 2020 **Published:** 03 April 2020

Abstract

Traditional IT security mechanisms are generally not well suited for IoT devices, where processing and network connectivity should be kept to a minimum. Consequently, IoT devices have been recently identified as an easy target for cyber-attacks, like for example on the Mirai botnet Distributed Denial of Service attacks in 2016, where various devices were hacked into and taken over. Different solutions have been developed aiming at guaranteeing the security at both the device application layer and the network layer. Few succeeded to deliver the flexibility necessary for IoT devices. Even fewer have implemented an effective threats detection system, and just a handful have realised all the previous features in a fully decentralised fashion, including this one. This Distributed Ledger Technology (DLT) attestation system is maintained and supported by most, or all, IoT devices because it is based on a light-weight DLT protocol. It comprises of a system for authorisation and authentication for the individual devices as well as includes an anomalies detection system based on smart contracts. A demonstration was built to support a Smart City use case. The objective is to guarantee, in a decentralised manner, the security of low computational power devices executing the sensing function and their connectivity, and therefore the correct functioning of the system. On the demonstrator, the system was run using DLT supported by the sensors connectivity bridge (built using Raspberry Pi's). The system proved to be rapid to develop, flexible with regard to systems changes and resilient to attacks to both individual IoT devices and to the DLT.

Keywords: *Internet of Things, Distributed Ledger Technologies, Blockchain, Attestation, Smart Cities*

JEL Classifications: *H00, L22, L60, L86, M1, O32, P11, R00, Z13*

1. Introduction

a. Internet of Things

First deployed during the Second World War by the Royal Air Force for assets identification [1], radio frequency identification (RFID) tags are nowadays widely used by retailers to replace bar codes of products or to prevent shoplifting. In October 2003, during the McCormick Place conference in Chicago, USA, retail, technology and academic partners realised a local network including connected products using RFID tags. Because this network involved tracing and gathering information about different things in real time, it was called *internet of things* [3].

Now that more than a decade has passed since the McCormick Place conference, the Internet of Things (IoT) remains a technology model under development and it is expanding rapidly across different sectors. The definition of IoT has gained a more comprehensive shape, now being defined as the collection of various devices, as opposed to only RFID tags, which are able to produce data and are inter-connected over the Internet [4].

According to recent studies, the number of Internet connected devices is expected to reach 34mi by the end of 2020 [5]. A great part of this explosion in numbers is due to the deployment of an ever-growing amount of different IoT devices. Devices that traditionally were not connected to the Internet, like utility meters, cameras and various sensors, are now being provided with Internet connection and are sharing data on the web. The estimated economic impact of the IoT applications across sectors like homes, offices, health, cities and other, is estimated to going to be at least £2.2tn per year by 2025, with confident forecasts predicting an economic impact of up to £9tn per year [6].
An example of an application of IoT is to enable intelligent cities. If data about air quality, traffic, buses and trains real time schedule, electricity production and consumption, cycling experience and car parking occupancy is produced in real time, applications like smart people routing, intelligent energy management and air quality enhancement policies can be implemented, making commute in big cities easier, improving the air quality and energy efficiency, and enhancing road safety.

The general idea of the IoT is to bring the right information to the right people at the right time. On an IoT system, information about different environments are collected and delivered in a relevant and secure way to the end users. In between the measured environments and the information consumption, four layers of infrastructure exist: the sensors, the connectivity, the information exchange and the application layers. Figure 1 depicts this architecture with examples of some possible components on each of them.

On the next page of Figure 1, different environments are conceived, representing various eco-systems where IoT services are intended to be provided. The first layer of the IoT architecture, called sensors layer, is comprised of the various sensors deployed. These sensors are used to produce data from different sources and are provided with Internet connection, which builds the second layer of the structure: the connectivity layer. At the connectivity layer, the data is transported from the sensors to an information exchange centre by different technologies, which are dependent on the application requirements. It can be over a Wireless Local Area Network (LAN), or Wi-Fi, connection if the sensors and the environment are close to each other, like for example on a smart home or factory; or it can be over a 4G or 5G connection if the application requires wider band or faster actuation time. Yet another example largely used for narrow bandwidth and low power consuming communications provision is the LoRa WAN (Long Range Wide Area Network) technology.

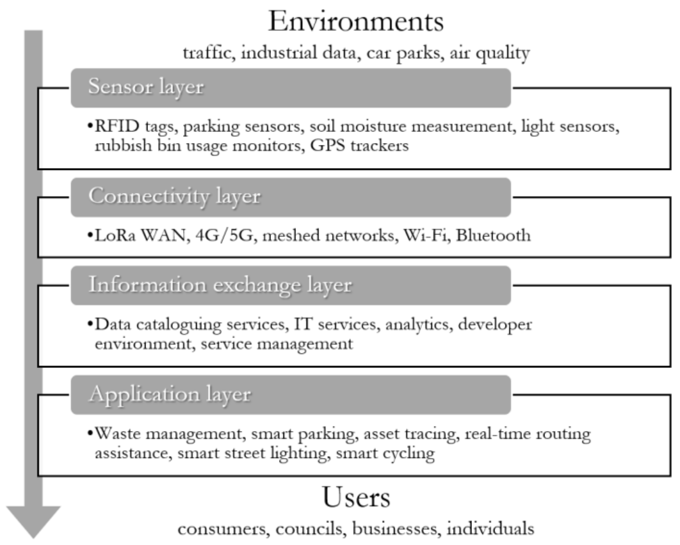

Environments
traffic, industrial data, car parks, air quality
Sensor layer
•RFID tags, parking sensors, soil moisture measurement, light sensors, rubbish bin usage monitors, GPS trackers
Connectivity layer
•LoRa WAN, 4G/5G, meshed networks, Wi-Fi, Bluetooth
Information exchange layer
•Data cataloguing services, IT services, analytics, developer environment, service management
Application layer
•Waste management, smart parking, asset tracing, real-time routing assistance, smart street lighting, smart cycling
Users
consumers, councils, businesses, individuals

Figure 1. High level architecture of a typical Internet of Things system

LoRa WAN is preferred for applications like smart solar panels within a campus, where only small data packets need to be exchanged in a power-efficient way. The third level, the information exchange layer, is where the data is stored, processed and shared across different parties. Here, the data is made uniform to be exposed and consumed, providing the ability for IoT data consuming applications to be developed rapidly. This is also where the data access policy is implemented and where the applications are provided with specific ways for interacting with the data, for example being provided with a uniform application programming interface for data input and consumption. The application layer, at the bottom of Figure 1, and is the one responsible for delivering the information to the end users in the most appropriate manner. The end users are the IoT information consumers, for example, cyclists, commuters, councils, banks or any relevant IoT information consumer.

b. Distributed Ledger Technologies

Distributed Ledger Technology (DLT) is a peer-to-peer networking system where the exact copy of a transactions ledger is shared, supported and trusted by all peers (nodes), without having to rely on a central authority [7]. If the transactions of the network are organised in the form of blocks of information, containing among the transactions, other identifiers, in such a way that one block is generated at every determined period of time and the blocks are linked (chained) to the previous ones, then the DLT is called *blockchain* [8].

Information stored on the DLT can be trusted by design because it has to undergo a decentralised and fair consensus algorithm. A consensus algorithm is a computational process by which the network collectively agrees on a single source of truth by determining which transactions are to be added to the ledger via a series of verifications. This algorithm is usually also used to decide which computing peer will be the sealing node, the node responsible to update the ledger with the newer transactions and to broadcast the newly created block to the other peers. Usually, the fairer the network is, the less repetition and predictability of sealing nodes there will be. Different consensus algorithms exist, depending on the type of blockchain and on the requirements of the use cases. For example, the Bitcoin network, where heavier requirements for security must be put in place, the proof-of-work was the chosen consensus algorithm. If an enterprise-level blockchain is designed, a more flexible consensus algorithm may be adopted, like, for example, the proof-of-authority or proof-of-stake types.

Another important feature of modern blockchain protocols is the implementation of smart contracts. Smart contracts are pieces of code executed in a decentralised fashion by all nodes of the network. They provide programmability to the system, are able to react to inputs and to the blockchain state and produce the program output at all nodes for the system. Smart contracts are pieces of code triggered either by conditions set, i.e. reacting to a certain blockchain state, or by a call from any node via a transaction [9]. They can perform various functions in a blockchain system, e.g. enabling an agreement between two or more parties, to provide virtual identities for devices, to check authorisation of nodes, to transfer digital assets, among others.

Since smart contracts reside on the blockchain, they must have an associated address, which is used to collect the funds in exchange of their execution. Moreover, smart contract scripts are inheritably deterministic, meaning that it will always provide the same outputs for the same inputs. Furthermore, all interactions with the smart contract will be supported by cryptographically signed messages registered on the ledger, meaning all smart contract interactions are traceable and auditable [13]. These factors are what make smart contracts so important for current distributed ledgers implementations.

In order to evaluate the benefits of immutable DLTs for any information technology (IT) project, five key dimensions should be evaluated in order to avoid falling into the technology hype:

- Does the project require an immutable ledger, where data cannot be deleted or updated?

This is primarily concerned with the IT challenge of access to historical data for system processes. Since blockchains structure the data in such a way that information cannot be changed, thanks to its hashing algorithm implementation, deletion or change of data in the ledger is very complicated and energy consuming. At DLTs, the information is generally stored in a way such that it contains one field storing a reference to a series of previous transactions bundled together. In blockchains, this reference is usually implemented at block level as the hash output of all the previous blocks bundled together to generate the hash output. This means that in order to change or tamper with one or more transactions on any block, a new recalculation of the entire blockchain is necessary, requiring an immense computational cost and a prolonged time. This makes changes to the ledger generally an impractical task.

- Do the interested parties need access to a single and trusted source of truth?

This is primarily concerned with the IT challenge of access to true information for processes. DLT is a repository of transactions and data which is synchronized, shared and supported by peers without the requirement of a central authority mediation. Usually guaranteed by the network consensus algorithm, DLTs assure all peers of the network trust on the data stored on the ledger. All nodes have a local and synchronised copy of the ledger of transactions and can fetch any transaction or provide access means to non-peer users at any time, representing an attractive technology candidate for IT projects where various parties need to access a singular repository of data which all can inheritably trust in order to convey truthful information.

- Is an independent and cryptographic audit trail required for the use case, e.g. to prove identity, state or provenance of an asset?

This is primarily concerned with the IT challenge of access to data for audit purposes. DLTs process transactions using uniquely referenced signatures for peers based on enhanced cryptographic protocols. Furthermore, all the history of actions of the unique signatures is stored on the immutable ledger. Hence, provided DLTs are powerful tools to store immutable and historical data and are a trusted source of information to all peers, it proves to be a strong technology candidate to power audit trails IT systems.

- Does the system have good reasons for not putting a centralised utility in place or to have a single entity in control of the architecture activities?

This is primarily concerned with IT systems which are by nature, or need to be, decentralised. DLTs are systems that enable trust, immutable information and audit trails in a decentralized fashion. In general, the consensus algorithms for a DLT require a plurality of peers to be effective, meaning that it is designed to enable access to decentralised, and trusted information provided multiple parties participate in the system. If this is the case, and there are reasons for not having an authority, or a peer, with elevated control of the network activities, DLTs are a candidate technology to enable trust on the data when there is no central authority in place. This is often referred as the trustless feature of DLTs.

- Does the interest of the parties lie on the success of the system, to keep its distinct characteristics?

As explored previously, DLTs can adopt different types of consensus algorithms, depending on the use case requirements. After all, a DLT system will only make sense for any application if the previously explored characteristics will add value to the IT project and if the participants are interested in keeping these distinct characteristics. This is especially true for enterprise DLTs, where the levels of computational power requirements might need to be reduced, provided the parties are interested in participating fairly on the system. If this is not true, then the computational requirements for a proof-of-work type of consensus algorithm may be prohibitive.

2. Blockchain transactions verification process

General blockchain algorithms implement a recursive and powerful transaction verification process to guarantee that no malicious transactions are sent. Currently, the systems verify for double spending problems (if a user is trying to send the same funds twice in subsequent transactions), verifies the existence of the receiving account, checks for enough funds on the sending account and verifies the key of the sending node (to check if the sending node is the same as the one that signed the transaction). However, there are other fields on a blockchain transaction which are not verified before they are fully processed by the network, including the transaction data field. This data field can be used, for example, as an identifier of the transaction (like reference numbers of bank transfers) or parameters for a smart contract function call (the arguments of the code functions).

One of the ways of invoking a smart contract is through DLT transactions. This is accomplished by sending a transaction of funds in exchange for the code execution efforts. It is therefore important that when a peer is invoking a smart contract with arguments sent in the transaction data field that this is accurate and verified for the system safety. Of more important here is that this is verified in a use case-dependent manner, for instance, if a smart city application is concerned, the sensors data sent across the transaction data field on a blockchain transaction should be accurate.

Therefore, verifying the transaction data field before the transaction is processed by the network can save execution time, and it also helps to reduce the risks of deceptive invoking of smart contracts from happening, hence improving the value of an IoT solution. Moreover, if this verification is flexible enough to perform checks that are relevant to the DLT use case, for example, if it is able to verify that the arguments of the smart contract invoked are pertinent, the aggregated value of this solution for the network is even greater.

3. Internet of Things devices security

Because of the unprecedented increase in the number of IoT devices over the past decade and the growing importance of IoT in IT infrastructures, ensuring the security of IoT devices is at the centre of numerous research projects of the Information and Communications Technology (ICT) industry and academia, and a valuable market niche. It is estimated that the aggregated spending in IoT security measurements has been £780mi in 2018 and it is estimated that it will be four times bigger in 2022 [10].

The design constraints and low computational power of these devices can make them an easy target for cyber-attacks, as it happened in August 2016 with the Mirai botnet attack. The Mirai botnet was a malicious piece of software released to take control of devices like web cameras and digital video recorders running a specific version of a light-weight operational system. From these devices, the botnet took control of other IoT devices connected nearby, causing a big Distributed Denial of Service (DDoS) [11]. Since August 2016, other types of IoT devices were infected in various attacks of the world, exposing the need to increase the security of IoT devices.

Traditional IT security mechanisms designed for computers, servers and systems are based on a three-layer defence structure: static perimeter network layer (i.e. firewalls, intruder detection systems), end-host defence tools (e.g. antivirus software) and software patches (i.e. re-deployment of security packages on a regular basis) [12]. This traditional security structure is not well suited to IoT devices, where software processing and network communications should be kept at a minimum. More specifically, different use cases require different types of IoT structures and security levels; thus, generic IT security systems are difficult to implement for these cases and are often not flexible enough. For instance, a mobile phone application which controls IoT devices via different channels and an IoT ecosystem where one device can affect both its concerned application and another IoT device, require different types of perimeter, end-host and patch security measurements. Moreover, the constrained hardware and software on-boarded to an IoT device reduce their ability to run mechanisms to detect anomalies on the network traffic and to perform complex signature protocols. Furthermore, because IoT devices will often tie the sensing and connectivity layer activities together, and in some cases will also respond with actuation, effectively providing application interface and traditional perimeter defence mechanisms are not efficient. Finally, yet importantly, considering these devices do not run full operating systems, the traditional end-host tools and patching will not work as effectively as they would on traditional IT systems.

In sum, there are two key points to highlight as main network security issues around IoT: end-host defence tools (like antivirus or software-based anomaly detection systems) are not feasible, once the devices are restricted in resources, and traditional static perimeter mechanisms are not as straight-forward as they are for traditional IT systems because these devices are deployed deeper into the network, with their physical and computational behaviour constantly changing.

4. IoT Devices Attestation System for Smart Cities

The solution comprises of a DLT, herein described as a blockchain system with a proof-of-authority type of consensus algorithm, which is used as a registry of IoT data transactions as well as a repository of device profiles, containing, but not limited to, their expected behavior, their system authorisations and an actions registry. These transactions can be the purchase or selling of data feeds, e.g. councils selling air quality information to an IoT service provider, or simply a commit of data regarding a smart utility meter, as a blockchain transaction to a smart contract, for instance.
The selection of the blockchain nodes is flexible. The nodes can be deployed into the IoT edge computing devices, with a mixture of light and full nodes (if the blockchain infrastructure is light enough to support such

a development); it can also be on the servers of the IoT service provider (in a cloud type infrastructure), since they usually have more storage and processing capabilities; it can be a set of trusted and bespoke computing nodes for the application; alternatively, it might also be a public and shared infrastructure (as long as it is compliant with the use case privacy requirements).

The generic architecture of the solution comprises of an IoT ecosystem together with a blockchain backend to provide an anomaly detection system based on smart contracts. The solution accomplishes this by introducing a mechanism capable of inspecting the data field of the blockchain transactions in real time. This can be implemented as an interface, for example an application programming interface (API), to compare the data sent within a transaction with the device expected behavioural data stored in the relevant smart contract. This provides unexpected behaviour detection if one or more IoT devices are compromised, once the registry on the blockchain cannot be changed, are trusted by nature and provide any party on the IoT ecosystem with the ability to check if the current behaviour of the devices is correct according to the device role, profile or expected behaviour. This is designed to provide near real-time information about intrusions, attacks, data tampering or device failures.

In a simple example, represented in Figure 2, suppose a town council is building a smart city ecosystem which comprises of, amongst other sub-systems, an air quality monitoring system. During the system set-up, the town council sets out the expected gas levels to be a given maximum which are then registered as one of the expected behaviour parameters inside the concerned smart contract within the blockchain of cloud-type. Other parameters can be, for example, frequency of data updates, usual data packet size exchanged, and others. Because these parameters reside on the blockchain, they are immutable and shared across all the peers of the blockchain network. When the system starts operations, the air quality information flows from the air quality sensor, to the left of the diagram, to the town council, to the right of the diagram, via the transaction data inspection interface and the blockchain system. This inspection interface serves the purpose of allowing the system to verify the data sent by sensors against the expected devices behaviour parameters residing at the smart contract. As the second step on this information flow, the sensor data is registered on the blockchain for the purposes of anomaly detection. With the aid of the data inspection interface introduced, the relevant smart contracts can process the transaction data sent to another party against the expected parameters and flag a malfunctioning device. This system will then flag the device for further investigation, and depending on the system design choices, can halt the sensors' activities remotely by changing its authorisation parameters on another smart contract.

On the system described, IoT transactions are completed via the blockchain system with the aid of smart contracts. In order to provide full integration of the IoT ecosystem with the blockchain, lightweight APIs were developed. By using these APIs, the devices are locally provided with the ability to commit sensor readings and, more importantly, to verify other devices' integrity. The system is also capable of providing signature verification and implementing identity provisioning mechanisms if required to build a comprehensive authentication, authorization, and accounting (AAA) system. In case devices are flagged as malfunctioning, the system manager can halt their actions on the system by changing their authorisation parameter on the AAA agreement until they are fully recovered. Alternatively, the system can impede the compromised device to ever participate again, by revoking its identity on the blockchain, which represents a ban on the unique device signature.

In an alternative setting, the system can detect anomalies independently, meaning the IoT devices when transacting via the distributed ledger will be able to independently verify the transactions. On a generic setting, the IoT sensors participating on a typical IoT system are comprised also of a blockchain to actively trade data. This system is distributed and does not require a central authority to process the transfers, nor to verify and detect anomalies on the data transacted. Figure 3 depicts this setting, where a smart utility meter replicating the blockchain represents the data purchaser and can make calls to a transaction verification interface, which can run locally, to perform the checks on the data field of the blockchain transactions. The transaction verification interface will enable the data consumer to compare the transaction data against the device expected behaviour registered on the DLT shared across all IoT devices, including the smart utility meter. This is essential in keeping the system safe from failures and is accomplished in a distributed fashion, happening automatically.

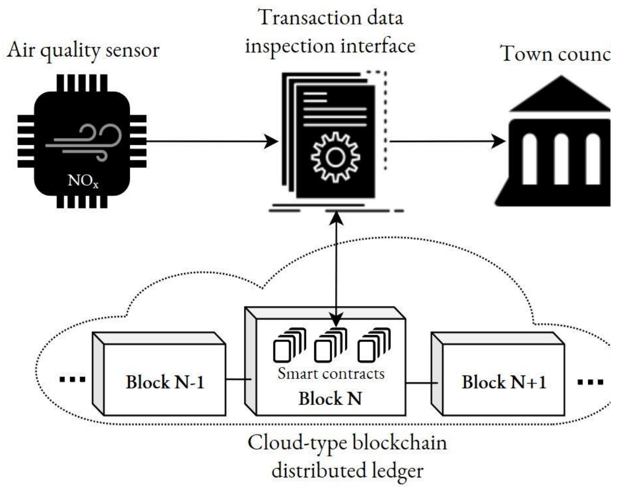

Air quality sensor
NOx
Transaction data inspection interface
Town counc
...
Block N-1
Smart contracts
Block N
Block N+1
...
Cloud-type blockchain distributed ledger

Figure 2. Example application of the IoT devices attestation system based on a cloud type blockchain and a set of relevant smart contracts.

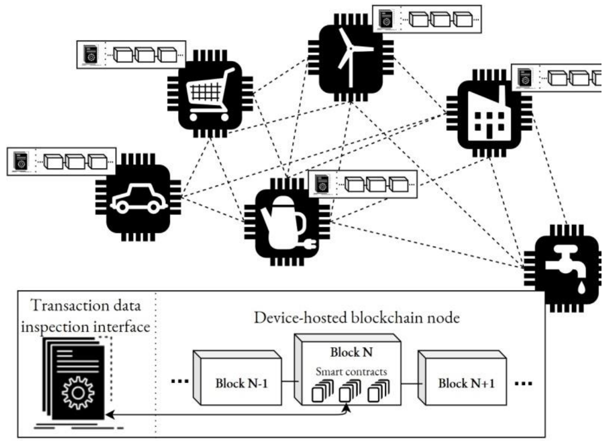

Transaction data inspection interface
Device-hosted blockchain node
...
Block N-1
Block N
Smart contracts
Block N+1
...

Figure 3. Generic architecture diagram of the solution proposed for deployment at the IoT devices with edge computing capabilities.

5. Analysis

This solution leverages from the decentralisation feature of blockchain to implement a detection system that is independent of a central authority and which can still be trusted by any peer on the network even when they do not have an established trust relationship with each other. v

This system does not implement end host software in order to allow for maximum performance of the constrained IoT devices. On the other hand, the system implements a strong perimeter network layer protection, by using blockchain smart contracts to interface the IoT transactions while verifying for anomalies. This network layer protection provides means to detect attacks to IoT devices and measurements to reverse them, as well as to provide preventive actions against malfunctioning devices. Additionally, the solution is flexible and agile. Although immutable by nature, new smart contracts can be deployed to all peers quickly and therefore updates about the network operation to cover for new devices expected behaviours can be quickly put in place.

This solution helps adding value to the IoT by realising a decentralised, auditable and trusted devices attestation system. With a light-weight and flexible implementation of DLTs, the solution enhances the trust on the data shared on the IoT, enabling a use case of DLTs as a platform of trust.

6. Conclusion

The rapid development of the IoT over the past decade brought many different applications to life and truly revolutionised the way society lives and consumes data. It made cities smarter, helping to improve the way people commute, made energy more flexible, helping to take down barriers of energy trading, helped councils to save tax payer money by pre-empting road quality issues, among other many applications. At the same time, this quick deployment of millions of low processing power devices revealed the need of to increase device and networking security for the IoT.

The blockchain technology, conceptualised in the early 1980s but only first implemented in 2009 [14], truly revolutionised the way information can be trusted without relying on a central authority. This technology has already been adopted by different sectors to enhance security over transactions. Banks, insurance providers, aircraft manufacturers, and others, leveraged this technology to provide assurance over their data, avoiding the risks of having divergent information and to enable trusted systems and agreements without the central authorities' instrumentation.

The need to improve the technological architecture of blockchain protocols for specific use cases together with the need of increasing the security of IoT devices, has broached an interesting research topic. The solution proposed comprised of a blockchain system serving the purpose of providing an IoT system with predictive failure and attack detection capabilities, by monitoring the information exchanged by the devices against their designed role on the system.

The synergy between IoT and DLTs is believed to still be in its infancy. DLT has already been proven to be efficient in addressing issues around trust and security of ICT data. It is important to realise that, although blockchain technologies help to solve various issues faced by ICT systems, it still has its own challenges such as relatively high computing processing and large data storage demands, if not carefully designed. Considering these limitations and analysing the benefits is of ultimate necessity when designing a DLT system for the IoT, which demands rapid and trustworthy information exchange. The solution presented in this report is flexible with regard to the type of DLT and is designed to be quickly adapted to newer types of DLTs, regardless of their design.

Nonetheless, it is believed that DLTs are still in the early days of its development, with immense potential to continue revolutionising the way information is stored, shared, audited and trusted. The IoT is one of the biggest potential beneficiaries of this new technology, since it requires trustworthiness on the information it processes, usually in a decentralized way. Developing a powerful interconnection between these two technologies represents a demanded enhancement on IoT systems security and it is therefore expected to bring new business models and to drive changes across many of the existing systems and processes, helping to deliver greater value to the Internet of Things.

References:

[1] Dodson, S. (2003). The internet of things. [online] The Guardian. Available at: https://www.theguardian.com/technology/2003/oct/09/shopping.newmedia [Accessed 24 May 2019].

[2] Bonsor, K. and Fenlon, W. (2019). How RFID Works. [online] HowStuffWorks. Available at: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm [Accessed 24 May 2019].

[3] Sundmaeker, H., Guillemin, P., Friess, P. and Woelfflé, S. (2010). Vision and Challenges for Realising the Internet of Things. Brussels: European Commission - Information Society and Media DG, p.12.

[4] Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey, Computer Networks, Volume 54, Issue 15, 2010, Pages 2787-2805, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2010.05.010.

[5] Business Insider. (2019). BI Intelligence projects 34 billion devices will be connected by 2020. [online] Available at: https://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11?r=US&IR=T [Accessed 8 Feb. 2019].

[6] Colin Tankard, The security issues of the Internet of Things, Computer Fraud & Security, Volume 2015, Issue 9, 2015, Pages 11-14, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(15)30084-1.

[7] Iansiti, M. and Lakhani, K. (2017). The Truth About Blockchain. Harvard Business Review, R1701J, pp.4-5.

[8] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, 2016, pp. 1392-1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198

[9] Sun, J., Yan, J. and Zhang, K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1).

[10] IOT Analytics. (2017). IoT Security Market Report 2017-2022. IoT Analytics. Retrieved from https://iot-analytics.com/product/iot-security-market-report-2017-22/

[11] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-5. doi: 10.1109/CCWC.2017.7868464

[12] Yu, T., Sekar, V., Seshan, S., Agarwal, Y. and Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices. Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016. doi: 10.1109/ACCESS.2016.2566339

[14] Luther, W. (2016). Bitcoin and the Future of Digital Payments. The Independent Review, 20(3), 397-404. Retrieved from www.jstor.org/stable/24562161

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Evandro Pioli Moro is the author. Alistair Keith Duke proof read the article.

Funding:
None declared.

Acknowledgements:
I would like to thank Prof John Davies for the research leadership within the team as well as Dr Alistair Duke for the daily support on my projects.

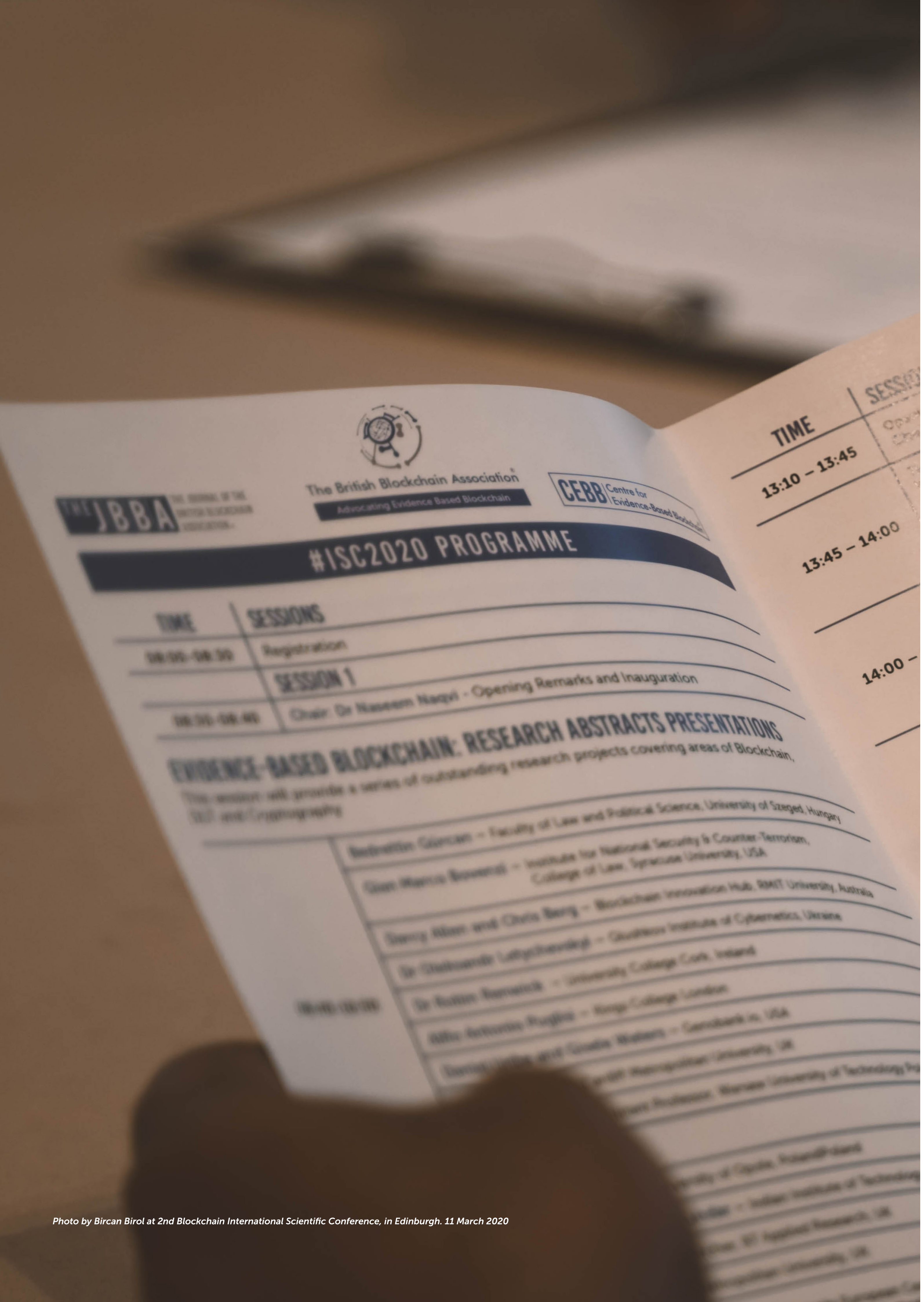

THE JBBA
The British Blockchain Association
Advocating Evidence Based Blockchain
CEBB Centre for Evidence-Based Blockchain
#ISC2020 PROGRAMME
TIME
SESSIONS
Registration
SESSION 1
Chair: Dr Naseem Naqvi - Opening Remarks and Inauguration
EVIDENCE-BASED BLOCKCHAIN: RESEARCH ABSTRACTS PRESENTATIONS
TIME
13:10 – 13:45
13:45 – 14:00
14:00 –

Photo by Bircan Birol at 2nd Blockchain International Scientific Conference, in Edinburgh. 11 March 2020

CONFERENCE PROCEEDINGS

2nd Blockchain International Scientific Conference 11 March 2020, Edinburgh

1. Cryptocurrencies And Cyberlaundering: The Need For Regulation

Gian Marco Bovenzi
Syracuse University College of Law, USA
Category: Oral Presentation

Abstract

Data show that cyber organized crime was beyond 39% of global cyber breaches in 2018, with peaks of 70% in 2011 and 80% in 2015. In addition, 46% of Bitcoin transactions involve illegal activities (for an estimated value of $76 billion) and cryptomining is the motive of 30% of security breaches. Given this alarming scenario, the objective of this paper is to stress the urgent need for governments to enhance regulations specifically addressing the issue of cryptocurrencies exploitation for cyberlaundering purposes. Criminal organizations historically breathe through money laundering, and according to scholars and media reporting they currently might find in cryptoassets fertile grounds for their aims of financial gain. The anonymity underlying blockchain causes indeed serious biases to investigations, as encryption represents a challenge for law enforcement officers in linking transactions to physical identities. Adopting a comparative legal analysis methodology, the paper will assess the current global legal framework underlining its positive outcomes, its deficiencies, and what is yet to be done. This paper concludes pointing out two possible solutions: first, the implementation of international instruments of cooperation is crucial, given the transnational and cross-border nature of organized crime. Considering sovereign States' hesitancy in adopting globally accepted protocols or treaties, bi- or multi-lateral agreements might represent a temporary solution. Second, governments should tailor their national legal and policy frameworks focusing on cyberlaundering prevention, such as cash control or limitation of fund transfers for single users, or ensuring methods of identification such as mandatory registration of users.

Keywords: *Cryptocurrencies, cyberlaundering, organized crime, money laundering, blockchain*
Themes: *Cyberlaundering, organized crime, cryptocurrencies*

2. Jurisdiction on the Blockchain

Bedrettin Gürcan
University of Szeged Faculty of Law and Political Science, Hungary
Category: Oral Presentation

Abstract

Blockchain technology brings several services to our daily and business life. Its impact on the business culture, moral of the law and the data security has been discussing since the blockchain technology has been emerged. In this paper, we will discuss the jurisdiction of the blockchain technology. Blockchain was developed through the combination of several technologies including peer-to peer networks, asymmetric (public key) cryptography, time stamping, and the proof of work consensus mechanism. Blockchain provides an infrastructure for smart contracts to be executed in decentralized, without 3rd party presence.

Business transactions on the blockchain is completely independent from the location where parties of the legal entities located. Some challenges are decentralized storage of large computer networks, anonymity of the parties, and unspecified values exchanged where it is not sure it these "goods" are included United Nations Convention on Contracts for the International Sale of Goods. (CISG). With the developments of smart contracts, parties can devise mechanism whereby disputes on the agreement can be resolved by private adjudicators through self-enforcing decisions, the enactment of which does not depend on state controlled recognition and enforcement procedures.

3. 5 W's of Workers Compensation insurance, compliance and fraud

Srinivas Ratnam
Andhra University College of Engineering, Vizag, India
Category: Oral Presentation

Abstract

Workers compensation is type of insurance that grants benefits to injured worker who are injured on the lines of the duty. Quantum of benefits such as payment of bills/providing medical care vary depending upon the premium purchased. Employers participate in this program by law or to protect themselves from lawsuit in case of worker going legally against them. Workers Compensation Insurance benefits both employer (to protect their business against lawsuit) and employee/worker (to get benefits related to injury at worksite). In order for all the involved parties to be protected under the Workers compensation Insurance benefits or from liability benefits, they have to be in compliance with the state law. But due to the existing and disconnected parading of people/process/processors/information asymmetry, many frauds are taking place by involved stakeholders such as Insurance leakage/underwriter leakage due to people/process, submitting false claims due to people/processors and many more. The impact of being non-compliant and committing fraud leads to heavy cost of premium, higher medical care cost and so on. This paper attempts to address 5 W's (WHO, WHAT, WHEN, WHERE, WHY) of workers compensation insurance, compliance and various source of frauds and how state-of-the-art technology such as Blockchain, Artificial Intelligent, IoT, Virtual Agents can address such problems by focusing on Aviation industry and Independent contractors and the rush in adopting Blockchain/AI. This report provides statistics on insurance fraud, fraud indicators and so on. This paper also addresses various ways to protect environment by reducing massive consumption of papers. Keywords: Blockchain, Artificial Intelligent, IoT, Virtual Agents, Workers compensation insurance intermediation, monitoring the monitor Themes: blockchain, information asymmetry

4. The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework

Robert E. Campbell, Sr.
Capitol Technology University, USA
Category: Oral Presentation

Abstract

Critical infrastructure sectors are increasingly adopting enterprise distributed ledgers (DLs) to host long-term assets,systems, and information that is considered vital to an organization's ability to operate without clear or public plans and strategies to migrate safely and timely to post-quantum cryptography (PQC). A quantum computer (QC) compromised DL would allow eavesdropping, unauthorized client authentication, signed malware, cloak-in encrypted session, a man-in-themiddle attack (MITM), forged documents, and emails. These attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. In 2018, Gartner revealed that a QC is a digital disruption that organizations may not be ready and prepared for, and CIOs may not see it coming.1 On September 18, 2019, IBM announced that the largest universal QC for commercial use would be available in October 2019.2 On October 23, 2019, Google officially announced "Quantum Supremacy," "by performing a calculation in 200 seconds that would take a classical supercomputer approximately 10,000 years."3 DL cyber resilience requires "reasonable" measures, policies, procedures, strategies, and risk management before large-scale deployment. Cyber resilience implementations must be a critical component during the design and building phase, or during the initialization phase. The most significant existing attack vector for enterprise DLs is the public key infrastructure (PKI), which is fundamental in securing the Internet and enterprise DLs and is a core component of authentication, data confidentiality, and data and system integrity [1] [2]. Effectively implementing and managing a quantum-resistant PKI solution requires adherence to PKI standards, industry requirements, potential government mandates, certificate management policies, training personnel, and data recovery policies that currently do not exist. This research discusses security risks in enterprise DL PKI, areas that can be compromised, and provides an idea of what should be in a PKI DL Risk Management Framework plan.

Keywords: *cyber resilience, PKI, quantum computing, distributed ledger, cyberattack, risk management framework, hyperledger fabric*

5. Blockchain Governance: What we can learn from the Economics of Corporate Governance

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

Abstract

Understanding blockchain governance is urgent. This paper uses the transaction cost economics of governance to identify and clarify the tradeoffs that projects make when they are designing blockchain governance systems. Blockchain governance is the processes by which stakeholders – all those are affected by and can affect the network – exercise bargaining power over the network itself. But blockchains interact with, and are shaped by, external institutional frameworks (such as firms who act as institutional investors for tokens, firms that provide exchange services, and governments who regulate on-ramps to the network). Bargaining power in blockchain governance is shaped by 1) the distribution of bargaining power endogenous to the consensus mechanism, 2) exogenous governance structures built on top of an instrumental consensus mechanism, and 3) the needs of bootstrapping. Each impose contradictory pressures towards and against decentralisation. The paper argues that blockchain governance is a specific instance of the general category of the governance of decentralised economic organisation, from protocol decision-making processes, to the organisation of blockchain foundations, to the structures of decentralised autonomous organisations built as applications on top of the blockchain protocol, to the coordination of business consortia that data on a blockchain network. Approaches to governance design in blockchain systems are infused with normative beliefs about the institutional systems outside the blockchain space. We map this against a subjective institutional possibility frontier, offering a framework whereby the tradeoffs for different approaches to blockchain governance can be examined.

Keywords: *governance, blockchain, transaction cost economics, stakeholders, protocol*

6. Are Blockchain based systems the future of Project Management? A preliminary exploration

Robin Renwick
Cork University Business School, University College Cork, Ireland
Category: Oral Presentation

Abstract

Modern institutions are increasingly organized around the fulfilment of discrete goal-specific projects.Correspondingly, the scale, complexity, and diversity of actors involved in projects has also increased. Fortunately, a range of tools and technologies exist to support contemporary project management. The quality and fit of these tools is key to making sure projects remain successful. It is not yet clear whether incremental change and development of these tools is capable of keeping up with growing demands and evolving organisations; tasks involving disparate departments, members, and stakeholders with varying interests and priorities. Many issues with existing tools revolve around scale, trust, and valuation - leading to stratification as preferences appear for any number or combination of proprietary systems. Blockchain technologies may provide support for a new wave of project management systems, allowing managers a new range of capability and feature sets to aid their praxis. This paper presents an explorative case-study, in which open ended interviews are conducted with practicing project managers. Interviews are analysed to understand issues that exist with the currently deployed tools and technologies. Five constructs emerge: transparency, control, dynamic status updating, incentives, and trust. Feedback suggests blockchain-based alternatives could offer significantly better performance on each of these constructs.

Keywords: *blockchain, project management, trust, distributed ledgers, qualitative research*

7. Browser-based crypto mining and EU data protection and privacy law: a critical assessment and possible opportunities for the monetisation for web services

C.F. Mondschein
Maastricht University Faculty of Law, European Centre on Privacy and Cybersecurity (ECPC), The Netherlands

Abstract

Recently, browser-based crypto mining (or browser mining) received attention in academic literature, mainly from 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 code-bases. 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 monetisation of web services and digital content. A number of studies explored browser mining for monetisation purposes and highlighted its short-comings compared to 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, 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 monetisation by (i) exploring the legality of browser mining in relation to EU data protection and privacy law (ii) 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 advertisement that rely on the exploitation of large amounts of personal data and ad networks.

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

8. Algebraic methods in the analysis of persistency of attacks in decentralized systems

Oleksandr Letychevskyi
Glushkov Institute of Cybernetics, Ukraine
Category: Oral Presentation

Abstract

The paper considers the use of formal algebraic methods in blockchain system safety and security and in the evaluation of the persistency of an intruder's attacks. A model of blockchain algorithm is presented as the specification of a behaviour algebra. The research problem is the reachability of vulnerabilities and violations of safety properties that are presented in the database as behaviour algebra models. The model uses different methods realised in behaviour algebra theory: algebraic matching, symbolic modelling, static detection of invariants and other methods. It allows significant decrease of false positives and more accurate detection of issues, including deep hidden ones. The algebraic modelling of detected issues also allows for an evaluation of the persistency of attacks on the system. The advantages of this technology are that it can be successfully applied in multiagent environments of distributed systems. Examples of the technology demonstrate the detection of re-entrancy attack in smart contracts, double-spending attack in consensus algorithms and violation of equilibrium in a token economy. The algebraic methods are developed as SDK for decentralised system development and web platforms for access to an algebraic server.

Keywords: *algebraic modelling, symbolic execution, smart contracts, token economy, consensus algorithms, distributed systems*

9. Blockchain to Negate Malware

S.P.M Bergstrom
Quantum1Net, Spain
Category: Oral Presentation

Abstract

Just as Proof of Work was created by Cynthia Dwork and Moni Naor to manage DoS attacks and block spam emails, blockchain can be used to verify data consistency and negate malware and virus attacks. A firewall works by stopping all data that have not been requested from the inside of the firewall, as any data has not been requested is then considered malicious. So, to be able to introduce malware, phishing and social engineering is used to get to the inside of the firewall and infect the machine or device. By using a network overlay and register the network data movements on a blockchain, malicious software can be detected and negated via a consensus function of the network, where the work in the PoW would consist of the data transport not CPU cycles. The reason to use a blockchain is that without an immutable storage a malicious actor could first take over the data moment register and then inject the malware without being detected.

Keywords: *Malware, Blockchain, decentralized consensus, Cybersecurity*

10. Distributed Ledger Technologies And Internet Of Things, A Devices Attestation System For Smart Cities

E Pioli Moro and Alistair Duke
British Telecommunications plc, UK
Category: Oral Presentation

Abstract

Traditional IT security mechanisms are generally not well-suited for IoT devices, where processing and network connectivity should be kept at minimal. Consequently, IoT devices have been recently identified as an easy target for cyber-attacks, like for example on the Mirai botnet Distributed Denial of Service attacks in 2016, where various devices were hacked into and taken over. Different solutions have been developed aiming at guaranteeing the security at both the devices application layer and the network layers. Few succeeded to deliver the flexibility necessary for IoT devices. Even fewer have implemented an effective threats detection system, and just a handful have realised all the previous in a fully decentralised fashion, including this one. This Distributed Ledger Technology (DLT) attestation system is maintained and supported by most, or all, IoT devices because it is based on a light-weight DLT protocol. It comprises of a system for authorisation and authentication for the individual devices as well as includes an anomalies detection system based on smart contracts. A demonstration was built to support a Smart City use case. The objective is to guarantee, in a decentralised manner, the security of low computational power devices executing the sensing function and their connectivity, and therefore the correct functioning of the system. On the demonstrator, the system was ran using DLT supported by the sensors connectivity bridge (built using Raspberry Pi's). The system proved to be rapid to develop, flexible with regards to systems changes and resilient to attacks to both individual IoT devices and to the DLT.

Keywords: *Internet of Things, Distributed Ledger Technologies, Blockchain, attestation, smart cities*

11. Privacy Laws, Non-fungible-tokens and Genomics (DNA)

Daniel Uribe, Genobank.io, USA
Gisele A Waters, Symbiotica LLC, USA
Category: Oral Presentation

Abstract

This article analyses some of the main legal requirements in the new California Consumer Protection Act (CCPA) & General Data Protection Regulation (GDPR) with regard to the intersection between regional privacy law, smart contracts (such as Fungible & Non-Fungible-Tokens) and genomic data. The CCPA & GDPR law imposes several restrictions on the storing, accessing, processing and transferring of personal data. This has generated some challenges for lawyers, data brokers and business enterprise engaged in blockchain offerings, especially as they pertain to high risk data sets such as genomic data. The architecture and technical features of Non-Fungible-Tokens, Distributed Storage & Wallets to trace, store and govern DNA (Genomics) datasets will allow donors (data subjects) to establish digital ownership, control in alignment with privacy laws using customizable code or "Programmable Privacy Smart Contracts". Therefore, in order for stakeholders to be legally compliant, the design of blockchain value propositions should include additional privacy-by-design capabilities in the smart contract coding language itself. This article describes the three domains and begins to explore how data engineers can begin to explore the challenges of coding privacy law, the legal requirements into the earlier stages of the architectural design of the computer code. This automated process focuses on Smart Contracts (NFT's) and genomic data requirements which include selection of a genetic data information schema and a privacy-code that follows programming logic to process sensitive information based on that schema. Programmable privacy is a unique way to write and design computer code, which can automatically check the legal compliance of the smart contractual framework in a trustless and decentralized way. The schema contains a set of legal questions that have been specifically designed to require Cloud providers to disclose relevant information and comply with the legal requirements established by the CCPA and/or GDPR.

Keywords: *blockchain, NFT, smart contracts, California Consumer Protection Act, privacy, private cloud, distributed Storage, IPFS, genomics, DNA, data broker, privacy law, GDPR, CCPA*

12. Transformation or Adaptation of Blockchain at Crossroad of Institutional to Distributed Trust Journey? A Public Sector Perspective

Ali Shahaab[1], Ross Maude[2], Chaminda Hewage[1], Imtiaz Khan[1]
[1]*Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom*
[2]*Companies House, Cardiff, United Kingdom*
Category: Oral Presentation

Abstract

Blockchain technology has been commended as a solution that can help with disintermediation and filling the consistently increasing trust challenges faced by corporate and public sector. 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 argue that all information technology systems rely on a suite of technologies and therefore blockchain should also be added to the 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 mind set 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 needs 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 four 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*

13. Modern portfolio theory: a blockchain theoretical model

Alfio Puglisi
Kings College London, UK
Category: Oral Presentation

Abstract

Crypto assets, such as Bitcoin and Ethereum have attracted the interest of investors across the globe. The model presented in this paper is based on the idea of a DLT-based market for securities, where investors have the option of switching between traditional financial securities to crypto-assets. The model based on two game framework (government vs investors) demonstrates that investors are utility maximisers and in the event of unstable exchange rate policy and inflationary pressure, the investors switch between the two assets classes under consideration. In the event of a public DLT based market for crypto assets, the model also shows that there are AML risks and regulatory challenges both for regulators, central bankers in order to track online financial activities of retail consumers.

14. Cost Benefit Analysis of permissioned and permissioneless blockchain solutions

Carlos Castro-Iragorri [1], Federico Lopez [2], Olga Giraldo [3]
[1] *Universidad del Rosario, Colombia*
[2,3] *Linking Data, Colombia*
Category: Oral Presentation

Abstract

This paper is a case study that analyses the adoption of blockchain technology in the management of learning records and the issuance of academic certificates. In this use case we identify service providers that have adopted a permissionless approach and on the other hand 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 an approach for cost benefit analysis in blockchain projects.

Keywords: *permissioned, permissionless, digital credentials, cost benefit analysis, blockchain, economics*

15. Emerging Regulatory Approaches To Blockchain Based Token Economy

Agata Ferreira
Warsaw University of Technology, Poland
Category: Oral Presentation

Abstract

Blockchain enabled digital scarcity, which has opened up the whole new dimension of possibilities for token economy, particularly with relation to rights and assets that have not been traded electronically before. Blockchain based tokenization of rights and assets brought also new set of legal and regulatory challenges. Regulators and legislators are yet to address many of the issues raised by blockchain based tokenization, from decentralization, token characterization to cross border harmonization and regulatory compliance with traditional market infrastructure. Lack of regulatory alignment can undermine many of the benefits of token economy. Lack of legal certainty may not only stifle innovation and slow down mainstream adoption of blockchain based tokenization, but it can also raise the risks for the investors and harm the reputation of the industry. The emerging regulations vary in approach. Liechtenstein became the first country to have a comprehensive technology neutral regulation of the token economy. Malta and Singapore also represent progressive jurisdictions for blockchain regulations. However, most jurisdictions, including the US and the EU, have not yet formed clear policy for blockchain regulation and many legal questions remain open. The paper examines whether there is an emerging dominating regulatory approach or prevailing regulatory direction for the future of token economy. It also highlights the existing regulatory void and divergent approaches to blockchain based tokenization. Finally, the paper concludes that there is an urgent need to provide clear legal and regulatory framework if the potential of the token economy is to be realised.

Keywords: *blockchain, tokens, token economy, blockchain regulation*

16. Using Blockchain for Evidence purpose in Civil Cases in Poland

Rafael T. Prabucki
The University of Opole, Law and Administration Faculty, Poland
Category: Oral Presentation

Abstract

For some period of time Blockchain technology has been used for many purposes all over the world. There are many various types of reports that indicate that Blockchain technology is used to maintain a national database of records, for example for processing electronic records containing information about lands. Additionally, many private or public entities are interested in such a solution. The question arises - how to prove the facts in the dispute, when data is stored or protected by applying the solution based on the Blockchain technology? The answer to this question is narrowed down to civil issues. Currently, the Smart City trend will shows that blockchain issues will be intensively used in heavy contract area (energy, transport). 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 so-called smart contracts. The research methodology is based on the analysis of existing regulations, which may be relevant to the Polish Court's perception of evidence based on blockchain technology. Moreover, legal scientific studies that indicate the risks associated with proving certain facts in such a way will be analysed. All efforts have been taken in order to obtain conclusions regarding the future of this type of solution in Poland.

Keywords: *evidence, blockchain, registers, civil cases, smart contract, polish law*

17. Solidity + : A language for Robust programming of Smart Contracts

RK Shyamasundar, Snehal Borse, Prateek Patidar
Department of Computer Science and Engineering
Indian Institute of Technology Bombay, India
Category: Oral Presentation

Abstract

Smart Contracts handle and transfer assets of considerable value. Thus, it is crucial that their implementation be secure against attacks which aim at stealing or tampering the assets. In the recent past, there have been several attacks that have exploited existing vulnerabilities in smart contracts. The functioning and deployment of smart contracts is somewhat different from the classical programming environments. Once a smart contract is up and running, changing it, is very complicated and nearly infeasible. One of the reasons is that when a contract is created, it is immutable; once deployed on the Blockchain it stays there forever. If we find a defect in a deployed smart contract, a new version of the contract has to be created and deployed. When we deploy a new version of an existing contract, data stored in the previous contract does not get transferred automatically to the newly refined contract. We have to manually initialize the new contract with the past data which makes it very cumbersome. Similarly, neither updating a contract nor rolling back an update is possible; this greatly increases the complexity of implementation and places a huge responsibility while being deployed initially on the Blockchain. Smart contract languages today are derived from extensions of general purpose languages like Javascript. While the similarity make smart contract languages look familiar to software developers it is inadequate to accommodate the domain-specific requirements of digital contracts. Smart contracts have not only shed light on the benefits of digital contracts but also on their potential risks. Some of the prominent smart contract languages are Solidity, GO etc. Like all software, smart contracts can contain bugs and its' vulnerabilities can be exploited that can have direct financial consequences. Thus, it is very important to have a sound methodology, that is practical enough for use by a large community of smart contract programmers to check the contracts for crucial properties. Solidity is one of the widely used languages for programming smart contracts. It has been designed for Ethereum architecture. Several security vulnerabilities in Ethereum smart contracts have been discovered both by hands-on development experience, and by static analysis of contracts on the Ethereum Blockchain. These vulnerabilities have been exploited by several attacks on Ethereum, causing huge loss of money. One of the most successful of these attacks managed to steal $60M from the DAO contract, but its' effects were cancelled after an harshly debated revision of the Ethereum Blockchain. There has been a significant amount of work done in analyzing correctness of smart contracts. Some of the major deficiencies of these explorations are (1) analysis is based on the bytecode generated for Ethereum rather than smart contracts in Solidity, (ii) analysis is approximate and have severe limitations in usage due to over-/ or under-approximation. In this talk, we want to address the following question: Using a stark resemblance of Solidity programs with distributed programs, can we arrive at a concurrent programming language approach of arriving at simple specifications of Solidity programs similar to classical declarations used in concurrent programming languages that leads to robust programming of smart contracts. We describe the design and use of language Solidity!, for programming smart contracts; Solidity + is essentially the same as Solidity except for declarations. We show how a vast variety of vulnerabilities encountered in programming smart contracts in Solidity no longer exist in Solidity! , due to declarations. We further show that Solidity! can be automatically transformed to Solidity – thus, enabling effective debugging at source level. Another important outcome of using of Solidity +, is thatbrings out an outline of a proof carrying code for the smart contract for free – needless to emphasize that it is a very welcome feature for smart contracts on Blockchains.

18. A Peer-To-Peer Publication Model On Blockchain

Imtiaz Khan and Ali Shahaab
Cardiff Metropolitan University, UK
Category: Oral Presentation

Abstract

For centuries journals remain the primary platform for scientific communication and act as the trusted third party to ensure the quality and integrity of the peer reviewed published works. However, past few decades witnessed a sharp rise of research irreproducibility and retraction to a point that now is deemed as crisis. Addressing this crisis here we present a peer-to-peer (P2P) publication model that utilise blockchain and smart contract technologies. Focussing primarily on researchers and reviewers, the conceptual P2P publication model addresses the sociocultural and incentivisation issues related to irreproducibility crisis where publication will be incremental and authorship will be accumulative and shared with reviewers. The concept of P2P publication model was inspired by the transformational journey music publishing industry has undertaken as it traverse through vinyl age (complete album) to Spotify age (song-by-song) along with growing inclination towards building an incremental album with feedback from fans and establishing a decentralised and automated revenue collection and sharing system using blockchain and smart contract technologies. Incremental publishing of scientific work through P2P publication model will relieve researchers from the burden of publishing complete and "good results", also at the same time reviewers will be recognised and incentivised in a competitive manner to undertake rigorous review work. P2P publication model aims to transform the century old publication model and incentive structure in alignment with the context and aspiration of 21st century scientific endeavours.

Keywords: *research reproducibility, blockchain, sociocultural issues, publication*

THE BRITISH BLOCKCHAIN ASSOCIATION IS WORKING IN COLLABORATION WITH

British Embassy Lisbon

BBC GLOBAL NEWS LTD

Department for International Trade

GCPSE Global Centre for Public Service Excellence

UNDP Empowered lives. Resilient nations.

ENTERPRISE ETHEREUM ALLIANCE

INATBA

Edinburgh Napier UNIVERSITY

The Open University

FINTECH CIRCLE

appg BLOCKCHAIN

Ulster University

Isle of Man Government Reiltys Ellan Vannin

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

VOLUME 1 | ISSUE 1 | ISSN PRINT: 2516-3949

INAUGURAL EDITION JULY 2018

British Blockchain Association Collaboration. Innovation. Excellence

EUROPE'S FIRST PEER REVIEWED SCIENTIFIC BLOCKCHAIN JOURNAL

Setting the "Gold Standard" in Blockchain

International Blockchain Standards: A Research by ConsenSys

Blockchain & Post Brexit United Kingdom

IBM and Walmart Blockchain Pilot by BRI

Blockchain & GDPR: A Delphi Study

EXCLUSIVE INTERVIEW WITH LORD HOLMES OF RICHMOND MBE UK BLOCKCHAIN APPG VICE CHAIR

britishblockchainassociation.com/jbba

SPONSORS & ACADEMIC PARTNERS

Portrait courtesy The House of Lords

Volume 1 - Issue 1
July 2018

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

VOLUME 1 | ISSUE 2 | ISSN PRINT: 2516-3949

EDITION DECEMBER 2018

British Blockchain Association Collaboration. Innovation. Excellence

britishblockchainassociation.org/jbba

DECENTRALISED HEALTHCARE ON THE BLOCKCHAIN

Challenges of Investigating Cryptocurrencies & Blockchain related Crime

E-Voting on the Blockchain

Ethereum Registration Authorities for Private Sidechains

Crypto Ricardian Rent & a Crypto Coase Theorem

Utility Tokens & Quantity Theory of Money

The Cost of Trust: A Pilot Study

Blockchain Research: Exclusive Interview with Andreas M. Antonopoulos

patientory association

ACADEMIC PARTNERS

Volume 1 - Issue 2
December 2018

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

VOLUME 2 | ISSUE 1 | ISSN PRINT: 2516-3949

EDITION MAY 2019

The British Blockchain Association Collaboration. Innovation. Excellence

britishblockchainassociation.org/jbba

EVIDENCE BASED BLOCKCHAIN

Is EBB the New Currency of Blockchain Effectiveness?

Blockchain and Supply Chains: Value Redistributions, De-commoditisation and Quality Proxies

Crypto-friendly Index for the APEC Region

Valuation Method of Equity-based Security Token Offerings (STOs)

Evaluation of Post-Quantum Distributed Ledger Cryptography

Initial Coin Offerings: Are they Scams? An Empirical Study

Parameters for Building Sustainable Blockchain Application Initiatives

Application of Behavioural Heuristics to ICO Valuation and Investment

Proceedings of 1st Blockchain International Scientific Conference 2019

ACADEMIC PARTNERS

Volume 2 - Issue 1
May 2019

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION

VOLUME 2 | ISSUE 2 | ISSN PRINT: 2516-3949

OCTOBER 2019

The British Blockchain Association Advocating Evidence Based Blockchain

britishblockchainassociation.org/jbba

BUILDING QUANTUM RESISTANT BLOCKCHAINS

The Contractual Cryptoeconomy: An Arrow of Time for Economics

A Review of fast-growing Blockchain Hubs in Asia

Cryptocurrency Investing Examined

Blockchains & the Future of Art

Transitioning to a Quantum Resistant Hyperledger

Singapore's Open Digital Token Offering

Blockchain for Transportation in Low Income Country Cities (LICC)

2nd Blockchain International Scientific Conference, 11 March 2020

ACADEMIC PARTNERS

CEBB Centre for Evidence-Based Blockchain

Volume 2 - Issue 2
October 2019

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: 10 August 2020)

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 I admin@britishblockchainassociation.org

Follow us on: