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 Blockhain

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

Portrait courtesy The House of Lords

BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
12 MARCH 2019 | LONDON

WHY ATTEND ISC 2019?

World's First 'Scholars in Blockchain' Conference

International Recognition of your work by Blockchain Scientific Community

Prizes for Best Abstract, Project & Oral Presentations

Connect with Enterprises & Institutions looking for Blockchain innovators

Showcase your project to 2000+ delegates

Publish your work in Europe's First Peer Reviewed Blockchain Journal (The JBBA)

Network with some of the Most Eminent Blockchain Scholars

Pitch your ideas and research to Policy Makers and Enterpreneurs

Meeting point Conference of Blockchain Industry & Academia

CALL FOR PAPERS

Researchers, academicians, technologists, blockchain developers, policy makers and other stakeholders are welcome to submit their original research papers, pilot projects and case studies to ISC 2019 in one of the following disciplines:

Blockchain and Gov-tech
Crypto-assets & Cryptocurrencies
Blockchain for Banking
Blockchain in Healthcare
Blockchain in Supply Chain
Blockchain Governance
Blockchain & Law
Blockchain & Economics
Applied Blockchain
Initial Coin Offerings
Blockchain and Smart Cities
Theories of Blockchain and its Evolution
Smart Contracts
Blockchain and Bitcoin Security
Lightweight Protocols and Blockchain Algorithms
Blockchain based IoT Security Solutions
Blockchain and Artificial Intelligence
Blockchain in Social Networking
Blockchain for Public Good
Enterprise & Consortium Blockchains
Decentralised Applications (DApps)

IMPORTANT DATES

Abstract submission deadline
25 October 2018

Notification of review outcome
30 November 2018

Revised submission deadline
15 December 2018

Speakers notified of Oral/ Poster presentation slots
12 January 2019

Conference Registration deadline for Speakers
15 January 2018

Blockchain Scientific Conference
12 March 2019

TABLE OF CONTENTS

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.

Crossref

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

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

Online publication:
The issue can be viewed on the JBBA website: https://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.

Photo by Iñaki del Olmo on Unsplash

EDITORIAL

Dr. Naseem Naqvi
Editor-in-Chief

Prof. Dr. Kevin Curran
Associate Editor-in-Chief

Setting the Gold Standard in Blockchain

It gives us great pleasure to launch the inaugural edition of the JBBA – Journal of the British Blockchain Association. The JBBA is Europe's first peer reviewed journal devoted to Blockchain & other Distributed Ledger Technologies and Cryptocurrencies. It is an open access journal offering a wide ranging and comprehensive coverage of all facets of Blockchain and Distributed Ledger Technologies. The journal has been nearly 12 months in the making and we have witnessed an exponential growth in the blockchain space over the past 1 year, both in terms of scientific breakthroughs and early adoption of this technology.

All research submissions to the JBBA are peer reviewed. Peer-review is a critical part of the functioning of the scientific community, of quality control, and the self-corrective nature of science and our aim is to provide a journal which only publishes rigorously reviewed articles which enhance the body of knowledge growing around the Blockchain. A high-quality peer-reviewed journal will enable authors to showcase their work, and at the same time, allow policy makers to build on an evidence-based framework. This will enable stakeholders to provide government with sound academic support for experimentation, proofs of concept and knowledge transfer. We aim to become the "Gold Standard" for the highest quality, evidence based, peer-reviewed resource on blockchain technology.

In the best interests of the global blockchain community, *The JBBA* will be freely accessible via the internet for immediate worldwide, open access to the full text of articles. The JBBA applies the Creative Commons Attribution License under which all readers will be able to download and/or print any article at no cost. Authors who publish in the journal will retain the copyright to their article.

The JBBA follows the continuous publication model and publish content on a real-time basis on the journal's website. All articles are published online as soon as they become ready. Once published, articles will then be selected for a subsequent print issue, which we aim to publish 3-4 times per year.

AIMS & SCOPE OF THE JOURNAL

The JBBA attempts to cover the state-of-the-art advances in all aspects of blockchain technology. The international and multidisciplinary nature of this field enables us to cover both theoretical research and technological developments. The JBBA welcome contributions from blockchain scholars & scientists worldwide and will provide a forum for authors to share their knowledge, skills and experiences across a wide range of industries and technologies in which Blockchain is being deployed. The possible topics include but are not limited to:

- Blockchain and Gov-tech
- Cryptocurrencies
- Blockchain in healthcare
- Blockchain in supply chain
- Blockchain governance
- Blockchain & law
- Blockchain & Economics
- Applied Blockchain
- Initial Coin Offerings
- Blockchain for social good
- Blockchain and smart cities
- Theories of blockchain and its evolution
- Smart contract and distributed ledger
- Blockchain and Bitcoin security
- Distributed consensus on resource-limited devices
- Lightweight protocols and algorithms based on blockchain
- Blockchain based IoT security solutions
- Blockchain and Artificial Intelligence
- Blockchain in social networking

We will publish:

1. Original Scientific Research (Qualitative, Quantitative)
2. Randomised Control Trials
3. Systematic Reviews
4. Meta-analysis
5. Conference Research Abstracts
6. Comparative studies
7. Case Studies & Essays
8. Book Reviews
9. PhD/MSc thesis & Dissertations
10. Critical reviews and Analysis
11. Interviews / Opinions of Key Influencers / Thought Leaders
12. Commentary on latest issues and trends in blockchain & DLT
13. Editorial

We would also include selected mix of articles published on our website. Should you wish to be interviewed by us or like to showcase your work, please get in touch at:

Editorial@thejbba.com

The Editor-in-chief has overall responsibility for the content, production and strategic direction of the JBBA.

Submissions can be made online at:

https://jbba.scholasticahq.com/for-authors

The journal will be distributed to key industry, academic and government stakeholders including the House of Commons, the House of Lords, Whitechapel Think Tank, all major UK Universities, Blockchain entrepreneurs & industry leaders, DLT scholars, all major Banks, Fin-tech corporations and made available (upon request) at major international blockchain conferences, worldwide.

We wish to close this inaugural editorial by inviting you to submit your latest blockchain related work for publication in the second edition of the JBBA. We intend to be open to creating special issues to include conference proceedings and blockchain topics that may not receive sufficient consideration otherwise or that might require a more multidisciplinary focus. We welcome new ideas and suggestions from the blockchain community and finally, would like to thank you once again as readers, authors, reviewers, and editors; together we will bring our journal to new heights.

Best wishes,

Dr. Naseem Naqvi FRCP FHEA MAcadMedEd
Editor-in-Chief

Professor Dr. Kevin Curran PhD
Associate Editor-in-Chief

July 2018

Photo by Shawn Ang on Unsplash

EDITORIAL BOARD

Photo by Spencer Watson on Unsplash

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(1)2018

Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using Blockchain

Dr. Brendan Markey-Towler[1] PhD
School of Economics, University of Queensland, Australia
Correspondence: brendan.markeytowler@uqconnect.edu.au
Received: 19 February 2018 **Accepted:** 17 March 2018 **Published:** 19 March 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
BM-T [1] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
BM-T [1] acknowledges John Foster and Peter Earl for their feedback and suggestions on this paper.

Abstract

Blockchain technology makes it more feasible for individuals to exit political-socioeconomic systems at the level of the system itself and elect to accede freely to institutional systems which formulate, promulgate, keep and verify institutions and public records without a centralised authority. This essay investigates the dynamic of such a society in which political-socioeconomic systems may be organised using blockchain technology. We propose a theory of society as an evolutionary system in which the unit of selection is the institutional system associated with a particular blockchain or the state and selection pressures are applied by individuals deciding to interact within them and have their interactions entered into the public record. We establish the conditions under which institutions will thus be selected by considering the limits to substitutability and discover that any institutional system must meet requirements and provide sufficient complementarities in order to be selected and retained by the evolutionary process.

Keywords: *blockchain, sociology, institutions, anarchy, utopia*

JEL Classifications: *D02, D71, H11, P16, P48, P50*

1. Introduction: the anarchist utopia

The basic vision of anarchism – if indeed there can be one for such a diffuse and subtle mode of political thought – is of a society entirely free of the State and all its violence and coercion. The utopia of the anarchist is no free-for-all war of all against all either. Instead, it is a society in which individuals are entirely free to elect to associate themselves with others and interact with them according to a set of rules to which those others agree.

The anarchists have been crushed throughout history by those who wish the state to hold a monopoly over defining what is right and proper behavior, and those who fear what might happen if individuals were free to associate and interact as they wished (Marshall, 1992). Power ultimately relies on submission as Etienne La Boetie showed in On Voluntary Servitude, but as yet it has been found infeasible for a sufficiently large portion of society to repudiate the coercion of the state and associate freely to neuter the state's ability to use violence effectively to remove those who do from society. Yet now, even while the state exists all-powerful, the technology which might allow for such large-scale action is emerging in the form of the blockchain.
On the face of it a mundane and boring technology for bookkeeping, blockchain is actually revolutionary because it makes the anarchist utopia a more realisable dream than has ever before been possible. At the very least it provides the strongest challenge ever posed to the monopoly of the state over the promulgation, formation, keeping and verification of institutions and the public record. The purpose of this essay is to investigate the conditions under which this might occur, and the dynamics of a society organised using blockchain technologies.

In the next section, we will consider blockchain and how, as a distributed ledger technology, it provides a platform which might constitute the foundation of entire institutional systems which might compete with the state, and at the very least make exit from existing political-socioeconomic systems more feasible than ever before. We then investigate the dynamics of such a society as would be organised by blockchain by proposing a theory of society as an evolutionary system in which the unit of selection is an institutional system associated with a particular blockchain or the State and establish the properties of an institutional system which is likely to be selected and retained by the evolutionary process. We conclude by considering the likely outcome of this process and what will be required for the anarchist dream of a society formed by free association and interaction, or at least a serious challenge to the hegemony of the State over the institutional system to be realised.

2. What is Blockchain technology and why is it so important

Blockchain technology is a distributed ledger technology (Davidson, De Filippi and Potts, forthcoming; 2016; Catalini and Gans, 2017). What that means is that it is a technology by which a group of people can come to a consensus on the keeping of a record – a "book" – without requiring the surrender of their collective assent to a centralised authority. A public record can be kept without the requirement of a public authority.

The software, operating on the internet, registers all of the interactions which occur between individuals interacting using the corresponding medium of interaction. Individuals are rewarded for processing and verifying that information by building it into a record and then solving a mathematical problem posed at the end of the processing which allows all others to verify that the record has been correctly compiled. As each verifies that the record has been correctly compiled, the block of records is then added to a chain of such records – the blockchain – of which every single node in the network keeps a copy. Each individual has a private key which allows them to decrypt and access that portion of the blockchain which records their own interactions. The record of interactions is thus distributed among the entire network (making it extremely and increasingly secure) and it is updated and verified by the network as a whole, without the need for a centralised authority.

Now that sounds relatively prosaic: blockchain is a social technology which allows a collective to write a book and update it – a book-keeping technology. It is anything but prosaic. The keeping of records which can be publicly verified is the very foundation of our advanced political-socioeconomic systems.

The first systematic study of the economics of record-keeping was provided (somewhat unwittingly) by John Commons (1924) in his Legal Foundations of Capitalism. What he showed there was that the rise of humanity from the oppression of subsistence by economic development was accompanied by the emergence of the institutions (rules for thought, action and interaction) of the law, especially the law of contract and property. Only once the enforcement of property and contract became a greater surety could the expectations of reciprocity, of quid pro quo, and expectations of libertas (the right to use property) necessary for large scale market interaction be supported. The laws of contract and property were a precondition for the development of the capital base and technologies embodied within it which drove the industrial revolution (Landes, 1969) and was a guarantor of the emerging "bourgeois virtues" supporting exchange and enterprise (McCloskey, 2006).

The laws of contract and property demand the keeping of verifiable records to function well – without records establishing the alternative facts, a judge relies entirely upon the law of equity. Hence, since the very basis for our market economies is the law of contract and property, and these rely on the keeping of verifiable records, our entire economic system at the very least relies on the keeping of verified public records.

Really, we know that not only our entire economic system but also our entire political and social system relies on institutional structures and the recording of interactions within them in a public record as well. Institutions give us the basis for interaction in political socioeconomic systems by establishing the proper ways to act and interact in society (Hamilton, 1919; Williamson, 1985; North, 1990; Ostrom, 1990). Institutions establish the social positions individuals might occupy which are associated with rights, obligations and empowerments to act in particular situations (Searle, 2010; Lawson 2015). Public records inform us of, and verify, who occupies those positions. The law, for instance, which consists of rules for proper interaction and which deputises those who may use violence and coercion against those who transgress them (Hart, 1961) is predicated upon the keeping of public records: parliamentary statutes, executive regulations and rules, royal proclamations-in-council, judicial decisions.

Traditionally, the formulation, promulgation, keeping, verification and enforcement of public records of institutions and interaction according to them has been a process conferred exclusively upon and monopolised by the government. Now of course, when it was difficult to communicate with the entirety of humanity instantaneously this was efficient enough . But this efficiency is gained at the cost of creating a nexus of power which might be used by those occupying it for extortion by withholding the entering

Blockchain technology, by operating on the internet, largely eliminates the cost of communication even at the scale of populations. Since the public record is kept by everyone and updated by collective assent and any individual is incentivised to update it, there is no nexus of power which may be exercised to corrupt or use the public record as a tool of extortion. The cost of this gain is that the process is energy-intensive and requires significant digital storage capacities.

What is revolutionary about this technology therefore, is that it makes even yet more viable what Albert Hirschman (1970) called the "exit" response to decline in organisations. when faced with a system in which one's needs and desires are not being met, one has, in theory, two options. one may voice one's concerns with the system in the hope that the decision-makers in the system might address them by changing the system. or one may exit the system and join one more amenable to one's objectives. Hirschman's theory, of course, was that in the absence of loyalty, exit would become increasingly preferable as the response to voice on the part of decision makers within the system became less and less.

As the RMIT school of thought has rightly recognised (Berg and Berg, 2017; MacDonald, 2015b), the blockchain makes exit more viable at the level of entire political-socioeconomic systems by making possible (in principle at least) the acceding to a non-centralised political-socioeconomic system (MacDonald, 2015a). The government is one means by which a set of institutions may be formulated, kept, promulgated and verified and public records of interactions under their rubric kept. The blockchain provides another, and one which does not require the surrendering of assent to the institutional structure and public record to a centralised authority.

What does this mean more practically? Well we have already seen the emergence of Bitcoin as a public record of transactions and holdings of a medium of exchange. But blockchain is no mere money-counting device. Ethereum has already pioneered the keeping of contract records, and the striking of "smart" contracts which execute automatically. Horizon State is among a number of companies pioneering the use of Blockchain technology as a means of keeping voting records. Blockchains allow us to formulate, promulgate, keep and verify institutional structures and keep a public record of interactions within them which have the potential to revolutionise the financial sector and the way we conduct market exchange (MacDonald, Allen and Potts, 2016), the way we strike contracts and collaborate (Davidson, De Filippi and Potts, forthcoming; 2016) and the very way we govern ourselves as collectives constrained by agreeing particular rules for interaction (Allen, Berg, Lane and Potts, 2017).

But what if we went further? What if we used it as a means of issuing shares or keeping store credit as a "token"? What if it were used to build collectively funded and governed welfare or healthcare provision systems – modern friendly societies? What if it were used as a means of registering and verifying one's educational attainments or qualifications? What if it were used as a means of registering births, deaths and marriages?

No blockchain compels people by force (at present) to join it, interact according to its interactions and record those interactions therein, and by definition it requires the assent of the collective to function. As Etienne La Boetie showed in On Voluntary Servitude, power is ultimately submitted to rather than extended, and one might simply cease to interact by use of a particular Blockchain if one comes to repudiate its institutional structure, so it is in the final estimation a matter of choice to acquiesce to the institutions associated with any particular blockchain.
Blockchain technology therefore offers the possibility of finally realising the anarchist dream (Marshall, 1992) – a society which is composed of groups formed entirely by mutual association and absent violence and coercion. Blockchain might provide the missing link which allows for the formation of large-scale (therefore feasible) societies with institutions formulated and promulgated and records kept and verified collectively. Quite a utopia.

This is no mere matter of intellectual curiosity. The possibility of exit on the societal level is now a matter of desperate practicality. Even in the "Western" democracies (Australia is as good an example as any), the nexus of power has become hopelessly corrupt as the laws have finally reached the point of having to resist and repress the basic human tendency to form groups for mutual assistance (Murray and Frijters, 2017). Upward mobility has eroded drastically as the nexus of power has become ever more impervious to the Voice of all but those with the resources necessary to sustain lengthy campaigns – Mancur Olsen's (1965) nightmare of socio-political capture by vocal minorities prevails. The citizen seeking to survive and thrive is increasingly left with their last right – the right to repudiate the system of political-socioeconomy in its entirety and accede to a new system formed of voluntary association.

But how does such a system function? What does a society formed of individuals all, in the final estimation, voluntarily conducting their political-socioeconomic interactions in the medium they choose "look" like? The answer is provided by evolutionary institutional political economy and economic psychology.

3. A theory of political-socioeconomic systems organised using the Blockchain

Take a population of people and imagine that, in addition to the institutions of states, there exists a set of institutional systems associated with various blockchains in which interactions governed by those institutions are recorded. Institutional systems are to be understood as a set of rules which guide thought and action and stipulate the proper form of interaction in society (Hodgson, 1998; 2004; Hodgson and Knudsen, 2010). We can imagine the population of people to be partitioned into demes (Hartley and Potts, 2014) according to the institutional systems by which they elect to conduct their political-socioeconomic affairs and the corresponding blockchain on which interactions within the confines of those institutions are recorded and verified. The residual of the population who do not elect to accede to any institutional system with a corresponding blockchain either elect to, or by default, conduct their affairs under the institutional system, and have them recorded within the public records, of the State.

An individual leaves the institutional structure and its corresponding deme (defined by its corresponding blockchain or the institutions of the state) if they elect to cease interacting according to its institutions with others in the deme, therefore cease to have their political-socioeconomic interactions entered into the public record of blockchain or state, and thus repudiate that institutional structure. An individual cease to be part of a deme, an institutional system, when they elect to exit it rather than exercise voice in an attempt to change it. Thus, in principle at least, we have movement between demes and a sort of competition between them for adherents. Institutional systems compete to have individuals elect to adhere to their institutions, rules for interaction, and have their interactions entered on the public record.
Such a society is, in principle at least, anarchic. In principle individuals elect to adhere to a particular set of institutional systems and not others, provided the state or blockchain deme does not coerce or compel. It is a society based on mutual association and elective submission to rules for interaction.

3.1 Society as an evolutionary system

Now, because of the tendency introduced for an a priori set of institutional systems to be reconciled into posteriori set through the interactions of individuals, such a society is also an evolutionary system (Price, 1970; 1972a; 1972b; Page and Nowak, 2002). It is a society therefore subject to variation of institutional structures, selection between institutional structures and their retention (Nelson and Winter, 1982; Metcalfe 1998; 2008; Dopfer and Potts, 2007; Witt, 2008; Hodgson and Knudsen, 2010, Markey-Towler 2017). It is a society, in a sense, where various visions of utopia are competing for adherents (Almudi, Fatas-Villafranca, Izquierdo and Potts, 2017; Almudi, Fatas-Villafranca and Potts, 2017). The unit of selection in this evolutionary process is the institutional system associated with any given blockchain (or the State), and the process of selection is the decision of individuals in society to conduct their political-socioeconomic affairs therein and have their interactions recorded on its blockchain (or by the State) as part of the public record.

Selection pressures are therefore exerted upon institutions by the behavioural change of individuals, specifically, their decision to conduct their political-socioeconomic affairs in this institutional system or that. When individuals choose exit over voice in the presence of whatever displeasure with their current system, that system is deselected in favour of some other system to which those individuals accede. So, if we wish to understand the characteristics of institutional systems which will likely be retained by the this process we must seek to understand the conditions under which individuals will opt to exit the one institutional system and accede to another.

3.2 The limits to substitution and the selection and retention of institutional systems

Here we are assisted by economic psychology, especially that of Peter Earl (1986a, b; 1990, 1995; 2017) (formalised in Markey-Towler (2017b, c; forthcoming)) which identifies exactly what such conditions are and the limits of their application. Individuals may be induced to exit the one system and accede to the other (provided they perceive the opportunity to do so and have sufficient knowledge) if a state of substitutability exists between them. That is, an individual will exit one system and accede to another if there exists a state in which they expect that outcomes of roughly equivalent preferability will obtain as a result. They may then be induced to substitute systems.

It is, perhaps, easier to establish conditions for retention by reference to what may cause a state of substitutability to not exist and therefore to establish the limits of institutional competition. This will be the case if there does not exist a state of substitutability between any two institutional systems, if the one cannot be substituted for the other without a significant change in the preferability of expected outcomes. There are two reasons this might be the case; either two institutional systems are basically non-substitutable, or some complementarity is realised in the one which is not realised in the other.

3.3 Non-substitutability: institutional systems must meet requirements

Basic non-substitutability exists when people aren't concerned with what economists call "tradeoffs" but are instead applying "cutoffs", applying requirements which must be met by the courses of action available to them before they will consider taking them. Individuals do this any time they are applying simple rules to eliminate alternative courses of action rather than making complex considerations of tradeoffs. So, in order to survive and be retained by the evolutionary process, an institutional system and the blockchain recording interactions according to it (or the state) must meet requirements individuals impose on any institutional system.

It isn't difficult to imagine what such requirements might be. To interact in society, we must be guaranteed a certain reciprocity and security with respect to exchange and property. Traditionally this has been underwritten by the violence and coercion of the state, but the most basic of anarchist theories recognises that there are other non-violent means of enforcement which involve exclusion (Ackerman and Krueger, 1994). The institutional system must therefore be sufficiently exclusionary toward those unwilling to abide by its institutional structure. To interact in society, we must also be able to use any technologies or artefacts which facilitate such interaction. The institutional system must therefore be sufficiently easy to interact and keep records within. Finally, to interact in society requires a certain degree of libertas – the freedom to use one's property. So, one must be able to keep records of one's property and interactions sufficient to prove their existence which is difficult as possible to manipulate or destroy. The institutional system must therefore be secure from theft, corruption and manipulation.

What is interesting is that technically speaking, blockchain was designed to meet the first (reciprocity and security) and third requirements (integrity and retention), and massive advances are being made with respect to the second. The state, on the other hand, is increasingly providing evidence that it can meet none, and that as through all history, it cannot overcome the innate corruption of the human individual if they occupy a nexus of power by being the keeper of the public record of political-socioeconomic interaction. The limits to substitutability between state and blockchain at this level are increasingly psychological and therefore liable to collapse.

3.4 Complementarity: institutions must be integrated

A more potent barrier to substitutability between institutional systems is the existence of complementarity. Complementarity exists when the taking of two courses of action together is more preferable than taking either alone. The ability to do so might therefore be decisive for the existence of a state of substitutability, which is to say that the feasibility of a particular course of action might be decisive for behavioural change insofar as it may be taken together with others.

Complementarity presents a more imposing barrier to substitution and competition than basic non-substitutability as regards institutional systems. Despite appearances, political-socioeconomic interactions are not the totality of our existence. Even social media has not eliminated the coexistence of a private sphere alongside the public sphere in which our political-socioeconomic interactions occur (Habermas, 1962). It is, therefore, in all likelihood a major consideration for a large part of the population whether or not they may conduct and have entered on the public record all or at least a large portion of their political-socioeconomic interactions within the context of a single institutional system. One definitely important aspect of institutional systems then is the range of political-socioeconomic interactions which may be conducted within them and integrated into the public record.

It matters then that I might within the one institutional system with its associated public record at once purchase my groceries, manage my investment portfolio, strike contracts, be paid for my services, pay my rent or mortgage, and register my property in the public record. It also matters that I might be able to enter my qualifications, my educational achievements, my endorsements and public profile, the existence of my children and their relationship to me, and my spousal arrangements into the public record. It matters that I might be able to insure myself and others against future unemployment, ill health, or damage to my property and have my rights thereby recorded in the public record. It matters that I may at once register my voice as to how the institutional structure might be modified, have recourse to arbitration to settle disputes, and have a certain security in doing so.

This is the major challenge presented to any given institutional system – how it can provide an integrated system for conducting political-socioeconomic affairs. If it doesn't, it will struggle to offer the complementarities which attract the ordinary individual in such weighty decisions. The state has an advantage in this respect over blockchain technologies as an institutional system and system for public records for it has had some thousands of years to discover and develop institutional capabilities, but there is no reason in principle other than the current monopolisation of violence by the state (and willingness to use it) which prevents their similar development.

3.5 The properties of "fit" institutional systems

In any evolutionary system such as a society with competing institutional systems, selection pressure is harnessed into selection and retention based on the "fitness" of the units of selection. Those which are "fit" are selected by the evolutionary process and retained, those which are not are deselected and discarded. Even the anarchist utopia has a degree of brutality to it – institutional competition like biological evolution is "red and tooth in claw"- but only in a metaphorical sense, for selection pressures in this system are (in principle) exerted by the free decisions to associate and interact according to rules to which all relevant individuals agree.

From the above considerations, we now understand better the factors which cause selection pressures to be exerted differentially in the process of institutional evolution in political-socioeconomic systems organised by blockchain technology. Those institutional structures, and the technology (blockchain or the state) employed for keeping public records within them will be selected and retained which meet requirements for reciprocity, security, usability, integrity and retention and which provide sufficient complementarities between the range of interactions which might be engaged in and entered into the public record. At present, the State remains unchallenged in the wholesale sense, for in addition to the violence it may visit on those who resist its coercion, blockchain technologies have been focused on facilitating particular interactions in relative isolation and their ability to meet requirements has been constrained.

However, as their capacity for exclusion to enforce reciprocity, security, integrity and retention grow, and as their usability improves, and as the range of interactions which might be conducted within them and entered into the public record grows, we can expect the "fitness" of institutional structures founded upon blockchain technologies to improve. As we move into the future and toward a more recognisably anarchist society based on free mutual association, we can expect those blockchains or states associated with institutional systems which are more usable, which offer greater enforcement of reciprocity, security, integrity and retention, and which offer a greater range of political-socioeconomic interactions which might be conducted within them and entered into their public record to be selected and retained by the process of competition and evolution of institutional systems.

4. Conclusion: the road to utopia

It is unlikely that the state will ever be entirely superseded by another institutional system in the process of societal evolution. What is more likely is that either it will make use of violence to coerce adherence to certain or all of its institutional system and public records, or it will enter with some degree of success into the competition between institutional systems alongside blockchain technologies. But the challenge posed to the State simply by the emergence and potential of blockchain to facilitate interactions entered into freely according to rules agreed to freely means that in some sense, the anarchist utopia has become a little closer than before.

What we have done in this essay is investigate the technology which has made this possible, and consider the dynamics of a society organised using blockchain technology. We have seen what it means that blockchain is a distributed ledger technology which allows a collective to formulate, promulgate, keep and verify an institutional system and public record of interactions within it, and how it is revolutionary because it (in principle) makes exit an increasingly feasible option at the level of entire societies. We have applied the theory of evolutionary institutional political economy and economic psychology to study the dynamics of a society in which institutions associated with blockchains or the state are competing with one another. We discovered that those institutional systems selected and retained by the evolutionary process in society which meet requirements and provide complementarities. That is to say, those institutional systems will be more likely selected and retained as systems for political-socioeconomic interaction which provide reciprocity, security, usability, integrity and retention as well as a greater range of interactions which might be engaged in and entered into the public record.

The anarchist utopia of a society in which individuals are entirely free to elect to associate themselves with others and interact with them according to a set of rules to which those others agree is not here yet, and it probably never will be in all likelihood; but it has been made more possible, and we can expect the challenge to be increasingly presented to the state to reform in order to become more competitive with blockchain in a society which is constantly evolving.

Mathematical Appendix

The population of individuals i is N. The set of demes $D(I_r) \in D$ associated with an institutional system $I_r \in I$ for interaction and the public record r for doing so which is compiled either by blockchain or the state. We say that some action a_i on the part of an individual constitutes an agreement to interact within a particular institutional system if it is contained within the set $S(I_r)$ of actions which satisfy the rules of proper action which constitute the institutions of a particular system *and* which will be entered into the public record r. Thus, we may define a *deme* $D(I_r)$ to be the set of individuals who agree to interact within a particular institutional system, that is,

$$D(I_r) = \{i \in N: a_i \in S(I_r)\}$$

Thus, the rate of selection of the institutional system I_r at any given time t may be defined by the rate at which individuals who aren't currently are now deciding to interact within it and have their interactions recorded on its public record r. That is, the rate of selection of the institutional system I_r and its public record r (either state or blockchain) is given by

$$\frac{d|D(I)|}{dt} = |D_t(I_r)| - |D_{t-1}(I_r)|$$

or

$$\frac{d|D(I)|}{dt} = |\{i \in N: a_i^t \in S^t(I_r)\}| - |\{i \in N: a_i^{t-1} \in S^{t-1}(I_r)\}|$$

where, following convention, |X| denotes the cardinality (number of elements) of the set X, and we are allowing for the possibility that the set S(I_r) of proper actions per the institutional structure I_r which will be recorded in the public record r varies over time. What we can see clearly here is that the rate of selection of the institutional system I_r by the process of evolution is dependent on the rate at which individuals alter their behaviour. Specifically, it relies on the rate at which individuals are deciding to change their behaviour from not agreeing to be part of the institutional structure

$$a_i^{t-1} \notin S^{t-1}(I_r) \rightarrow a_i^t \in S^t(I_r)$$

It is discussed in Markey-Towler (forthcoming)[5] that this will, *inter alia*, be dependent on whether or not a state of *substitutability* exists between the two courses of action. This will be the case if the outcomes $g_{a_i^t} \in S^t(I_r)$ the individual expects to attend from interacting within the institutional structure I_r to be as preferable as those the individual expects to attend from *not* interacting within the institutional structure I_r $g_{a_i^{t-1}} \in S^{t-1}(I_r)$

$$g_{a_i^t} \notin S^t(I_r) \sim g_{a_i^{t-1}} \notin S^{t-1}(I_r)$$

If this is the case then it is demonstrable (see Markey-Towler (forthcoming)) that it is technically possible to induce the individual to opt to interact within an institutional system and have their interactions recorded on its public record.

This may not be the case, and barriers might exist which prevent the selection of a particular institutional system, if a state of substitutability does not exist. This might be the case either due to basic non-substitutability or the existence of complementarity.

If two institutional systems are non-substitutable, then the outcomes $g_{a_i^t} \notin S^t(I_r)$ the individual expects to attend from interacting within the institutional structure I_r are not as preferable as those the individual expects to attend from not interacting within the institutional structure I_r $g_{a_i^{t-1}} \notin S^{t-1}(I_r)$

$$g_{a_i^t} \in S^t(I_r) \nsim g_{a_i^{t-1}} \notin S^{t-1}(I_r)$$

This might be the case because rather than making complex tradeoffs between alternative courses of action, individuals are applying cutoffs contained within rules for eliminating courses of action.

Complementarity exists if the outcomes expected to attend upon the taking of two actions α,α' together a⊃α,α' are more preferable than those expected to attend upon taking one alone, α⊂ a ⊅α', that is, if a⊃α

$$g_a \succ g_{a \not\supset \alpha'}$$

This might present a reason that a state of substitutability might not exist between two institutional systems, as would be the case if there were some action α^' which might not be included within any feasible action which would constitute agreement to the institutional structure I_r. If $\alpha' \subset a_i^t \notin S^t(I_r)$ but $\alpha' \not\subset a_i^t \in S^t(I_r)$ and this were complementarity with some other action α then by definition we would find a non-substitutability between the two institutional systems and a barrier to the selection of I_r by the process of evolution.

1. For a more technical introduction to blockchain technology, see the original Bitcoin white paper by Satoshi Nakamoto (2008), or the excellent overview by Kariappa Bheemaiah (2015).

2. To put it in a technical manner, the transactions costs of the keeping and verification of public records collectively rather than by a centralised authority were far too high to justify not having a government for that purpose (Catalini and Gans, 2017).

3. "Crypto-secession" as we might call the Exit from adherence to the institutional structures of States in favour of those organised by blockchain technologies.

4. See Markey-Towler (2017b) which is an informal discussion of certain points in Markey-Towler (forthcoming) on this point of subtlety.

5. Markey-Towler, (2017b) provides a non-technical exposition of these factors.

References

Ackerman, Peter and Kruegler, Christopher (1994) Strategic Nonviolent Conflict, University of Michigan Press, Ann Arbor

Allen, Darcy W. E. and Berg, Chris and Lane, Aaron M. and Potts, Jason, (2017) "The Economics of Crypto-Democracy", Available at SSRN: https://ssrn.com/abstract=2973050

Almudi, Isabel and Fatas-Villafranca, Francisco and Izquierdo, Luis R., and Potts, Jason (2017) "The economics of utopia: a co-evolutionary model of ideas, citizenship and socio political change", Journal of Evolutionary Economics, 27(4), pp.629-662

Almudi, Isabel and Fatas-Villafranca, Francisco and Potts, Jason (2017) "Utopia competition: a new approach to the micro-foundations of sustainability transitions", Journal of Bioeconomics, 19(1), pp.165-185

Berg, Alastair and Berg, Chris, (2017) "Exit, Voice, and Forking", Available at SSRN: https://ssrn.com/abstract=3081291

Bheemaiah, Kariappa, (2015) "Why Business Schools Need to Teach About the Blockchain", Available at SSRN: https://ssrn.com/abstract=2596465

Catalini, Christian and Gans, Joshua S., (2017) "Some Simple Economics of the Blockchain", Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16. Available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598

Commons, John R., (1924) The Legal Foundations of Capitalism, Macmillan, New York

Davidson, Sinclair and De Filippi, Primavera and Potts, Jason, (forthcoming) "Blockchains and the economic institutions of capitalism", Journal of Institutional Economics

Davidson, Sinclair and De Filippi, Primavera and Potts, Jason, (2016) "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology", Available at SSRN: https://ssrn.com/abstract=2811995

Dopfer, Kurt and Potts, Jason, (2007) The General Theory of Economic Evolution, Routledge, London

Earl, Peter, (1986a) Lifestyle Economics, Harvester Wheatsheaf, Brighton

Earl, Peter, (1986b) "A Behavioural Analysis of Demand Elasticities", Journal of Economic Studies, 13(3), pp.20-37

Earl, Peter, (1990) "Economics and Psychology: A Survey", Economic Journal, 100, pp.718-55

Earl, Peter, (1995) Microeconomics for Business and Marketing, Edward Elgar Ltd., Aldershot

Earl, Peter, (2017) "Lifestyle changes and the lifestyle selection process" Journal of Bioeconomics, 19(1), pp.97–114

Habermas, Jurgen, (1962) Structural Transformation of the Public Sphere, MIT Press, Cambridge, Massachusetts

Hamilton, Walton H. (1919) "The Institutional Approach to Economic Theory", American Economic Review, 13(1), pp.92-95

Hart, Herbert L.A., (1961) The Concept of Law, Oxford University Press, Oxford

Hartley, John and Potts, Jason, (2014) Cultural Science, Bloomsbury, London

Hirschman, Albert, (1970) Exit, Voice and Loyalty, Harvard University Press, Cambridge, Massachusetts

Hodgson, Geoffrey, (1998) "The Approach of Institutional Economics" Journal of Economic Literature, Vol. XXXVI, pp.166-192

Hodgson, Geoffrey, (2004) The Evolution of Institutional Economics, Routledge, London

Hodgson, Geoffrey, and Knudsen, Thorbjorn, (2010) Darwin's Conjecture, Cambridge University Press, Cambridge

Landes, David S., (1969) The Unbound Prometheus, Cambridge University Press, Cambridge

Lawson, Tony, (2016) "Comparing Conceptions of Social Ontology: Emergent Social Entities and/or Institutional Facts?" Journal for the Theory of Social Behaviour, 46(4), pp.359-399

MacDonald, Trent J. (2015a), "Spontaneous Order in the Formation of Non-Territorial Political Jurisdictions", Available at SSRN: https://ssrn.com/abstract=2661250

MacDonald, Trent J. (2015b), "Theory of Non-Territorial Internal Exit", Available at

SSRN: https://ssrn.com/abstract=2661226 or http://dx.doi.org/10.2139/ssrn.2661226

MacDonald Trent.J., Allen Darcy W.E., Potts Jason, (2016) "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking", In: Tasca P., Aste T., Pelizzon L., Perony N. (eds) Banking Beyond Banks and Money. New Economic Windows. Springer, Berlin

Markey-Towler, Brendan, (2017a) "Law of the jungle: firm survival and price dynamics in evolutionary markets", Journal of Evolutionary Economics, 26(3), pp.655-696

Markey-Towler, Brendan (2017b) "How to win customers and influence people: Ameliorating the barriers to inducing behavioural change", Journal of Behavioral Economics for Policy, 1(Special Issue: Behavioral Policy and its Stakeholders), pp.27-32

Markey-Towler, Brendan, (2017c) "Economic Dark Matter: On the Theory of Substitutability", Available at SSRN: https://ssrn.com/abstract=2971744

Markey-Towler, Brendan (forthcoming) An Architecture of the Mind, Routledge, London

Marshall, Peter, (1992) Demanding the Impossible, A History of Anarchism, Harper Perennial, New York

McCloskey, Deidre, (2006), The Bourgeois Virtues, University of Chicago Press, Chicago

Metcalfe, Stanley, (1998), Evolutionary Economics and Creative Destruction, Routledge, London

Metcalfe, Stanley, (2008), "Accounting for economic evolution: Fitness and the population method", Journal of Bioeconomics, 10(1), pp.23-49

Murray, Cameron and Frijters, Paul, (2017), Game of Mates, Brisbane

Nakamoto, Satoshi, (2009), "Bitcoin: A Peer-to-Peer Electronic Cash System", Available at URL: https://bitcoin.org/bitcoin.pdf

Nelson, Richard and Winter Sidney, An Evolutionary Theory of Economic Change, Harvard University Press, Cambridge, Massachusetts

North, Douglass C., (1990) Institutions, Institutional Change and Economic Performance, Cambridge University Press, Cambridge

Olsen, Mancur, (1965) The Logic of Collective Action, Harvard University Press, Harvard

Ostrom, Elinor, (1990) Governing the Commons, Cambridge University Press, Cambridge

Page, Karen M. and Nowak, Martin A. (2002) "Unifying Evolutionary Dynamics", Journal of Theoretical Biology, 219(2), pp.93-98

Price, George R. (1970) "Selection and Covariance" Nature, 227, pp.520-521

Price, George R. (1972a) "Extension of covariance selection mathematics", Annals of Human Genetics, 35(4), pp.485-490

Price, George R. (1972b) "Fisher's 'fundamental theorem' made clear", Annals of Human Genetics, 36(2), pp.129-140

Searle, John (2010) Making the Social World, Oxford University Press, Oxford

Williamson, Oliver E. (1985) The Economic Institutions of Capitalism, MacMillan, London

Witt, Ulrich, (2008) "What is specific about evolutionary economics?" Journal of Evolutionary Economics, 18(5), pp.547-575

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(4)2018

Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study

Simon Schwerin[1] MSc
Berlin School of Economics and Law, Germany
Correspondence: simon@schwerins.de

Received: 28 March 2018 **Accepted:** 17 April 2018 **Published:** 19 April 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
SS [1] acknowledges Bruce Pon, Roland Müller andIng. Katarina Adam for their feedback and suggestions on this paper.

Abstract

The present work deals with the interrelationships of blockchain technology and the new European General Data Protection Regulation, that will be intact after May 28th, 2018. The regulation harmonizes personal data protection across the European Union and aims to return the ownership of personal data to the individual. This thesis, therefore, addresses the question how this new technology that is characterized by decentralization, immutability and truly digitized values will be affected by the strict privacy regulation and vice versa. The aim of this work is to clarify whether blockchains can comply with the new regulation on the one hand and to identify how blockchain could support its compliance, on the other hand. The questions are validated through an extensive literature review and are further investigated by using a Delphi study that asks a panel of 25 renowned experts to find opportunities, limitations and general suggestions about both topics. In addition, a framework is proposed to support the assessment of privacy and related risks of blockchains.

Keywords: *blockchain, privacy, data protection regulation, General Data Protection Regulation (GDPR), Delphi study, Data Protection Impact Assessment (DPIA), blockchain Privacy Impact Assessment*

'...To obtain full text of this research study, please visit: http://dx.doi.org/10.31585/jbba-1-1-(4)2018

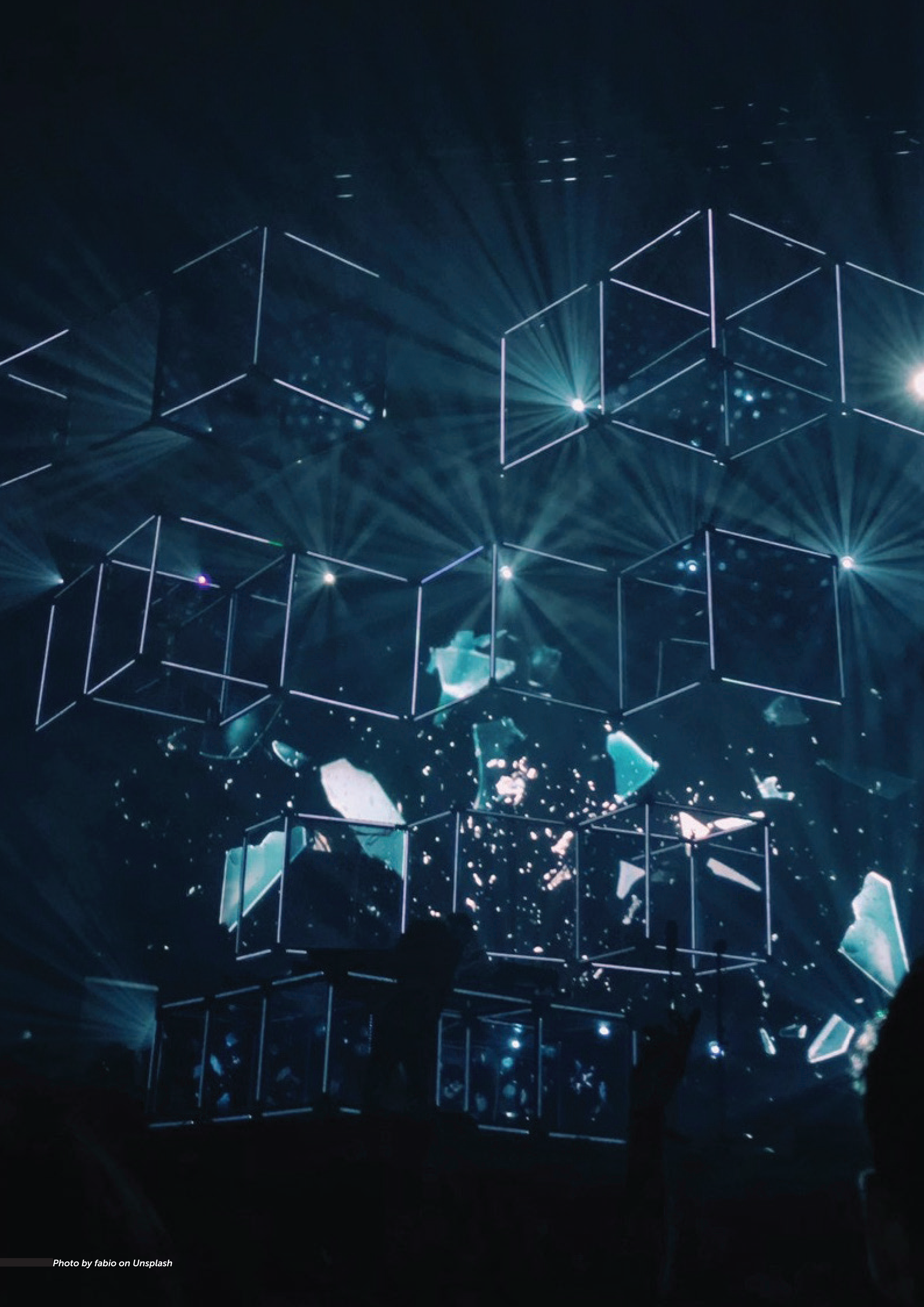


Photo by fabio on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(11)2018

A Future History of International Blockchain Standards

David Hyland-Wood[1] and Shahan Khatchadourian[2]
[1] School of Information Technology and Electrical Engineering,
The University of Queensland, St. Lucia 4067, Queensland, Australia
[2] ConsenSys AG, Zug 6300, Switzerland
Correspondence: d.hylandwood@uq.edu.au
Received: 29 May 2018 **Accepted:** 14 June 2018 **Published:** 29 June 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
DH-W [1] & SK [2] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
Funding is provided by ConsenSys.

Acknowledgements:
DH-W [1] & SK [2] acknowledges Vanessa Bridge, Robert Coote, Matt Halpern, Grant Noble, and Peter Robinson of ConsenSys AB, and Mariano P. Consens of The University of Toronto, and Marius Portmann of The University of Queensland for their feedback and suggestions on this paper.

Abstract

Blockchain and blockchain-related technologies are being rapidly invented to the point that it is difficult to define specifically which properties are necessary to constitute a blockchain. It may therefore seem far too early to meaningfully discuss the creation of international blockchain standards. This article will argue the opposite by summarizing some existing international standards work related to blockchains and propose directions for additional standards development that could meaningfully be explored in the near future without negatively impacting additional invention.

Keywords: *Blockchain, distributed ledger, standards, consensus, decentralisation, interoperability, identifiers, BPMN, enterprise systems.*

Introduction

Any new technological paradigm wherein implementations have similar or overlapping functionality by many vendors has historically seen vendor cooperation via international standards development organizations (SDOs). We categorize international standards into two broad areas. Backward-looking standards formalize existing de facto implementations into a specification, e.g. ECMAScript (ISO 2018). Forward-looking standards fill gaps between black-box implementations by creating a specification that defines how such different systems may communicate, generally for the purpose of assisting interoperability, which we consider to be communications between systems that are "liberal in what you accept, and conservative in what you send" (Braden 1987). Recent and obvious examples include the development of international standards defining the World Wide Web, e.g. HTTP (Fielding et al. 1999), URL (Berners-Lee, Fielding, and Masinter 2005), HTML (Faulkner, Eicholz, Leithead, Danilo, and Moon 2017), the Internet and the TCP/IP (Braden 1987) family of protocols that includes its OSI (ISO 1994) conceptual abstraction and application-level protocols such as DNS (Mockapetris 1997), as well as other industry standards like relational databases, e.g., SQL (ISO 2016), and mobile telephones, e.g., GSM (3GPP 1999). Each of the mentioned standards began as technical implementations which were later harmonized into international standards as they converged and matured. It seems reasonable to expect blockchain technologies to follow a similar course.

There is little agreement within the blockchain community on the very definition of a blockchain. Ten years ago, Bitcoin (Nakamoto 2008) was the blockchain. Within a few years, others had implemented variations on a theme, some of which added substantial innovations, such as Ethereum's (Buterin 2013, Wood 2014) introduction of a Turing-complete virtual machine for execution of smart contracts (Szabo 1994), a computerized transaction protocol that executes contract terms, which Ethereum enables through algorithmically specifying and autonomously enforcing rules of interaction. After a decade of constant innovation in various (often competing) directions, what exactly is a blockchain?

One reasonable answer is that a blockchain is a public distributed ledger technology (DLT) used for the transfer of cryptocurrencies. That definition certainly matches Bitcoin, although it leaves out later innovations including the flexibility of smart contracts. Many newer blockchains would argue to exclude the word "public" or even the transfer (or existence) of cryptocurrencies. Should the resulting definition then be that a blockchain is a distributed ledger?

We argue not.

Imagine that one wished to create a simple double-entry accounting system in software. Each transaction is entered, a new running total is calculated, and the entire record stored. They might call each record a "block". Each record (or block) is linked (perhaps not even cryptographically) to the previous record. To keep data safe, the transaction is uploaded to a remote machine, which in turn copies it to other machines. They would have made a distributed ledger. Have they made a blockchain? Probably not. Surely blockchains have other intrinsic features such as cryptographically linked blocks to provide the feature of nonrepudiation, atomic commits, and a presumption of a peer relationship between nodes. Some might argue that a common consensus algorithm to determine block additions is also necessary.

In Table 1, we show several blockchains that support a variety of consensus algorithms, including proof of work (PoW), proof of stake (PoS), proof of authority (PoA), as well as byzantine fault tolerant (BFT) variants. Essentially, a consensus algorithm provides an atomic commit capability in which peers on a blockchain network agree on the blockchain network's current state as well as any state updates. Furthermore, consensus algorithms affect how blockchain networks enable peers to engage with each other. In one instance, a public blockchain network, such as Ethereum's public network, intends to provide fair ability for peers of its peer-to-peer network to observe, validate, and participate in blockchain state updates. In private, permissioned settings, as supported by blockchains like Quorum and Hyperledger Fabric, more efficient BFT variants allow higher transaction throughput by restricting scalability in the number of peers actively participating in the consensus algorithm. In providing a range of modular, pluggable consensus algorithms, and with their integration at different layers of what is often seen as a decentralizing technology, it is a challenge to define and distinguish blockchains from their DLT counterparts.

The authors suggest that the current difficulty in defining a blockchain argues strongly against the creation of backward-looking standards. There is as yet simply no agreement as to which features a de facto blockchain possesses, nor is there broad agreement on a reference architecture. Facing such a challenge, it becomes especially important to free blockchains and DLTs from standardization that can impact their future development. We therefore suggest that SDOs do not pursue development of such standards at this time, focusing instead on future standards development.

This article explores areas and directions related to interoperability between different blockchains, between blockchains and blockchain-like technologies, and between blockchains and traditional technologies. A survey of existing and forthcoming standards is presented, and some suggestions made for future standards development.

Methods

In this short paper, we review existing international standards, including those that are related to blockchain technologies, followed by a survey of international standards development organizations to determine current work related to blockchain technologies. The authors then extrapolated informal likelihood of success of various efforts based upon knowledge of both emerging blockchain industry participants and the structure and concerns of standards development organizations. Suggestions for success criteria and likelihoods of success, as well as proposals for future standards efforts, are the conjecture of the authors.

Since SDOs are generally reluctant to develop new technologies, we categorize their activities into two predominant (sometimes opposing) directions: The first is to formally agree to some practices that already have wide adoptions, the so-called industry or de facto standards. The second is to create means to better allow competing interests to interoperate, in particular, the many national and international SDOs allow for standardization adoption at various levels of jurisdictions to address cultural, regional, and legal differences (Fyrigou-Koulouri 2018). It is in this latter area where we suggest the most useful blockchain standards could assist growth in the field.

We propose three areas for future interoperability standards: a representation of smart contracts in BPMN systems to integrate blockchain systems into enterprise modelling systems, decentralized identifiers to facilitate cross-blockchain identity, and interledger protocols to reduce data boundaries between blockchain systems.

Results

In this section, we review several existing and proposed enterprise and blockchain standards and relate them to technologies that we believe play a critical role in the advancement of blockchain standards.

Existing standards are relevant to the goal of interoperability between blockchains while also enabling flexible development of future blockchain technologies. Existing technologies not only allow interoperability between public blockchains, enterprise blockchains, and existing enterprise systems, they also support the extensibility of blockchain standards and their enterprise variants. One example of this arises with companies that are looking to integrate decentralized applications into their current businesses processes. Reasons to do so include cost reduction, increased transparency, as well as benefiting from novel privacy and security schemes. As an existing standardized enterprise technology, BPMN is well-suited for enabling interoperability between blockchains in a variety of ways. First, BPMN supports interoperability between existing enterprise technologies and blockchain networks using typical approaches to service orchestration and choreography. These approaches are also applicable in the interoperability between public blockchain networks and private, permissioned variants, although their diversity and distinctiveness continue to undergo ongoing community debates (Buterin 2015, Khatchadourian, Lubin, Millar, & Buterin 2017, Ferris 2018, Allison 2018). It is important to note that the use of existing enterprise standards, such as BPMN, does not restrict how blockchains are used nor their future development.

Several forward-looking standards either exist or are in progress. Figure 1 summarizes the Enterprise Ethereum Client Specification version 1.0 developed by the Enterprise Ethereum Alliance (EEA) (Enterprise Ethereum Alliance 2018). As far as the authors are aware, that specification represents the first blockchain standard created and approved by an SDO. The specification was publicly announced on 16 May 2018 and is the sole entry in Table 2, which lists existing blockchain standards.

Standardization efforts known to be being actively pursued at the time of this writing are listed in Table 3.

A list of current exploratory efforts at SDOs is provided in Table 4. It is worth noting that many exploratory efforts are likely to be abandoned prior to standardization. A recent example is the expired effort at the IETF to apply Application-Layer Traffic Optimization techniques to blockchains (Hommes 2017).

Many blockchains have developed implementation-specific APIs to allow applications such as cryptographic wallets and cryptocurrency exchanges to communicate with blockchain nodes. One might be tempted to conclude that standardization of such APIs could be fruitful areas for backward-looking standards development. However, blockchain-specific APIs are unlikely to generalize well across radically different technical implementations. Furthermore, it may be possible to develop general protocols to represent high-level conceptual actions such as data migration, data copying, cryptocurrency exchange or transfer, cross-chain smart contract operations, etc. Generalized protocols are more likely to be standardized than APIs as shown historically by successful standards efforts such as HTTP or the TCP/IP family.

In this section, we described existing blockchain standards that have focused on the interoperability of existing blockchain technologies, as well as ongoing standardization efforts and explorations. In the next section, we discuss the relevance of these standardization efforts with respect to interoperability of future blockchain developments.

Discussion

The International Standards Organization (ISO) is currently the only SDO actively pursuing backward-looking standards development related to blockchains. In an attempt to understand and ground the blockchain space, ISO's TC 307 Technical Committee is defining a reference architecture, taxonomy and ontology. Blockchain-related formal vocabulary is also being collected. As mentioned above, the rapid invention of blockchain types and the lack of an industry-wide agreement on a definition of a blockchain make such work particularly difficult. The authors believe such work to be premature.

A more productive approach is likely to be found by considering standards development in areas with the following properties:

- Pre-competitive or non-competitive areas of interest to blockchain developers and vendors (necessary with SDOs to preclude formal objections from disadvantaged vendors);
- Specifications that seem likely to enhance interoperability between different types of blockchains;
- Activities that would not limit explorations or invention of additional cryptography, privacy, consensus, management, or similar features of any individual blockchain.

We thus conclude that forward-looking interoperability standards are most likely to result in successful standards creation and facilitate industry growth.

We expect blockchain standards to mature in areas that foster interoperability. Apparently fertile areas for standardization would include those efforts that would assist with interoperability between blockchain implementations and between blockchains and established enterprise information systems. In neither area would vendor representatives to SDOs likely see competitive disadvantage.

Examples of work that would foster interoperability between blockchains include decentralized identifiers (Reed et al 2018), being considered for standardization at the W3C, verifiable claims (Burnett et al 2017), a data model and message syntax currently being standardized at the W3C, and various attempts to define interledger protocols. Decentralized identifiers would allow a given user to take coordinated action on multiple blockchains using a single identity. Verifiable claims take advantage of blockchains' properties of being difficult to write yet simple to read to represent common social claims (including identity). Interledger protocols would facilitate necessary and common operations such as data migration from one blockchain to another, facilitate the creation of smart contracts that operate on information held by multiple blockchains, and allow data held canonically by one blockchain to be readily validated by another.

Two interledger protocols have been proposed: The Interledger Protocol (W3C Interledger Payments Community Group 2018) has been proposed by Ripple to allow cross-blockchain payments. The Web Ledger Protocol (Sporny and Longley 2018) has been proposed by the W3C Blockchain Community Group.

Some existing or upcoming standards efforts would support interledger protocols, such as the W3C's Verifiable Claims and Decentralized Identifiers. A properly specified and widely adopted interledger protocol would benefit from a decentralized identifier scheme to provide common user information across blockchains. The concept of operations of Verifiable Claims would be more easily implemented in an environment where a standard interledger protocol and decentralized identifiers exist and are adopted.

As an existing enterprise standard that is agnostic to blockchains, BPMN has successfully enabled blockchain interoperability in proof of concepts. However, enterprises could gain additional benefits from the consideration of significant blockchain paradigms in BPMN's evolution. For instance, defining new role and activity types based on decentralized identifiers and smart contracts, potentially hosted on one or more decentralized peer-to-peer systems, could help businesses define, model, and validate their processes more easily and accurately.

Table 5 lists suggested areas for potential standardization that have the desired properties.

Conclusions and Further Work

The current state of blockchain standards is both nascent and exploratory. Two existing international SDOs are currently producing blockchain standards (W3C and EEA), and several others are exploring future standards development (ISO, IEEE, IETF, IRTF, and OMG).

Of the SDOs currently pursuing blockchain-related standards development, the authors propose W3C as the best candidate for interledger protocol development if the consortium's membership allow for a broadening of the definition of the World Wide Web (W3C 2017). ISO, as a body consisting primarily of national standards bodies is unlikely to agree on interledger protocols in a time frame that will promote market growth. The missions of IEEE, IETF, and IRTF are rather far afield from application-layer protocols. The EEA's mission is specifically limited to the Ethereum blockchain, and the EEA executive has expressed a desire to produce a single blockchain client standard. The W3C could readily adopt work on blockchain protocols if (and only if) their membership permits the consortium to accept blockchain's "Web 3.0" positioning as a broadening of the definition of the World Wide Web. The current W3C definition of the Web is based on the HTTP and HTML client-server structure of the historic Web. We propose that the W3C broaden their definition of the Web to include any peer-to-peer or other non-client-server protocol relationships between components. Such a broadening of mission might be easier than establishing a new SDO with a mandate specific to blockchain developments.

The authors support continued development of cross-chain smart contract specifications at the W3C and ISO and propose that extensions to the existing BPMN standards be conducted at the Object Management Group.

Efforts by national standards organizations were not comprehensively surveyed by the authors. National standards organizations, e.g. the American National Standards Institute (ANSI), Standards Australia (SA), and Standardization Administration of China (SAC), coordinate national interests with ISO and other international SDOs. The authors note that several such organizations (including the ones named) have some local efforts to explore blockchain standardization. A comprehensive survey of those activities would be a valuable additional contribution, and hopefully lead to a more complete understanding of worldwide efforts.

References

3rd Generation Partnership Project (3GPP), Technical specifications and technical reports for a GERAN-based 3GPP system, 1999, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=5.

Allison, I., Public or private? blockchain distinctions are falling out of fashion, 2018, https://www.coindesk.com/public-private-blockchain-distinctions-falling-fashion/.

Berners-Lee, T., Fielding, R. and Masinter, L., Internet Engineering Task Force, IETF RFC 3986, Uniform resource identifier (URI): generic syntax, 2005, https://tools.ietf.org/html/rfc3986.

Braden, R. (ed), Internet Engineering Task Force, IETF RFC 1122, Requirements for internet hosts -- communication layers, 1989, https://tools.ietf.org/html/rfc1122.

Buterin, V., Ethereum white paper, 2013, https://github.com/ethereum/wiki/wiki/White-Paper.

Buterin, V., On public and private blockchains, ethereum blog, August 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

Enterprise Ethereum Alliance. Enterprise ethereum client specification v1.0, 2018, https://entethalliance.org/resources/.

Faulkner, S., Eicholz, A., Leithead, T., Danilo, A. and Moon, S., HTML 5.2, W3C recommendation, 2017, https://www.w3.org/TR/html/.

Ferris, C., Two enter, one leaves, May 2018, https://developer.ibm.com/code/2018/05/11/two-enter-one-leaves/

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and Berners-Lee, T., Internet Engineering Task Force, IETF RFC 2616, Hypertext transfer protocol -- http/1.1, 1999, https://tools.ietf.org/html/rfc2616.

Fyrigou-Koulouri, M., Blockchain technology: an interconnected legal framework for an interconnected system, 9 Case W. Res. J.L. Tech. & Internet 1 (4th), 2018, https://scholarlycommons.law.case.edu/jolti/vol9/iss1/7.

Hommes, S., Fiz, B., State, R., Zuenko, A., Caetano, R. and Gurbani, V. ALTO for the blockchain, expired internet-draft (individual), 2017, https://datatracker.ietf.org/doc/draft-hommes-alto-blockchain/.

International Organization for Standardization, ISO/IEC 9075:2016 Information technology -- database languages -- SQL -- part 1: framework (SQL/framework), 2016, https://www.iso.org/standard/63555.html.

International Organization for Standardization, ISO/IEC 7498-1:1994 Information technology -- open systems interconnection -- basic reference model: the basic model, 1994, https://www.iso.org/standard/20269.html.

International Organization for Standardization, ISO/IEC 22275:2018 Information technology -- programming languages, their environments, and system software interfaces -- ECMAScript® specification suite, 2018, https://www.iso.org/standard/73002.html.

Khatchadourian, S., Lubin, J., Millar, J. and Buterin, V., Enterprise ethereum alliance - vision, 2017, https://www.researchgate.net/publication/325655669_Enterprise_Ethereum_Alliance_-_Vision.

Mockapetris, P., Internet Engineering Task Force, IETF RFC 1035, Domain names - implementation and specification, 1987, https://tools.ietf.org/html/rfc1035.

Nakamoto, S., Bitcoin: a peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R. and Sabadello, M., Data model and syntaxes for decentralized identifiers, draft community group report, May 2018, https://w3c-ccg.github.io/did-spec/.

Sporny, M. and Longley, D., Verifiable claims data model and representations, W3C first public working draft, August 2017, https://www.w3.org/TR/2017/WD-verifiable-claims-data-model-20170803/.

Sporny, M. and Longley, D., The web ledger protocol 1.0, draft W3C community group report, June 2018, https://w3c.github.io/web-ledger/.

Szabo, N., Smart contracts, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

W3C. W3C mission, 2017, https://www.w3.org/Consortium/mission.

W3C Interledger Payments Community Group. Interledger protocol v4, draft W3C community group report, 2018, https://interledger.org/rfcs/0027-interledger-protocol-4/.

Wood, G., Ethereum: a secure decentralised generalised transaction ledger, ethereum project yellow paper 151, 2014, https://ethereum.github.io/yellowpaper/paper.pdf.

Tables

Table 1. Variations of "Blockchains" and their Consensus Algorithms

Project/Product	Consensus Algorithm
Bitcoin	Proof of Work (PoW)
Ethereum	PoW, Proof of Authority (PoA), Proof of Stake (PoS)
Hyperledger Fabric	Practical Byzantine Fault Tolerance (PBFT)
Hyperledger Sawtooth	Proof of Elapsed Time (PoET)
Quorum	Raft, Istanbul BFT (IBFT)
Corda	Validity and Uniqueness
Veres One	Leaderless electors
Hashgraph	Gossip about Gossip/Virtual Voting
Byteball	SPECTRE

Table 2. Existing Standards

SDO	Effort
EEA	Enterprise Ethereum Client Specification v1.0

Table 3. Current Standardisation Efforts

SDO	Effort
W3C	Verifiable Claims data model and message syntax
EEA	Enterprise Ethereum Client Specification v1.1

Table 4. Current Explorations by Standards Development Organisations

SDO	Working Group	Exploration
ISO	• ISO/TC 307/SG 1 Reference architecture, taxonomy and ontology • ISO/TC 307/SG 2 Use cases • ISO/TC 307/SG 3 Security and privacy • ISO/TC 307/SG 4 Identity • ISO/TC 307/SG 5 Smart contracts • ISO/TC 307/SG 6 Governance of blockchain and distributed ledger technology systems • ISO/TC 307/SG 7 Interoperability of blockchain and distributed ledger technology systems • ISO/TC 307/WG 1 Foundations • ISO/TC 307/WG 2 Security, privacy and identity • ISO/TC 307/WG 3 Smart contracts and their applications	• Vocabulary • Reference architecture • Taxonomy and Ontology • Legally binding smart contracts • Identity • Cross-chain contracts • Security risks
IRTF	• Decentralized Internet Infrastructure Research Group	• Decentralizing infrastructure services (e.g. P2P transport and naming)
IEEE	• P2418	• IoT security • Pharma provenance • Digital identity
W3C	• Not yet established	• Decentralized identifiers
EEA	• Core Layer • Integration Layer	• Vertical industry-specific extensions

Table 5. Proposed Standards Development

Possible SDO	Area of Interoperability
W3C	• Interledger protocol(s)
ISO, W3C	• Cross-chain smart contracts
OMG	• BPMN

Figure captions

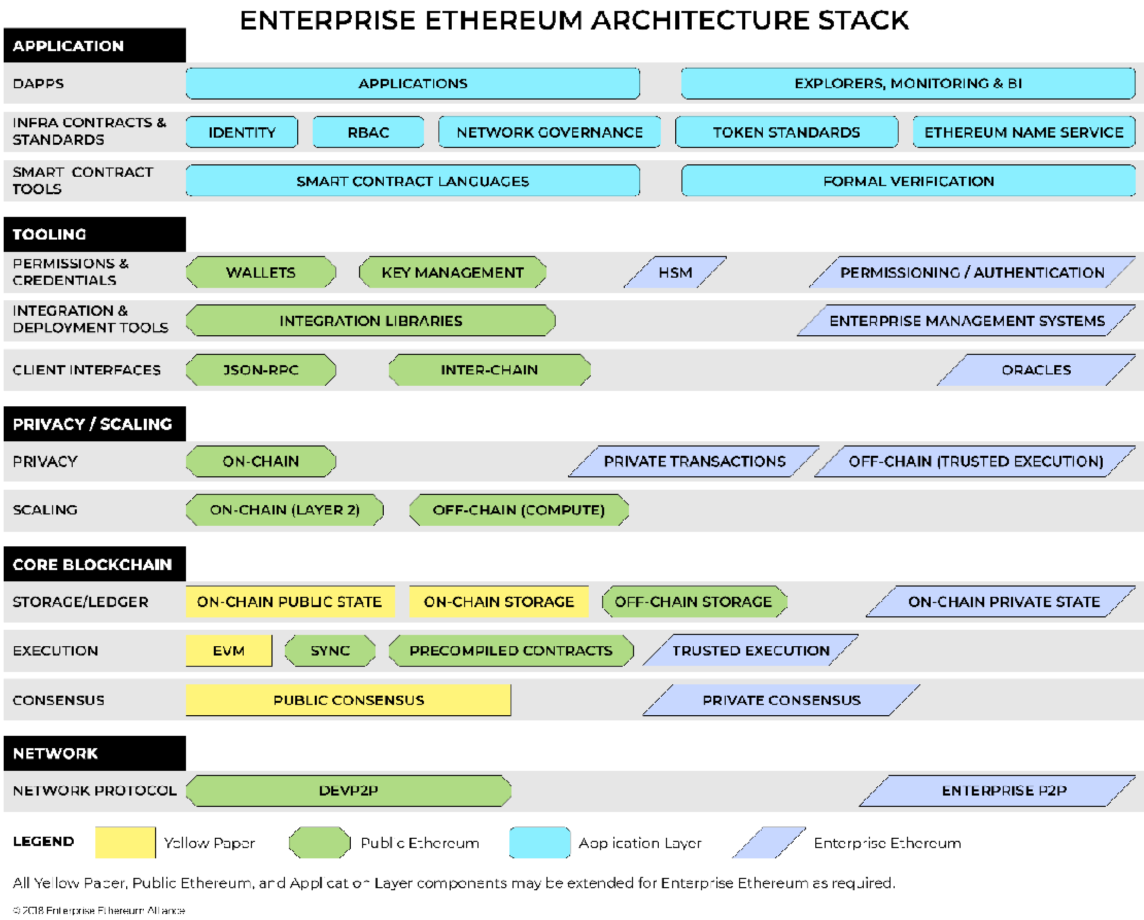


Figure 1. Enterprise Ethereum Stack Diagram

"BLOCKCHAIN HAS THE POTENTIAL TO REFRAME THE ROLE OF THE STATE"

Portrait courtesy The House of Lords

INTERVIEW WITH

LORD HOLMES OF RICHMOND MBE

UK Blockchain APPG Vice Chair

Interview conducted by Helen Disney

Our journal has a global reach and a broad international readership, so for people who may not know you, who is Chris Holmes and what is your long-term vision of Blockchain and why it matters?

I grew up in a working class town where aspirations for kids were low – at best, you were expected to do woodwork or metalwork or something of that sort. I was lucky enough to do something different and my journey took me to Cambridge University then into a law firm and eventually I became Director of Paralympic Integration, responsible for the organisation of the 2012 Paralympic Games in London, which is ultimately why I ended up in the House of Lords.

There was always a technology thread running through what I did right from when I got my first Sinclair ZX Spectrum and used to spend my time playing computer games like Manic Miner! Then, after I lost my sight overnight at the age of 14, technology became my lifeline – it was something that helped me cope and survive.

When I entered the Lords, the first select committee report I was involved in was on technology and, most recently, I've been a member of the Select Committee on Artificial Intelligence in the UK. Our first report and recommendations were published in April 2018. More broadly, as co-chair of various All-Party Parliamentary Groups I am interested in all aspects of the 4th Industrial Revolution and I see blockchain as a key part of that. My initial interest in the blockchain space came though a concern that there was so much potential for deployment of blockchain for public good but the only thing that seemed to be known about blockchain among public servants was bitcoin. I didn't want blockchain to be inextricably linked with bitcoin in the public mind and I didn't want a crash in the bitcoin price to derail efforts to use blockchain or distributed ledger technologies for public good. I see this technology as too important to be left just to the technologists. In other words, I think it also needs to be rooted in real-world problems.

Let's take border control problems as just one example. Could blockchain solve the Northern Ireland border control problem by 29 March 2019? No. But in the longer-term, the application of blockchain could profoundly change the way we see borders and our experience of going through an airport would be radically different in the future. The same argument can be applied to supply chains or welfare benefits. Ultimately I see that blockchain has the potential to reframe the role of the state and fundamentally reimagine the social contract between citizen and government.

There is a lot of hype around blockchain and it is said that DLT is not a silver bullet, so how do we separate facts from fiction and what lessons can be learnt from the journey to date?

To slightly misquote the pop star Jessie J: "it's not just about the money, money, money". What do I mean by that? I think that in this case, implementing blockchain is not about expecting the government to allocate large amounts of resources or taxpayers' money. Instead, I see the Government's role as signalling interest, playing an enabling role and sending out a positive message that blockchain is worth exploring. We might also want to nail our colours to the mast by just taking even a handful of specific use cases – intractable issues that have been around for decades – and saying we will incubate that, who wants to have a go at fixing that? That could be passports or food security or any other use case. Government's role is my mind is ultimately as an enabling state.

What is your message to countries that are experimenting and trying to adopt Blockchain technology? What can other countries learn from Britain?

The Walport report was an excellent piece of work and probably could have gone even further if external politics had not intervened. My own report on Distributed Ledger Technologies for Public Good was built on those foundations – building understanding, setting out recommendations, reaching out to academia and also getting the private sector more involved with government projects. I think the key lesson I have learned in all aspects of the 4th Industrial Revolution is around the need for collaboration. We can't enable a kind of blockchain 'arms race', however, so interoperability or work on interledger activity is much needed. If the advent of blockchain does indeed end up having the same impact as the arrival of the Internet, as many people have argued, we need to capture its benefits and find effective solutions for the public good.

And what can Britain learn from countries that have successfully implemented blockchain/DLT (e.g. Dubai, Estonia etc.) in terms of creating a national strategy?

I think what Estonia shows us is the importance of leadership – it shows how much can be done when leaders have a vision they believe in and really drive it forward. But we should also not forget that Estonia is a very small country compared to the UK and has a very different political history and context for decision making so it's always hard to compare like with like when you make national policy comparisons. Dubai also shows what can be done through political will and committing funds.

In the UK, what we are trying to do is find a governance structure that enables both public and private sector activity but which cannot become dominated by either. And we need to always track this back to the purpose. What is the purpose of blockchain if not to solve entrenched problems that have existed for decades and find new ways of dealing with them?

"Peer-review is a critical part of the process of becoming a trusted source of information because it builds authority and leads to increased collaboration and creativity, so I welcome the arrival of the journal and look forward to reading it."

What do you see as the key challenges and roadblocks for public and private sector implementation of blockchain projects?

I think the roadblocks in the public and private sectors are probably not that different because I think on both sides it is about organisational change and new ways of thinking. If we look at the Department for Work and Pensions' proof of concept, which took place in the North West of England, it's a good example. A fantastic pilot was conducted with 20 benefit recipients who had a tokenised benefit run on a blockchain. This not only proved the worth of the infrastructure in terms of the platform and the technology being used but also even more significant, in my view, was the people part. Real-life benefit recipients got to use the system, become familiar with the technology, give feedback on how it worked and contribute their own ideas. Active engaged citizens then become consultants on the programme. Sadly, this project didn't go any further forward because it was not prioritised. In that respect, and going back to the question of leadership, Lord Freud's departure was a great loss.

Going forward there is always fear about changing something that is "mission critical" so it is likely to be easier and will alllow us to build in a comfort factor if we pick on significant but scaleable use cases and show people rather than tell them what the benefits of blockchain are likely to be.

In the private sector, I think companies can minimise problems by building partnerships in a shared endeavour where relationships are built for the longer-term and therefore become less transactional. I imagine it a bit like the journey to the South Pole where many different funders and actors played a part but all with the common goal of exploring our world.

Overall, the key challenges are the need for strong leadership, combined with the need to overcome organisational design issues and inertia and the need to keep educating leaders in business and public policy. As policymakers, we don't need to be soothsayers. It's not a kind of "Tomorrow's World on speed" approach where we try to pick winners. I'm always reminded of the story of the Air Ministry asking the boffins to make them a ray gun. They didn't end up with the gun but they did end up with radar instead. It is always worth experimenting and going on innovation journeys and it's not necessarily our role to worry about what the final destination will be.

The British Blockchain Association (BBA) now has a presence in 6 continents, an active network of students, academics, thought leaders, influencers and blockchain companies. How would you like to see the BBA positioning itself among the global community and taking leadership?

My hope for the BBA is that it can provide a credible, coherent and authoritative voice. In that sense, the key aspect is not under or over-claiming about what blockchain and DLT can do but rather playing a role in telling truths, sharing information and research and providing a connecting hub for what is happening in policymaking in different jurisdictions, as to how that may affect the UK.

The Journal of The British Blockchain Association is Europe's first Peer reviewed Journal on Blockchain technology. We have done a lot of work on establishing a pool of academics, publishing proofs of concept, knowledge transfer, and dissemination of evidence-based research? Any advice/ suggestions for us as we move forward?

Peer-review is a critical part of the process of becoming a trusted source of information because it builds authority and leads to increased collaboration and creativity, so I welcome the arrival of the journal and look forward to reading it.

How would you envision stakeholders' involvement in the advancement of blockchain technology and the role BBA could play in the education, training, collaboration and networking to benefit the global community in general and the UK in particular? How can the BBA best help and support the government to advance its vision?

The UK is taking a somewhat different path from other countries like the USA or France when it comes to Blockchain and cryptocurrency regulation. The challenge is not to make a kneejerk reaction. We want to avoid a "something must be done" approach which often ends in a sort of Dangerous Dogs Act approach. Instead, our approach has been quite British and very considered, for example, the creation and expansion of the Financial Conduct Authority (FCA) sandbox which has been admired all over the world. I'd like us to continue down that line – being positive and inclusive but also pragmatic. BBA's support in that endeavour and in sharing global examples of best practice would be very welcome.

In terms of future vision, I believe we have only achieved true cross-governmental working once in the past - for the 2012 Olympics and Paralympics where 18 different government departments had to pull together to achieve a major infrastructure project. I think blockchain and DLT could ultimately help us to do that again and maybe in a more systematic way so that Britain can truly become the innovative country we want to be and should be.

UK Parliament / CC

Photo by Thomas Kvistholt on Unsplash

ANALYSIS

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(9)2018

The Internet of Public Value

John Reynolds[1]
Blockchain Digital, London, United Kingdom
Correspondence: john@blockchaindigital.co.uk
Received: 29 May 2018 **Accepted:** 5 June 2018 **Published:** 7 June 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
JR[1] prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Not declared.

Abstract
The UK Government is under growing pressure to improve the performance of public services whilst reducing costs. Services are under stress at a national and local level. This pressure to improve the value being delivered to citizens whilst reducing operational costs and risks is analogous to the pressure the financial service industry has been under since 2008. Financial services organizations are increasingly turning to Distributed Ledger Technology (DLT) to address these challenges. Distributed ledger technology is enabling a new paradigm in financial services where organizations collaborate and integrate at the infrastructure and transaction level, freeing up resources for innovation and competition at the application and value proposition level; what we are seeing is wholesale business model transformation.
This paper explores how a new Public Value Network might enable Public Service Organizations to retain their existing decentralized business models, (budgets, decision making, business, service design) yet optimize and synchronize locally and nationally, collaborate in the design and delivery of frictionless human centric services, automate- services, adherence to and auditing of regulation, policy and process and improve financial transparency across public service value chain.
Keywords: *Distributed Ledger Technology, Public Value Network, Internet*

Imagining a new Public Value Network for the UK based on a Distributed Ledger Platform

1. Challenge

UK Public Services are no longer affordable, and there is a growing expectation gap between what citizens want from their public services and what is affordable.

Citizens' expectations are met on the front line, by the doctor, teacher, social worker, policeman, inspector, council worker and the public-facing civil servant.

2. Approach

The only viable approach to closing the expectation gap in a world of declining tax revenues and therefore declining budgets, is to make a bigger impact with the existing resources, to remove friction, cost and duplication so services can be optimized and synchronized enabling resources to be moved to front-line services that deliver direct value for the citizen.

3. Opportunity

It has been estimated that reducing back office administration by 40% could free up £46bn per year for front line services.

The first generation of the digital revolution brought us the Internet of information. - Don Tapscott

With the 1st generation of the internet brought us the large platform providers, Google, Facebook and Amazon. Governments looked at these innovative platforms and thought, surely government can be more like these businesses? Surely government can learn and replicate these business models and yes, over the past 20 years central and local government has made progress in replicating these business models, removing front line staff, carrying out 'channel shift' where, instead of talking to a person, you talk to an Interactive Voice Recognition (ICVR) system or navigate a website.

Progress has been made also with reducing costs by consuming cloud-based services from large platform providers like: Azure AWS, Office 365, SharePoint, and ServiceNow - just an example of some of the common shared services that have been widely adopted by public service organisations.

Yet despite 20 years of digitizing government, we have not achieved one fully integrated, fully optimise identity that delivers cohesive fully joined-up public services. On one level, despite all the funding and energy invested in building this so-called *'fully integrated'* business model for the delivery of public services it feels like public services are still very disconnected and distinct; but then again, is it a bad thing that the delivery and culture of the service for doing farm inspections is very different than the service that provides mental health support to teenagers?

Is our awe of Facebook and Amazon as templates for Public Services still valid? Should we be holding up business models of platform / advertising providers that harvest and monetize user data up as exemplars for the design and delivery human centered public services?

The second generation—powered by blockchain technology—is bringing us the Internet of value: a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better. - Don Tapscott

Imagine a world where instead of trying to turn the 25 ministerial departments, 20 non-ministerial departments, 300+ agencies, local councils, schools, police and wider public services into a commoditised, homogenised version of Amazon; we decided to embrace, celebrate and empower the individual specialisms and purpose of each organisation delivering a public service. What if instead of battling against the decentralised nature of these organisations culture, values, budgets, workforce and the unique character of their services we seek to radically embrace and optimise the rich tapestry of UK public service delivery?

Want to know how to deliver great public services? Ask the Bankers!

What about instead of looking to internet companies for the answers on how to make UK public service affordable, we looked instead to financial services? Asking bankers how to deliver public services might seem ridiculous, but banks have far more in common with public service providers than Amazon or Facebook. Banks are heavily regulated, they touch the lives of every citizen, they provide face-to-face services and, like UK Public Services, they have been under massive strain to join up service and reduce costs. The following are two extracts that articulate the challenges in the financial services sector:

'Market infrastructure has evolved incrementally over years without consistent architectural design and is characterised by siloed data stores, maintained independently by each participant. The redundant storing of common information provides resilience but gives rise to expensive and time-consuming reconciliation activities between siloed data stores as each market participant strives to ensure their books match those of their counterparties.' *(Digital Asset Holdings White Paper Dec 2016)*

'In particular, each financial institution maintains its own ledgers, which record that firm's view of its agreements and positions with respect to its customer set and its counterparts. Its counterparts, in turn, maintain their views. This duplication can lead to inconsistencies, and it drives a need for costly matching, reconciliation and fixing of errors by and among the various parties to a transaction. To the extent that differences remain between two firms' views of the same transaction, this is also a source of risk, some of it potentially systemic. A plurality of financial institutions drives competition and choice but the plurality of technology platforms upon which they rely drives complexity and creates operational risk.' *(R3 Corda: An Introduction August 2016)*

Here's a quote from a March 2018 paper on UK Public Services:

"Be spoking your own finance or payments system, or hand-cranking your own local licensing system (instead of consuming one already available) are now no longer a productive or cost-efficient use of public resources. "Yet this is effectively what much of the public sector is doing, in multiple places across many organisations—and all at great cost. Such large-scale duplication of commodity functions and processes offers little or no value to citizens. Instead, it consumes precious resources that should be going to the front line and prevents services from joining up properly around the needs of citizens and public-sector workers alike' *(Better Public Service a Manifesto 2018)*

What's clear is that the essence of the problem is the same, and we believe the technology solving the problem for financial services can also solve the problem for Public Services.

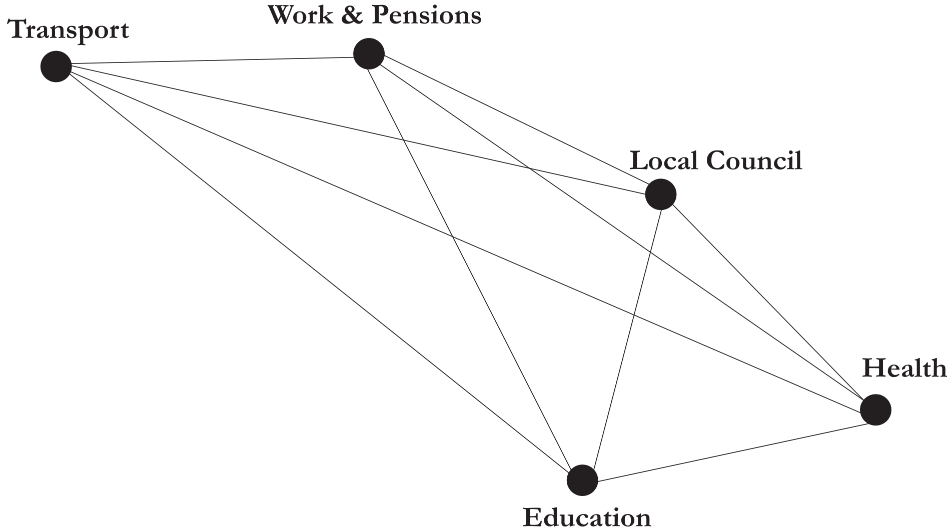
Corda

To refine the remainder of this paper and get a little more specific, we have chosen to zoom in on Corda, an open source blockchain platform built specifically for financial services but with far wider applicability.

The Internet of Public Value

1. How might this new Internet of Public Value enable Public Service Organisations to retain their existing decentralised business models (budgets, decision making, process, partners, value proposition and service design) yet optimize and synchronise locally and nationally?

The key point about this question is that, instead of trying to completely re-engineer the highly distributed tapestry of public service organisations' business models into some type of centralised 'platform' type business model, we seek to optimise, reduplicate and



Based on a Corda Distributed Ledger Network

synchronizse the existing public service network.

The first building block would be for each actor in the public service network to have their own node as illustrated *above*.

The first thing to note about a public service organisation on boarding to the Public Value Network is that they would (within the context of the overall network) individually fund, design, build and support their own node. Risk, reward and investment for joining the Public Value Network would be owned by the individual public service organisations, not with some central mega project team. There is a long list of examples where this centralised project approach has failed, including:

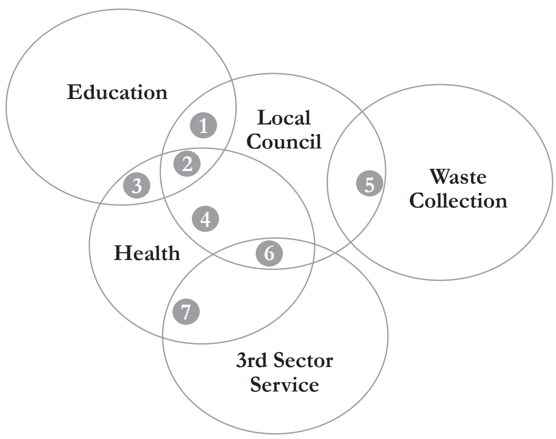
1. NHS IT—The £12.7bn National Health Service National Program for IT (NPfIT)
2. The Department for Transport's Shared Services—was initially forecast to save £57m
3. £7.1bn Defence Information Infrastructure (DII)
4. £350m Single Payment Scheme system (SPS)
5. Map of the Public Value Network

As part of joining the network, each Public Value node along with the services it provides would be available to the network in the form of a searchable network map; immediately opening opportunities for collaboration and innovation.

2. How might this new Internet of Public Value enable Public Service Organisations to collaborate in the design and delivery of frictionless human centric services

We know that for decades the holy grail has been this concept of a joined-up government and joined-up public services, but until now it has not really been possible at a holistic level.

The Corda network as a peer-to-peer network has a unique feature that makes it particularly suited to be a Public Value Network. Whilst each node of the network can communicate with every other node, the design of the network means that for each transaction or exchange, the participants must be defined and only the participants related to a transaction get to see the transaction.



In this model above, each of the numbered circles represent a shared fact or piece of information. You can see that 'fact 2' (perhaps about the welfare of a child) is shared between the local council, the health service and the education service, but not the waste collection service or 3rd sector provider.

In the Corda architecture, each node has its own private ledger and can only share the facts from its ledger with those parties that need to see them i.e. a party they are jointly delivering a service with, or that is providing an adjacent service.

What this means is that when designing services around the citizens, public service organisations on the Public Value Network can come together and decide which facts they want to share and under which circumstances.

What we can see from this model is that with the peer-to-peer network described under point 1 and the node-to node direct communication on specific shared facts, creates a new opportunity for autonomous public service entities, to integrate without friction and to design highly personalised, automated, cross-organisation joined-up services, centered on the human needs of the citizens they seek to serve.

3. How might this new Internet of Public Value enable Public Service Organisations to automate adherence to regulations, policies and procedures?

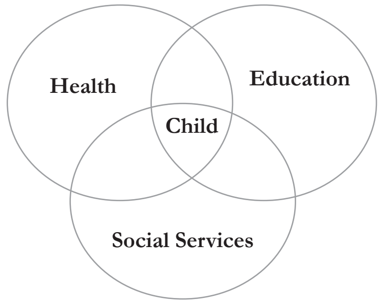
Our public services operate in highly regulated environments, in the same way our banks operate in highly regulated environments. Corda was designed from 'the ground up' to be able to act as a value network within the financial services industry and the smart contract features can be equally applied to a Public Value Network. In providing public services, organizations need to adhere to regulations, policies, and procedures. In designing services that sit on the Public Value Network, service providers can automate processes and flows in smart contracts.

Let's say education, health and social services come together to think about the services they provide to children. If we assume the team decide that the right implementation of legislation, regulation, policy and procedure is that, if a child presents in A&E more than once in a given period, and in the same period has a certain % absence from school, this would trigger an automated sharing of this fact with the social services.

We are not child care service experts. The purpose of the illustration is to show that (with a Public Value Network and Smart Contracts) regulations, policies, process and procedures can be automatically shared across service providers based on given events.

From a compliance point of view, all transactions and the history of data sharing is immutable so from a public trust and transparency point of view, each of the service providers can demonstrate that they acted in accordance with the regulations and this can be independently verified by a regulator.

The regulator as real-time observer. With a Public Value Network based on Corda, the regulators would have observer nodes on the network where they can observe events in real-time rather than retrospectively auditing when things go wrong. Regulation of non-compliance events can be automatically flagged to the regulator or indeed anonymously raised by participants in the Public Value Network.



4. How might this new Internet of Public Value enable Public Service Organisations to Improve financial transparency across public service value chain?

People care about where public funds are spent, people want to see investment making it to the front line, people want to see more front-line staff. There are many ways distributed ledger technology could bring transparency to public sector finances. One interesting example would be based on the concept of "wooden dollars". Imagine if the Treasury, as a node of the Public Value Network, decided to issue at the time of annual budget, for every £1 of actual budget an equivalent digital coin.

As the budgets then flow through the system and get assigned to services, projects, and front-line agencies, the public can see in real time where the money is and where the money is being spent.

Very quickly and visually, the public could see how money flows around public services, they would see the vast sums that never make it out of the center and the ratio between back office and front-line services. This transparency would drive a national conversation and would put increasing pressure on public service providers to join-up, synchronise, de-duplicate and ensure resources are invested in front line staff.

Conclusion

There is an ever-widening gap between public services and the expectations of the public, this expectation gap cannot be met by applying the same thinking and technology that we have applied for the past decade; we haven't got to where we need to be and more of the same is not going to change the game.

Just when we need it most, a new technology and a new opportunity has emerged. Many people still hold the banks responsible for creating the financial crisis that triggered austerity and the continued downward trajectory in Public Service funding resulting in the major expectation gap we see today; it would be a little ironic and poetic if it turns out to be the imagination and innovation of today's generation of financial service professionals who end up creating the technology that repairs and restores our Public Services.

References

Bitcoin White Paper -Satoshi Nakamoto - Jan 2009

Ethereum White Paper - Vitalik Buterin - 2015

R3 Corda, An Introduction - Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn - August 2016

Corda Technical White Paper - Mike Hearn - November 2016

Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World - Don Tapscott - 2016

Digital Asset Holdings White Paper - Dec 2016

Better Public Service a Manifesto - Jerry Fishenden, Mark Thompson and Will Venters – 2018

Photo by Pedro Carballo on Unsplash

ANALYSIS

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(7)2018

Building the Future of EU: Moving Forward with International Collaboration on Blockchain

Bill Buchanan[1], OBE, PhD; Naseem Naqvi[2] FRCP MAcadMed
[1] Professor of Computing, The Cyber Academy, Edinburgh Napier University, UK
[2] Co-founder, The British Blockchain Association, UK
Correspondence: B.Buchanan@napier.ac.uk
Received: 15 April 2018 **Accepted:** 25 April 2018 **Published:** 27 April 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
BB [1] and NN [2] prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

A blockchain enabled 'Digital Single Economy" can act as a catalyst for growth and could provide a platform where borderless innovative practices will thrive and create a true collaborative global economy, with shared goals and objectives for the benefit of wider community. A society where digital economy flourishes irrespective of geopolitical ideologies and where a technology like Blockchain holds transformative potential to unite the nations together. The UK currently has strong collaborations around blockchain including with the British Blockchain Association which aims to integrate with the EU on the adoption of Blockchain based methods around a range of application areas. However, at the core of these alliances must be the promotion of technology which link industry, the public sector, and academia, whilst also integrating key stakeholders, such as law enforcement, finance, health care, professional bodies and the legal industry.

Keywords: *digital, blockchain, economy, British, European, collaboration*

1. An old world

The Internet we have now differs little from the one that was created in the 1980s. Basically we are often using the methods developed around TCP and IP, with security integrated to fill-in the gaps around security. Few things on the Internet, though, can be trusted, and where every email we receive cannot be properly verified for its sender, and whether someone else has either viewed or edited the email. Our IT infrastructure is thus often frozen in the 20th Century, with very little usage of integrated security especially in defining ownership and for access control. For identity checking we have grown accustomed to usernames and password, and where our passwords are stored in a hashed format. We end up, too, having multiple identities across multiple platforms, and often have very little control of our own data.

The IT systems have created have been basically mirrored on a form filling work, and where we repeatedly enter the same information across multiple systems. For a world which aims to move to a citizen-centric approach, and where data is controlled by its owner, we are a long way off, and will probably never get there without a radical change in our approach. This change will be to build the Internet has it was meant to be, and where trust is integrated into every part of the infrastructure. Our failure is generally around the concept of a third-party trust model, and where Bob and Alice rely on Trent to identify themselves to each other. But what if Bob and Alice do not trust anyone?

Our new world will embed identity, rights and citizenship at its core, and be built around Bob and Alice transacting, and only requiring Trent when they think it is best for them. This world will properly define identity and enact smart contracts which do not need a third party to be involved.

2. Rebuilding a new world

To build this new world requires international collaboration, and it is a world which might not respect international borders, laws and rights. Without collaboration we cannot build an infrastructure that can scale from the local level (micro) to a world-wide level (macro). It will require new models of operation, and where laws are rewritten to be enacted as smart contracts. Isn't it a strange world that we see a scrawl of a pen across a page as a more creditable proof of our identity than our private key or our biometrics? This, though, will change, but requires the collaboration of technologists, academics, politicians, and law makers.

Blockchain is thus seen by Gartner as one of the ten technologies in the next decade will are likely to be one of the most disruptive [1].

The US has moved greatly on integrating cryptography and smart contracts into the statute on several states. At part of this the federal Electronic Signatures in Global and National Commerce Act (ESIGN Act) [2] and the Uniform Electronic Transactions Act (UETA) [3] aim to support the legal basis for the integration of legal contracts. Using these Acts as a foundation, on 3 April 2018, Arizona has defined that organisation can now hold and share data on a blockchain. These amendments build on laws which recognise digital signatures and smart contracts as legal entities.

The EU, though, has not moved as fast on supporting the usage of digital signatures and smart contracts, but it has moved on the rights of the citizen. With GDPR to be enacted in May 2018, the requirement to rebuild the Internet has never been so relevant.

3. International collaboration

The Internet is no respecter of national borders, and new eco-systems are being built which often have little respect for the laws and regulations within national borders. International collaboration thus must be at the heart of most economies, especially in emerging areas of technology. Without it nations can often struggle to catch-up with others when they are excluded from research projects. Along with this politicians and law makers could end-up suppressing innovation within their countries.

In order to advanced Blockchain collaboration, 22 EU countries have now signed up to a collaboration document, with a focus on creating a Digital Single Economy. List of countries among the signatories of the Declaration are: Austria, Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Ireland, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK.

This collaboration will allow the nations to exchange knowledge and thus prepare for the roll-out of systems based on blockchain methods. This will include private sector areas around finance and energy, along with public sector applications within government systems and health care. In order to show that the UK aims to continue to collaborate within digital applications it has eagerly signed up to both the implementation of GDPR and to the Digital Single Economy.

The Commission for Digital Economy and Society - Mariya Gabriel – showcases the transformation that Blockchain, smart contracts and digital signing are likely to bring [4], by saying:

"In the future, all public services will use blockchain technology. Blockchain is a great opportunity for Europe and Member States to rethink their information systems, to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, benefiting citizens, public services and companies. The Partnership launched today enables Member States to work together with the European Commission to turn the enormous potential of blockchain technology into better services for citizens".

With the collaboration around blockchain, the 22 nations will be able to more closely share data, and define new models for governance, consent and rights. To support this the European Commission has also created the EU Blockchain Observatory and Forum and has invested over €80 million in blockchain and has set aside more than €300 million in investment by 2020.

4. Conclusion

Trust is at the heart of EU economy and in incorporating the transition to a digital single market. The Blockchain can streamline public & government interactions and provide frictionless opportunities for consumers and businesses. All too often, these opportunities get stifled by onerous regulations due to lack of standardized benchmarks. It is time we put this right by building foundations on a blockchain based ecosystem which can unlock an enormous, untapped, growth potential. We believe that blockchain, if harnessed appropriately, can be a source for significant productivity and would nurture tangible benefits for the post Brexit United Kingdom. We need to work together constructively and make decisions based on best available evidence to ensure that we reap the full potential of Blockchain and other Distributed Ledger Technologies.

References

[1] D. W. Cearley, B. Burke, and M. J. Walker, "Top 10 strategic technology trends for 2018," Gartner Research, 2017. [Online]. Available: https://www.gartner.com/document/3811368?ref=TrackDBDTextEmail&refval=1507125606933. [Accessed: 15-Apr-2018].

[2] "Summary: Bills Pertaining to Digital Signatures and Authentication in the 106th Congress." [Online]. Available: http://www.techlawjournal.com/cong106/digsig/Default.htm. [Accessed: 15-Apr-2018].

[3] J. P. Mazurek, D. Benjamin, and C. R. Beattie, "UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)."

[4] "European countries join Blockchain Partnership | Digital Single Market." [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership. [Accessed: 15-Apr-2018]

Photo by chuttersnap on Unsplash

THE JBBA

CASE STUDY

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(10)2018

Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM

Reshma Kamath[1]
Northwestern University, Chicago, IL, USA
Correspondence: reshmakamath2017@gmail.com
Received: 1 June 2018 **Accepted:** 9 June 2018 **Published:** 12 June 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
RK[1] is the primary author responsible for data collection and writing the manuscript. The Blockchain Research Institute (BRI) provided layout and proof-reading services.

Funding:
The project is funded by the BRI.
IBM is a paid member of the BRI.

Acknowledgements:
RK[1] would like to acknowledge Irving Wladawsky-Berger, Visiting Lecturer at MIT (Massachusetts Institute of Technology) Sloan School of Management, for reviewing and providing feedback on the manuscript; Don Tapscott and Alex Tapscott of the BRI for facilitating conversations between the author and the parties involved in the pilot projects, namely Brigid McDermott, IBM's Vice President of blockchain business development, and Frank Yiannas, Walmart's Vice President of food safety and health.

Abstract

In response to food contamination scandals worldwide, retail giant Walmart is tackling food safety in the supply chain using blockchain technology. In 2016, it established the Walmart Food Safety Collaboration Center in Beijing and plans to invest $25 million over five years to research global food safety (Yiannas and Liu, 2017). Using IBM's blockchain solution based on Hyperledger Fabric, Walmart has successfully completed two blockchain pilots: pork in China and mangoes in the Americas (IBM, 2017). With a farm-to-table approach, Walmart's blockchain solution reduced time for tracking mango origins from seven days to 2.2 seconds and promoted greater transparency across Walmart's food supply chain (Yiannas, 2017). IBM called it "complete end-to-end traceability" (McDermott, 2017). This case study highlights the challenges of implementing blockchain technology in the food supply chain and the opportunities for deploying blockchain solutions throughout the global food ecosystem to increase safety and reduce waste.

Keywords: *Food safety, provenance, supply chain, Walmart, IBM, traceability*

Broken food chains: food contamination scandals

Health hazards from food mismanagement and contamination are well documented. The Centers for Disease Control and Prevention estimate 48 million people in the United States contract foodborne illnesses every year (2011). The World Health Organization estimates that one in ten people suffers from food poisoning worldwide, with 420,000 fatalities, each year (2017).

In North America, isolating the cause of the E. coli outbreak in 2006 wasted time, energy, and the resources of the entire ecosystem (wholesalers, retailers, farmers, and regulators), shattering public trust in the supply chain. American consumers stopped eating spinach altogether, while restaurateurs and grocery stores pulled spinach off their shelves and menus. Health officials took almost two weeks to identify the source of the contamination: one supplier, one day's production, and one lot number (Produce Processing, 2007). The inability to rapidly track and trace the source of the contaminated spinach resulted in significant and lasting economic harm to spinach farmers and erosion of consumer trust (Yiannas, 2017).

In 2011, China witnessed a massive pork mislabeling debacle, along with a contamination hoax in which donkey meat products were recalled because they were found to include fox meat (Bradsher, 2011; Clemons, 2014). Additional contaminants such as melamine, Sudan red, clenbuterol, Sanlu toxic milk powder, and trench oil—all of which had breached the food supply chain—further eroded Chinese trust in food markets (Hatton, 2015). With arcane agricultural food logistics systems, China faces an agri-food loss ratio of 25 to 30 percent annually. The Office of Economic Cooperation and Development identified several challenges: deficient information at each stage of the food value chain, decentralized storage of food, waste in the restaurant and catering sector, and a lack of coordination among regulatory agencies and ministries (Liu, 2013).

In 2013, bad actors in the EU supply chain replaced lamb and beef with horsemeat (Castle, 2013). The illegal substitution affected more than 4.5 million processed products representing at least 1,000 tons of food (Ruitenberg, 2013). This fraud caused lasting damage to profits and corporate reputations. According to PricewaterhouseCoopers and Safe and Secure Approaches in Field Environments (2016), food fraud is estimated to cost the global food industry $40 billion a year.

In July 2017, papayas in the US market were linked to a multi-state outbreak of Salmonella. By mid-August 2017, the CDC reported 173 cases of salmonellosis, 58 hospitalizations, and one death across 21 states (2017). Health officials advised consumers to avoid eating papayas and retailers not to sell them. Even by replicating measures in the spinach outbreak, health officials took almost three weeks to trace the source to a single farm in Mexico. Papaya farmers from unaffected areas suffered economic losses because of the inability to rapidly track and trace food products (Yiannas, 2017).

The inability to trace products in the supply chain comes from the disparate record-keeping methods in use (Culp, 2013). The widely-accepted "one up, one down" (OUOD) approach—whereby food supply chain participants know only the immediate supplier (one link up the chain) and the immediate customer (one link down the chain) for a product—is simply insufficient. In suspected contaminations, investigators review paper documentation step by step. Erroneous or incomplete data can further delay their investigations. Multi-ingredient foods and bulk containers may include elements from a variety of sources and multiple countries and traceability gets even more complicated. As a precautionary step, entire shipments are thrown out under OUOD parameters (Blanchfield and Welt, 2012). With blockchain technology, such food shipments "will be identified as being safe at a much earlier juncture," while saving millions in sales as well as valuable human lives (Hodge, 2017).

Walmart's blockchain pilots for food provenance

Walmart worked with IBM to develop and implement its food provenance pilots using blockchain technology (Tiwari, 2016). According to McDermott (2017), "Blockchain solves business problems where trust is part of the solution" by providing what traditional databases cannot: data immutability as well as speed and security of dissemination.

Leaders at IBM recognized that they could accelerate the adoption of blockchain and avoid a proliferation of internal systems and data formats by using existing open standards such as the Electronic Product Code Information Services and Core Business Vocabulary of Global Specifications 1 (Blanchfield and Welt, 2012). IBM's blockchain is based on Hyperledger Fabric, which supports modular architecture and plug-and-play components such as consensus and membership services (IBM, 2017). It allows both efficient data capture and data control. Most importantly, users have a shared view of the truth at any point in time as well as ownership and control over their own information. Records include audits, agricultural treatments, identification numbers, manufacturers, available device updates, known security issues, granted permissions, and safety-protocols, all logged in real time and permanently stored as e-certificates.

This foundational trust has a flywheel effect. According to McDermott (2017), "The trust it delivers enables more efficient and complete sharing of the critical data that drives enterprise transactions."

Pork chains across China

China is both a leading importer of pork and a producer of nearly half of the world's pork; large, industrialized pork production systems similar to those in the United States have been displacing small-scale "backyard" pork producers (Gale, 2017). In line with this trend, government officials in China called for the country's pork industry to modernize its production system from farm to fork.

As consumer focus in China has shifted to food safety and quality, trust is critical to purchasing decisions. The Chinese government is investing heavily in its food system, upping food inspection and safety methods, putting pressure on production systems, and partnering with corporate retail giants. Given the country's sizeable population and its immense appetite for pork (with an annual consumption of 12.7 million tons), Walmart had an incentive to explore new technologies for creating trust in food provenance in China (Bunge, 2015).

Collaboration, collaboration, collaboration

In October 2016, Walmart launched the Food Safety Collaboration Center (Burkitt, 2014). At the center's opening, Doug McMillon, president and CEO of Walmart Stores, said, "By bringing together the best food safety thinkers from across the food ecosystem, from farmers to suppliers, retailers to policy regulators, we'll accelerate food safety awareness and help make Chinese families safer and healthier" (Walmart, 2016). The center studies food-borne contaminants and develops risk assessment models that other corporations and organizations will be able to use (Bloomberg, 2016). Walmart also invested in food-related technologies to detect food-borne pathogens and to monitor packaged food for contamination in the supply chain.

Cooperation with governmental entities was crucial to the success of Walmart's blockchain pilot. Regulators were enthusiastic about blockchain technology and its potential, as it aligned with their work (McDermott, 2017). With collaborators in place and a green light from regulators, Walmart was ready to apply features of blockchain technology to pork safety and supply chain management.

Farm and slaughterhouse tracking

For pork, the process begins at pens—where every pig is smart-tagged with bar codes—and follows the product all the way to packaged pork. While using radio frequency identification and cameras, participants record the pig's movement as well, and cameras installed in slaughterhouses capture the entire production process. These efforts protect both piglets and sows and modulate temperature so that babies stay warm while mothers stay cool (Clark, 2017).

In pork production, shipping trucks have deployed temperature and humidity sensors, along with global positioning and geographic information systems, to ensure the meat arrives at retailers under safe conditions; Walmart can trace whereabouts of trucks and monitor conditions in each refrigerated container and, if conditions exceed established thresholds, receive alerts to prompt corrective action (Gale, 2017).

Walmart distribution center and store tracking

With blockchain, procurement managers can remotely trace all information, from expiration dates to warehouse temperatures (Kaye, 2016). Information about farm origination, batch numbers, processing data, soil quality and fertilizers, and even storage temperatures and shipping details can be uploaded on an e-certificate and linked to the product package via a QR code (Murphy, 2016).

Walmart's blockchain pilot involved different systems of data capture and improved speed and accuracy in providing relevant information from the farm to the store (Blanchfield and Welt, 2012). Such systems typically include Global Trade Identification Number with a handler's production lot or batch number (National Mango Board, 2017).

Traceability improves food safety and public confidence. Should any tainted food reach a consumer, the system can better pinpoint which products should be discarded without jeopardizing an entire product line (Bottemelier, 2011). This holistic traceability model has the potential to cut costs of product recalls, reduce process inefficiencies, and enable retailers to track individual pork products in seconds, not days (Del Castillo, 2016).

Mango chains in the Americas

Walmart concurrently conducted a pilot using IBM's Hyperledger-based blockchain* to trace sliced mangoes from South and Central America to North America (Burkitt, 2014). Mangoes as well as mango origins and derivatives are shipped worldwide and susceptible to Listeria and Salmonella contaminations (Yiannas, 2017; Andrews, 2012). Therefore, Walmart's mango pilot had to demonstrate transferability and accountability across borders (Andrews, 2012) so that, were there another recall of such produce, blockchain traceability would enhance public trust in the information about the supply (McDermott, (2017).

** (Hyperledger is a non-paying affiliate of the Blockchain Research Institute.)*

Food production: pre-seedling stage

In production, mangoes can suffer from "fruit decay, surface defects, internal breakdown symptoms, chilling and heat injury, disorders during ripening, and more" (National Mango Board, 2017). The production phase tends to require an all-hands-on-deck approach. Producers may cut corners by using contaminated fertilizers, hiring children, paying poverty wages, or requiring laborers to work extremely long days. Workers may have no contracts and no trade union to defend their interests (Humbert, 2013). Marginalized farmers have limited information on market prices and production inputs, limited quality control, variable access to quality fertilizer and pesticide, and non-existent bargaining power with traders (Matta, 2013). Blockchain technology can raise red flags as to these practices (Van der Wal, 2013).

Food processing: warehouse storage stage

Greater perishability of agri-foods mandates an exacting check of temperature and moisture in the logistics process (Ontario, 2016). For mangoes, Walmart analyzes fruit quality throughout the supply chain—on the tree, at harvest, at the packing shed, at wholesale markets and at retail outlets—to determine quality and marketability at each stage. Such analysis could help to anticipate potential losses from sap burn, bruising, physical damage, diseases, poor methods of harvesting, and poor transportation from packing shed to wholesale markets (Mazha, 2010). At all stages, participants can collect and store data to benchmark industry performance beyond traditional practices (Matta, 2013).

Food distribution and aggregation: shed stage

Mango importer facilities and retail distribution centers inspect for quality, measure and record shipments, document proper certificates, ascertain cargo and temperature excursions, measure temperature, sample at arrival, and evaluate external and internal quality (National Mango Board, 2017). All these data can be stored and traced on a blockchain. In distribution, blockchain-connected devices and smart sensors will eventually be able to record produce damage caused by excessive sunlight (or any rotting of meat) due to temperature and humidity (Gantait, 2017).
Walmart is working with shipping and logistics providers

to improve data capture of bills of lading (or warehouse warrants) and propel invoice consents, dispute resolution, and cargo provenance and tracking. For example, distributed ledger technology has the ability to record updates to legal agreements and platforms, thereby ensuring both legal and security integrity (essDOCS, 2017). Walmart has a patent application for a "delivery management system" involving distributed ledgers, robotics, and sensors (Hackett, 2017). IBM is also developing blockchain solutions for cross-border supply chains in collaboration with the global transport and container logistics giant, Maersk (IBM, 2017).

Marketing and retailing: supermarket stage

Traceability is a major competitive advantage for supply chain participants (Webb, 2004). Supermarkets will be able to connect their enterprise resource planning and point-of-sale systems to the blockchain-enabled platform and trace every item sold. According to Yiannas, "With blockchain, you can do strategic removals, and let consumers and companies have confidence" (Kharif, 2016). Retailers should be able to generate customer loyalty with transparent record keeping and could slash recall costs and increase profits, while reducing their risk exposure (Simon, 2016).

Household and food purchasing: consumer stage

Should a consumer fall ill, "Walmart will be able to obtain crucial data from a single receipt, including supplies, detail on how and where food was grown and who inspected…from the pallet to the individual package" (Kharif, 2016). Customers can also provide retailers with specific feedback regarding quality that can be linked to growers and sources (Yiannas, 2017). In addition, customers can enjoy reduced prices and fresher produce and know when their groceries will arrive. Restaurant owners and managers of school and government cafeterias will also benefit: by "digitally tracking the provenance and movement of food throughout the entire supply chain, purveyors have instant quality assurance that the products they receive and serve customers are safe" (Van Kralingen, 2016). Food inspectors could include restaurant or cafeteria health and safety ratings on the blockchain as well.

Post-cumulative data capture: post-harvesting or finish

Whether pork or mangoes, Walmart's blockchain pilots have the capacity to document post-cumulative losses from potential supply chain inefficiencies (Gantait, 2017). Such digital tracking could enhance food safety mechanisms, provide quality assurances, and smooth supply chain disruptions from food wastage and spoilage. Each transaction will generate a proof of record, from the pre-seedling stage to the consumer's table at home. Combined with data analytics and existing industry standards, the entire supply ecosystem should benefit from such a comprehensive data snapshot.

Discussion

Blockchain has demonstrated its potential for providing greater transparency, veracity, and trust in food information so that supply chain members can act immediately, should problems arise. To evolve their blockchain solution and apply it to the global food system, IBM and Walmart expanded their collaboration to include Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, and Unilever (IBM, 2017).

Traceability is essential in preventing or responding quickly to food contamination, disease, drug or pesticide residues, or attempted bioterrorism (IAEA, 2011). According to McDermott (2017), "Blockchain is not solving a technical problem, it is solving a social problem." With prevention, preparedness, and proof, Walmart's blockchain pilot serves a larger purpose and has a positive effect on the Walmart brand.

Walmart's blockchain solution needed to be "business-driven and technology-enabled," the capacity to solve such business problems as time efficiencies, cost reduction, long-term good will, and revenue generation (Burkitt, 2014). Ensuring value for all participants in the ecosystem will be critical to wider adoption; breeders/farms, processing plants, cold storage facilities, distribution centers, and retail stores need to have a strong value proposition to join.

To maintain whole-chain traceability, this kind of initiative requires leadership to coordinate stakeholders and promote awareness of different technology solutions. "This is not about competition, this is about collaboration," according to Yiannas (2017). "[It's about] creating a solution that offers shared value for stakeholders." Throughout the product life cycle, supply chain participants were able to record, crosscheck, and ensure a product's authenticity and trace its movement and quality (Doyle, 2014). This information gave all participants greater control over their brands and businesses and supported deeper learning capacities from enhanced gathering of data and analytics. Such a supply chain network could eventually include research and development centers, primary production facilities, aggregation and mobilization providers, trading and grading participants, wholesalers, retailers, and customers (Matta, 2013).

Blockchain technology enables food traceability to the item level, not just batch level, so that participants can trace each item in the supply chain (Wuest, 2015). Walmart's blockchain pilot identified which data were relevant to capture and compiled a list of mandatory attributes (lot number, pack date, quantity shipped, unit of measure, purchase order number, shipment identifiers) and a list of optional attributes (carton serial numbers, pallet number, harvest date, buyer identifier, vendor/supplier identifier). Consistency is key. Pilot leaders should adopt data structures that align with standards and develop requirements for master data and guidelines for data retention (Can-Trace Secretariat, 2004). This supply chain portrait accounts for interoperability among ledger participants with an in-depth grasp of data.

Walmart chose IBM's blockchain solution because it was "not recreating supply chain, but leveraging existing technologies to enhance supply chain traceability using Hyperledger" (Burkitt, 2014). Like Walmart's blockchain pilot, "traceability systems that are integrated with existing company business practices are more likely to be maintained and more likely to be accurate than stand-alone traceability systems" (Can-Trace Secretariat, 2004). "Visibility, optimization, and demand" are key challenges in creating interoperable devices and platforms (Gantait, 2017).

Walmart took a three-pronged approach to cultivating knowledge in food safety and delivery in China. First, it collaborated with a non-profit in China that provides food safety education developed for children. Second, it brought together American and Chinese academics and Chinese poultry producers to study safety in poultry supply chains. Third, it pooled talent from top academic institutions to leverage supply chain analytics and superior technology (Lindell, 2016). This approach will instantaneously predict and detect areas of greatest vulnerability and threats for food adulteration in China's food supply chains.

Walmart will continue to experiment, scale, and learn from its blockchain pilots as it builds coalitions within the supply chain ecosystem where members are seeking to implement blockchain applications more broadly. Blockchain is bigger and broader than these pork and mango pilots. However, for Walmart, blockchain technology was deployed specifically to solve societal issues of broken food chains. Leveraging existing devices and sensors, Walmart's blockchain pilots identify systemic vulnerabilities in the food supply chain and go beyond technology and business to regain people's trust and confidence in food.

References

Allison, I., "IBM enlists Walmart, Nestlé, Unilever, Dole for food safety blockchain," International Business Times, August 24, 2017. www.ibtimes.com/ibm-enlists-walmart-nestle-unilever-dole-food-safety-blockchain-2582490.

Andrews, J., "Mango outbreaks connected through interviews," Food Safety News, October 26, 2012. http://www.foodsafetynews.com/2012/10/mango-outbreaks-connected-through-interviews/#.WYtxMneGPBI.

Blanchfield, J.R., and B. Welt, "Food traceability," The International Union of Food Science and Technology, March 2012. www.iufost.org/iufostftp/IUF.SIB.Food%20Traceability.pdf.

Bloomberg, "Walmart to invest 25 million in china food safety research," Bloomberg Markets, October 19, 2016. www.bloomberg.com/news/articles/2016-10-19/Walmart-to-invest-25-million-in-china-food-safety-research.

Bottemelier, H., "IBM and China Team Up to Build Pork Traceability System," Food Safety News, Dec. 19, 2011. www.foodsafetynews.com/2011/12/ibm-and-china-team-up-to-build-pork-traceability-system/#.WZjWBCiGPIU.

Bradsher, K., "Chinese city shuts down 13 Walmarts," New York Times, October 11, 2011. www.nytimes.com/2011/10/11/business/global/wal-marts-in-china-city-closed-for-pork-mislabeling.html.

Bunge, J., "How to satisfy the world's surging appetite for meat," Wall Street Journal, December 4, 2015. www.wsj.com/articles/how-to-satisfy-the-worlds-surging-appetite-for-meat-1449238059.

Burkitt, L., "Walmart to triple spending on food safety in China," Wall Street Journal, June 17, 2014. .www.wsj.com/articles/Walmart-to-triple-spending-on-food-safety-in-china-1402991720.

Can-Trace Secretariat, "Can-Trace pork pilot project report," Can-Trace, Electronic Commission of Canada, Agriculture and Agri-Foods Canada, 2004. www.can-trace.org/portals/0/docs/Can-TracePorkPilotProjectReport.pdf.

Castle, S., "Europe says tests show horse meat scandal is 'food fraud,'" New York Times, April 16, 2013. www.nytimes.com/2013/04/17/business/global/european-study-affirms-role-of-fraud-in-horsemeat-scandal.html.

Center for Food Safety and Applied Nutrition, "FDA investigates multiple Salmonella outbreak strain linked to papayas," August 18, 2017. www.fda.gov/food/RecallsOutbreaksEmergencies/Outbreaks/ucm568097.htm.

Centers for Disease Control and Prevention, "Foodborne illnesses and germs," June 2011. www.cdc.gov/foodsafety/foodborne-germs.html.

Clark, J., "Pig premise ID registrations top 13 thousand and growing," The Pig Site, August 2, 2017. www.thepigsite.com/swinenews/43919/pig-premise-id-registrations-top-13-thousand-growing.

Clemons, S., "China's latest food scandal: fox-tainted donkey meat," The Atlantic, January 2, 2014. www.theatlantic.com/

international/archive/2014/01/chinas-latest-food-scandal-fox-tainted-donkey-meat/282776.

Culp, S., "Supply chain disruption a major threat to business," Forbes, February 15, 2013. www.forbes.com/sites/steveculp/2013/02/15/supply-chain-disruption-a-major-threat-to-business/#2ed93c7673b6.

Del Castillo, M., "Walmart blockchain pilot China pork market," CoinDesk, October 19, 2016. www.coindesk.com/walmart-blockchain-pilot-china-pork-market

DeCovny, S., "Blockchain in supply chain: edging toward higher visibility," ChainBusinessInsights.com, Chain Business Insights LLC, May 2017. www.chainbusinessinsights.com/uploads/1/0/0/0/100045726/blockchain_in_supply_chain_survey_brief_-final.pdf.

Doyle, T., "Enabling trusted trade through secure track and trace technology," World Customs Journal. International Network of Customs Universities, Vol. 8, Issue 1, Section 2, Practitioner's perspective, March 2014. worldcustomsjournal.org/Archives/Volume%208%2C%20Number%201%20(Mar%202014)/14%20Doyle.pdf

essDOCS, "2017 blockchain for freight panel," March 3, 2017.

Food Safety News, "Organic mangoes recalled for possible listeria contamination," May 26, 2014. www.foodsafetynews.com/2014/05/organic-mangos-recalled-for-possible-listeria-contamination/#.WYtxqneGPBI.

Gale, F., "China's pork imports rise along with production costs," Economic Research Services, US Department of Agriculture, January 2017. www.ers.usda.gov/webdocs/publications/81948/ldpm-271-01.pdf?v=42745.

Gantait, A., J. Patra, and A. Mukherjee, "Integrate device data with smart contracts in IBM blockchain," IBM Developer Works, January 9, 2017. www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/index.html.

GS1 AISB, "GS1 recommends use of existing data standards in enterprise blockchain implementations," The Global Language of Business, 2017. www.gs1.org/sites/default/files/docs/internet-of-things/gs1-blockchain-pov-paper-a4.pdf.

Hackett, R., "Walmart blockchain drones patent," Fortune, May 30, 2017. fortune.com/2017/05/30/walmart-blockchain-drones-patent.

Hatton, C., "Will China's new food safety rules work?" BBC News, Beijing, September 30, 2015. www.bbc.com/news/blogs-china-blog-34398412.

Hodge, S., "Can blockchain technology transform safety standards in the global food supply chain?" Supply Chain Digital, August 25, 2017. www.supplychaindigital.com/technology/can-blockchain-technology-transform-safety-standards-global-food-supply-chain.

Humbert, F., "Mangoes with blemishes: the market power of German supermarket chains and unfair working conditions in Peru," www.oxfam.de, Oxfam Deutschland e.V, June 2013. www.oxfam.de/system/files/130705_oxfam_mangostudie_englisch_web.pdf.

IBM, "Hyperledger–open source blockchain for business – IBM Blockchain," IBM Cognitive Advantage Reports, IBM Corporation, 2017. www.ibm.com/blockchain/hyperledger.html.

IBM, "IBM announces major blockchain collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, and Unilever, and Walmart to address food safety worldwide," press release, IBM.com, August 22, 2017. www-03.ibm.com/press/us/en/pressrelease/53013.wss.

IBM, "Maersk and IBM unveil first industry-wide cross-border supply chain solution on blockchain," press release, IBM.com, March 5, 2017. www-03.ibm.com/press/us/en/pressrelease/51712.wss.

Kaye, L. "Responding to food safety concerns, Walmart invests $25 million in China," Triple Pundit, Oct. 25, 2016. www.triplepundit.com/2016/10/responding-food-safety-concerns-walmart-invests-25-million-china.

Kharif, O., "Walmart tackles food safety with trial of blockchain," Bloomberg Technology, Bloomberg LP, November 18, 2016. www.bloomberg.com/news/articles/2016-11-18/wal-mart-tackles-food-safety-with-test-of-blockchain-technology

Lindell, C., "Walmart to invest in $25M in food safety in China," Food Engineering, BNP Media, October 20, 2016. www.foodengineeringmag.com/articles/96277-walmart-to-invest-25m-in-food-safety-in-china.

Lui, G., "Food losses and food waste in china: a first estimate," Office of Economic Cooperation and Development, 15 June 2013. www.oecd.org/site/agrfcn/Food%20losses%20and%20waste%20in%20China_Gang%20Liu.pdf.

Matta, M., et al, "Mango supply chain: who is more sustainable—MNC or co-operative society?" The George Washington University School of Business, March 20, 2013. talkaboutfoodjb.files.wordpress.com/2013/08/f_brittell_gautam_keefe_mata_shah_wang.pdf.

Mazhar, M.S., et al., "Managing mango fruit quality through the supply chain: a Pakistan case study," Institute of Horticultural Sciences, University of Agriculture, November 2010. www.researchgate.net/publication/235258157_Managing_Mango_Fruit_Quality_through_the_Supply_Chain_A_Pakistan_Case_study.

McDermott, B., IBM's vice president of blockchain business development, interviewed by R. Kamath, June 23, 2017; edited by B. McDermott, September 12, 2017.

Murphy, D., "Meat of the matter: when solutions are seen as problems," Farm Journal's Pork, November 29, 2016. www.porknetwork.co/community/contributors/meat-matter-when-solutions-are-seen-problems.

Nash, K.S., "Walmart readies blockchain pilot for tracking US produce china pork," Wall Street Journal CIO Journal, Dec. 16, 2016. blogs.wsj.com/cio/2016/12/16/wal-mart-readies-blockchain-pilot-for-tracking-u-s-produce-china-pork.

National Mango Board, "Production and post-harvest best practices," www.mango.org, 2017. www.mango.org/en/postharvest.

Ontario AgriFood Technologies, "User needs assessment final report: precision agri-food scoping study," Precision Strategic Solutions, September 1, 2016. static1.squarespace.com/static/583f56.1af7e0ab824c0b77c8/t/586ad4a23e00bec12e6c1ff7/1483396389489/User+Needs+Assessment.pdf.

PricewaterhouseCoopers and Safe and Secure Approaches in Field Environments, "Fighting $40bn food fraud to protect food supply," January 14, 2016. press.pwc.com/News-releases/fighting--40bn-food-fraud-to-protect-food-supply/s/44fd6210-10f7-46c7-8431-e55983286e22.

Produce Processing, "FDA finalizes report on 2006 spinach outbreak," Great American Media Services and Produce Processing, March 23, 2007. produceprocessing.net/news/fda-finalizes-report-on-2006-spinach-outbreak.

Ruitenberg, R., "Horse-meat suspect Spanghero denies beef scam responsibility," Bloomberg LP, February 15, 2013. www.bloomberg.com/news/2013-02-15/horse-meat-suspect-spanghero-denies-scam-admits-some-negligence.html.

Simon, G., "Supply chain loyalty – the evolution of coupons," Loyyal, February 15, 2016.

"Supply Chain Resilience Report," Business Continuity Institute, 2016, p. 11. https://www.riskmethods.net/resources/research/bci-supply-chain-resilience-2016.pdf.

The Pig Site, "IFA accuses pig processors of undermining pig meat market," 5m Publishing, August 7, 2017. www.thepigsite.com/swinenews/43938/ifa-accuses-pig-processors-of-undermining-pigmeat-market.

Tiwari, T., "Profit alert: Walmart is adopting the blockchain right now," Palm Beach Research Group, December 6, 2016. palmbeachgroup.com/content/palm-beach-daily/profit-alert-walmart-is-adopting-the-blockchain-right-now/32499.

Tiwari, T., "Walmart, IBM developing a food safety solution," The Association for Convenience and Fuel Retailing, February 28, 2017. www.nacsonline.com/Media/Daily/Pages/ND0228171.aspx#.WZNwQlGGPIV.

Van der Wal, S., "Peruvian mango production: not enough improvements," The Centre for Research on Multinational Corporations, July 30, 2013. www.somo.nl/peruvian-mango-production-not-enough-improvements.

Van Kralingen, B., "Blockchain's role in improving global food safety," IBM.com, October 19, 2016. www.ibm.com/blogs/think/2016/10/blockchain-food-safety.

Walmart, "Walmart invites global collaboration on food safety in China," press release, www.wal-martchina.com, October 19, 2016. www.wal-martchina.com/english/news/2016/20161130-4.htm.

Webb, J., "Tracking pork from pen to plate," Advances in Pork Production, 2004. www.prairieswine.com/pdf/2426.pdf.

WHO, "Food safety: key facts," World Health Organization, October 31, 2017. www.who.int/mediacentre/factsheets/fs399/en.

Wuest, T., "Identifying product and process state drivers in manufacturing systems using supervised machine learning," WTI-Frankfurt eG, 2015. www.wti-frankfurt.de/images/top-themen/Identifying-Product-and-Process-State-Drivers-in-Manufacturing-Systems-Using-Supervised-Machine-Learning.pdf.

Yiannas, F. and R. Liu, e-mail to R. Kamath, September 6, 2017.

Yiannas, F., Walmart's vice president of food safety, interviewed by R. Kamath, June 28, 2017.

Photo by Marc-Olivier Jodoin on Unsplash

CASE STUDY

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(3)2018

Blockchain Governance and The Role of Trust Service Providers: The TrustedChain® Network

Marcella Atzori[1] PhD
University College of London, Centre for Blockchain Technologies
Correspondence: marcella.atzori@gmx.com
Received: 13 April 2018 **Accepted:** 17 April 2018 **Published:** 18 April 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
MA[1] designed and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Not declared.

Abstract

Although the blockchain is widely acknowledged as one of the most disruptive technologies emerged in the last decades, many implementation hurdles at the technical, regulatory and governance level still prevent a widespread adoption of services based on open networks. This research discusses the role Trust Service Providers may play in permissioned blockchains, providing a reliable ecosystem in which services can be safely developed and preserved in the long run. As case study, the paper outlines the main features of TrustedChain®, the first blockchain network of European Trust Service Providers specifically designed for highly sensitive sectors, with cutting-edge applications for public administration, e-government, banking, e-health and industry. Emphasis is thus placed on systemic trust, law compliance, adequate technical performance, confidentiality of transactions and long-term preservation of data as essential conditions for blockchain networks to thrive and accomplish complex tasks in an effective and reliable way.

Keywords: *AI, banking, blockchain, governance, e-government, e-health, eIDAS, smart contracts, Trust Service Providers, TrustedChain®*

"Decentralise as much as possible, regulate as much it is needed." ~G. Paquet

1. The disruptive potential of blockchain and distributed ledgers for digital services. The European Parliament Resolution (2016/2007 INI)

Over the last years, blockchain technology has come to the forefront of international debate as a new organisational paradigm for the decentralized and trustless exchange of value within a network, potentially able to disrupt and re-engineer the way data, processes and digitalized assets are accessed, verified, shared, and preserved over time.

Scholars, technologists, and businesses have explored possible uses of the blockchain - and more generally Distributed Ledgers Technologies (DLT) - in areas as diverse as fintech and banking, e-government, notarial services, healthcare, and industry, including chain supply management, AI, Internet of Things and Machine-to-Machine applications. Depending on the context of use, design and implementation, the advantages of a blockchain-based governance have been recognised as being significant for many classes of services (Blockchain Technologies, 2016; Boucher, 2017; Government Office for Science, 2016; Swan, 2015), in terms of:

- Decentralisation and reduced reliance of processes on trusted authorities and third parties;
- Improved time- and cost- effectiveness of data management and workflows, leading to greater productivity;
- Tamper-resistance, verifiability and auditability of digital transactions, with consequent reduction of possible accidental errors, corruption, or fraud;
- Improved data security and digital infrastructure resilience;
- Enhanced privacy and protection of citizens' fundamental rights;
- Opportunities for value exchange and data sharing between unknown or untrusted Participants, reducing counterpart risk;
- Tracking of digitalized assets, protection and enforcement of associated rights;
- Greater competitiveness, also through the adoption of new business models and applications, such as smart contracts and digital signatures.

Even the European Parliament Resolution (2016/2007

INI) has emphasized the potential of Distributed Ledgers Technology "to contribute positively to citizens' welfare and economic development" (Art. 1). While the Resolution is not binding for Member States or European citizens, it represents nonetheless an important recognition of this technology at institutional level: it established a first conceptual framework for distributed ledger technologies, calling for an adequate regulatory supervision and the development of technical expertise, so to keep up with innovation and ensure timely response to the new challenges at stake (Art. 3).

In particular, the Resolution has acknowledged:

- The potential of DTL to disrupt the way digitalised assets and records are managed and kept, with implications in private and public sector, by means of accelerating, decentralising, automating and standardising data-driven processes at lower costs (Art. 5).
- The capacity of DLT to effectively process large volumes of transactions, with innovative applications for fintech industry and beyond, including clearing, settlement, proof of identity and property (Art. B);
- The transformational power of decentralised architectures in terms of efficiency, speed, and also resilience (Art. 6), since they might continue to operate reliably even if the network was to break down in part, due to malfunctioning or malicious attack (Art. 1- c);
- The possibility to use DLT to: protect individual privacy (Art. 1 - d, e); increase data sharing, transparency and trust between different players, such as governments, citizens, businesses and clients (Art. 8); help institutions to reduce fraud, corruption and money laundering (Art. 11); improve the land registry systems (Art. 12);
- The still unfolding potential benefits of DLT as related to crypto-equity crowdfunding, dispute mediation systems, smart contracts, digital signatures and data security applications for the Internet of Things (Art. 9).

The Resolution has therefore encouraged governmental agencies to test DLT solutions after adequate impact assessment, with a view of improving the quality of e-government and digital services provided to citizens, in accordance with EU data protection rules (Art. 12).

2. Open blockchains and implementation hurdles

In spite of the potential advantages of deployment of the blockchain technology in a great many areas, the adoption of blockchain-based services still appears to be slow and a critical mass of users has not been reached yet. This is surely caused by many hurdles and trade-offs still existing at the technical, regulatory and governance level, but it is also due to the way the implementation of the blockchain technology is often devised.

So far, practitioners, scholars and blockchain enthusiasts have vigorously insisted on the concept of individual-centricity and decentralisation of digital services through peer-to-peer interactions, with the aim to disrupt and re-conceptualise the traditional top-down structure of financial, political, legal and even social powers (Swan, 2015; Wright & De Filippi, 2015). The decentralisation of services, however, is often portrayed as a seamless, predictable and linear theoretical process, without properly addressing the complexity of integration mechanisms required at the social, juridical and technical level for effective implementation (Allenby, 2012). At the same time, it is often forgotten that the process of disintermediation may not unfold in a homogeneous way, because every society is different, with different social, cultural and institutional practice, and unpredictable dynamics (Allenby, 2012; Atzori, 2015; Boersma, Meijer & Wagenaar, 2009). A further problem is that the blockchain technology is frequently "picked up and discussed as if it were more mature than it actually is" (Martha Bennett in Earls, 2016).

The question thus remains of which blockchain should be used to safely achieving those ambitious, disruptive goals, and how it should be designed, in order to handle several trade-offs at stake and best make use of this technology.

Open, multipurpose networks such as Bitcoin and its clones have proved highly problematic in this regard. On one side, they are certainly appealing, insofar they aim at fostering innovation and making citizens less dependent on centralized services. On the other side, they still suffer from numerous limitations, related to specific contexts of use, but often overlapping, which may prevent or at least adversely influence a widespread adoption. For the scope of this paper, some of these drawbacks are particularly relevant and can be summarised as follows.

• Market dynamics and volatility of networks

Originally designed to achieve disintermediation in the financial sector, permission less blockchains are generally reliant on voluntary participation of individuals and speculative rewards mechanisms to validate transactions. By their own nature, they are hence exposed to unpredictable market fluctuations, which may endanger their operational capacity over time. While data are permanent in the blockchain, the blockchain is not permanent per se: it can be actually quite volatile, depending on factors such as quality and quantity of nodes, incentive mechanisms and speculation, network effect, and more. Since business continuity is not guaranteed in permission less blockchains, they may be unsuitable as a permanent store of value and digital data in the long run. This limit adversely affects first and foremost highly sensitive sectors such as e-government, public administration and banking (Atzori, 2015), but many other classes of services as well. Volatility has indeed particular relevance for long-term preservation and notarisation of data (namely proof-of-existence of data through time), costumer protection and law compliance in both public and private sector, potentially compromising persistence, preservation and future execution of agreements and transactions between parties, as in the case of smart contracts (Atzori, 2015; DuPont & Maurer, 2015). Which suggests that the functionalities of blockchain networks as a store of value and as a medium of exchange exposed to speculative investments should be kept separate, so to minimize systemic risk for sensitive services layered on the top of them (Atzori, 2015).

• Technical shortcomings

Services requiring high level of performance are unable to thrive in the absence of adequate technical standards. Open blockchains are still at an early stage of development and need to overcome many weaknesses, related for instance to insufficient security, scalability, and capacity of the network, in terms of latency, throughput and bandwidth (Bos et al., 2015; Cortois, 2014; Croman et al., 2016; Ittay & Gün Sirer, 2014; McConaghy et al., 2016). A further problem is caused by irrelevant data (Greenspan, 2015): since open blockchains are typically multipurpose, institutions running their services over such networks would process and store a significant volume of data, which are of no concern to them (Greenspan, 2015), in so also dissipating their computational effort (Monax.io).

Blockchains should rather be streamlined for the domain within which they have been deployed, ensuring high performance, low latency and appropriate level of security, so they can best fit specific purposes (Government Office for Science, 2016; Monax.io).

• Law compliance and lack of liability

Open networks are governed by their own technical codes, regardless of geographical boundaries, and this makes it difficult to enforce legal codes issued by state authorities (Government Office for Science, 2016). On one side, regulators have a limited capacity to put in place appropriate safeguards, establish responsibilities and ensure compliance within open peer-to-peer networks - which typically focus on decentralisation of services as a way to empower individuals and promote principle of self-organisation, with limited or no legal intervention in human affairs (De Filippi, 2014). On the other side, however, the services market and especially the financial industry are highly regulated: businesses and operators are required to provide information to authorities and prove compliance with an extensive set of rules, and transactions executed on a blockchain may not have adequate legal recognition. The lack of liability and regulations governing blockchain services – relating for instance to costumer protection – may also easily undermine users' confidence and discourage them to embrace innovative solutions.

This demonstrates the worth of developing new standards and ensuring effective interaction between technical code and legal code (Government Office for Science, 2016). To mitigate uncertainty and facilitate full compliance with the law are in fact essential conditions for businesses and services to thrive.

• Lack of confidentiality and privacy

In public blockchains, the nodes of the network have access to each other's data, and transactions are visible to those who explore the ledger. In Bitcoin, a pseudo-identity system allows users to be identified only by the public-keys, but existence, history and flow of transactions are publicly available, so all information associated with users can be retroactively mapped and exposed, if their identity will be revealed at some point in future (Greenspan, 2015; Nakamoto, 2008; Reid & Harrigan, 2011).

To overcome this problem, participants may use different addresses when sending or receiving transactions (Nakamoto, 2008); other solutions such as fully homomorphic encryption (FHE) and zero-knowledge proof are also interesting, insofar they make transaction inputs visible to senders and recipients only, but they are currently still time-consuming, not practical and inefficient to be widely deployed (Gentry, 2009; Greenspan, 2016; Zyskind, Nathan & Pentland, 2015a).

The transparency of the ledger is often referred to as one of the greatest advantage of the blockchain technology, in line with a new social trend which seems to prioritize transparency over anonymity (Boucher, 2017). Nonetheless, privacy, confidentiality of transactions and data protection are a prerequisite for a wide range of services, especially in sectors such as finance, banking, healthcare, e-government and public administration. Openness and transparency of ledgers usually represent a disadvantage also for firms, because they make it impossible to easily share confidential information or data aggregates with selected users only. Understandably, the risk of losing competitive position or other advantages while making information openly available may prevent many businesses from using public ledgers.

• Limits of open governance and the problem of democracy

Peer-to-peer systems like Bitcoin allow anyone to join the community and validate transactions according to a set of rules embedded in a code, with the possibility for each participant to opt-in or out at will. The new forms of direct interaction between individuals enabled by the blockchain technology have led many enthusiasts to challenge the existing political and administrative structures, promoting principles of self-governance based on consensus. In this regard, however, it is important to clarify some important points, and briefly expose the limits which make permission less blockchains unsuitable for sectors such as public administration and e-government.

The first problem is that open governance can easily turn out to be weak and fragmented. Understandably, the absence of stable, reliable governance structures and traditional safeguards for costumers (European Parliament Resolution, art. 2a,b), along with frequent blockchain forks or even hard forks, may aggravate uncertainty among users and stakeholders, discouraging application in risk-averse sectors.

The second is that, contrary to what is widely believed, open governance and decentralisation do not automatically mean fair and democratic governance, nor do they necessarily entail equal opportunities for citizens. While in theory no one owns or controls distributed networks, several factors may prevent open networks from gaining and preserving a true democratic and egalitarian structure over time, such as: digital divide and cognitive entry barriers to digital communities and hackathons; strong asymmetries of information between developers and users; moral hazard and the prevalence of economic individualism over common good; core developers' stewardship with special rights in conflict resolution; poor network neutrality and clusters of interests informally acting as centers of steering (Atzori, 2015; Curtois, 2014; Gasser, Budish & West, 2015; Gervais et al., 2013).

The last point is that democracy - as a principle and also as a procedure - cannot be reduced to majority rule and consensus ex post, typical of decentralised networks, which entails members of a community to accept (or not) rules already established by developers. Democracy is a much more complex concept, which requires, among other things, 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.

The potential of the blockchain governance and the limits of the mainstream narrative built around it should therefore be critically examined to the light of these concerns.

Thus, for example, the assertion that the blockchain has a sovereign dimension and the constitutional properties of a nation state, and that it is even able to compete against the State (Bitnation.co; Davidson, De Filippi & Potts, 2016) may risk to promote a deeply undemocratic trend in the application of the new technologies at global level. From the standpoint of democratic theory, a group of individuals who cluster around specific interests and temporarily agree on a common set of (algorithmic) rules is nothing more than a private club with no legitimate self-originated sovereign power, and importantly, it represents a relative experience, which cannot "compete" against institutions legitimised by universal suffrage.

Although democratic theory continues to evolve, any exuberant notion of self-organised sovereign community, "private polycentric governance" (Allen, 2016), "authority floating freely" (Swan, 2015) or "algorithmic authority" as a "legitimate power to direct human life" (Lustig & Nardi, 2015) still has to contend with the principle of legitimacy – also considering that algorithms are ultimately human artifacts and they entail assertion of human authority (Atzori, 2015; Musiani, 2013).

Now, the principle of legitimacy is not a trivial issue: it is actually crucial, on both the political and legal level. In fact, it marks the difference between a blockchain governance conceptualised within a democratic framework, and a possible new virtual feudalism, which seeks to justify and advocate the triumph of relativism, alleging technological progress, open innovation, and algorithm-based automatisms.

In this regard, it is important to recall that blockchain networks represent great organisational tools, which can significantly improve the democratic governance, and they should be construed and promoted as such; by their own nature, however, they do not have the properties of stand-alone, entirely self-sustainable political systems (Atzori, 2015), able to represent a viable democratic alternative to institutions and their constitutional principles.

It is true that in the network age, we cannot rely on too rigid, permanent rules (Paquet, 2005); however, if networks only consist of "a loose web of agreements" (Guéhenno, 1993; Paquet, 2005) and they are not anchored to stable and democratically shared principles, the risks is to deconstruct our socio-political dimension and transform it into what is was defined as spectralitè (Guillaume, 1984 ; Paquet, 2005): a new form of interaction where "spectres who do not know one other meet" (Baudrillard & Guillame, 1994; Paquet, 2005), giving rise to "a society of phantom-like nomads" (Paquet, 2005), where relationships are disembodied, coordination is difficult, and anonymous market-type linkages are the only ones feasible (Paquet, 2005).

Risks and drawbacks of open governance and permissionless blockchains must therefore be carefully assessed with particular reference to their possible undemocratic development, before promoting forms of "do-it-yourself public administration" (Swan, 2015) or other essential services on the top of them. As Kiviat (2015) rightly noted, "the blockchain technology can support different kinds of dreams": but precisely because there are so many different legitimate interests and stakeholders in society deserving protection, the main challenge of the blockchain governance is still to achieve a balance between innovation, individual ethos, and the broader public interest.

3. Permissioned blockchains and systemic trust: the role of Trust Service Providers

Technical structure, functionality and coordination of distributed ledgers can be streamlined for specific sectors and purposes, through controlled access permissions, different verification systems and visibility of data. While such permissioned blockchains are inevitably more closed and less transparent than those organized in fully-decentralised manner, they may bring other significant advantages, overcoming some of the limitations of public blockchains. For example:

- Ledgers can be designed as token less, keeping data safe from speculative rewards mechanisms;
- Security, scalability, capacity and general performance of the network can be optimised and adapted to specific functionalities;
- Law compliance, consumer protection and confidentiality of transactions can be achieved as needed, through an adequate degree of centralisation and even further regulation, if necessary.

Compared to open networks, thereby, permissioned networks enable a more effective and complex governance, suitable for complex tasks.

Even permissioned blockchains, however, may present significant challenges. The main problems lie with volatility and business continuity, since there may be no guarantee that networks will still be operative or even exist in some distant future. The question may thus arise of which entities can be sufficiently reliable as nodes of a blockchain, so to ensure long -term preservation of transactions, without exposing data to market fluctuations or token speculation.

To overcome volatility and ensure systemic trust of platforms - especially in sensitive sectors such as public administration, e-health or finance, which are not tolerant of service disruptions - one solution would be to engage Trust Service Providers (TSP) as the only full nodes, able to verify the transactions of the network.

The TSP are highly qualified market operators with EU trust mark, appointed by European governmental agencies after a strict conformity assessment, in compliance with Regulation EU No. 910/2014 -eIDAS. They typically provide services such as: the creation, verification and validation of electronic signatures, seals, time stamps or digital certificates; and the management of electronic storage and archiving for documents.

The eIDAS Regulation establishes a general legal framework for digital services provided to the public and having effects on third parties (21). It forces TSP to meet specific requirements in the provisioning of services, relating to high-level security standards (Art. 19), use of trustworthy systems (Art. 24), performance audit (Art. 20), legal certainty and costumer protection (Art. 13.2; Art. 19.2), with a view to ensuring trustworthiness of services and long-term preservation of information (61). Importantly, the Regulation provides for the liability of TSP in the case of non-compliance with due diligence (37) (Art. 13).

The deployment of blockchain-based services by TSP may be facilitated by Art. 62, which allows TSP to introduce new technologies and advanced methods to perform their duties, until they can provide an equivalent level of security and fulfil the obligations laid down in the Regulation.

Compared to other permissioned networks, the development of blockchain networks by TSP under eIDAS Regulation may have a strong added value, leading to significant benefits for sensitive services, such as:

- Systemic trust, technical performance and privacy

Long-term preservation of data, business continuity, high-level of security standards, privacy and confidentiality of transactions are essential factors for users, public administration and businesses, in order to develop reliable services and fully benefit from new technologies. Unlike other market operators which may run permissioned networks, the TSP are the only certified entities legally required to fulfil those conditions. Being highly regulated, they have a unique market position, with a unique kind of added value in terms of reliability, security and operative capacity over time. They can hence develop a clearly defined and robust blockchain governance, minimising hazards and compensating possible market failures caused by volatility and proliferation of hit-and-run services, in so countering the possible gamification of essential services. TSP are also obliged to protect confidentiality of data. Such a high level of reliability can affect positively the general perception of users, institutions and investors about blockchain-based services, leading to a safer and faster adoption.

• Automatic law compliance, liability and legitimacy

Unlike other market operators which may need further regulation, the TSP blockchain networks directly apply the EU strict provisions already existing for digital services under eIDAS Regulation, which already harmonizes TSP behavior, liability and procedures. EU follow-up measures and decisions by national regulatory authorities about the blockchain services can be automatically transposed into the TSP network and then applied in many areas, effectively combining legal and technical code, and easily establishing and enforcing responsibilities (Government Office for Science, 2016). Law compliance has the effect to anchoring the blockchain to stable principles set out by legitimate institutions, serving the broader public interest. If well-balanced by the principle of "decentralise as much as possible, regulate as much it is needed" (Paquet, 2005), common international standards and regulation automatically implemented in the TSP networks can be the source of technological development rather than just a constraint, speeding up the adoption of blockchain solutions, and fostering moral progress and innovation.

In turn, even TSP may gain significant benefits from the adoption of the blockchain technology.

The digital services they typically provide– such as timestamps, electronic seals, document storage and archiving – can be managed in a cheaper and more effective way with the blockchain technology, improving security and efficiency across industry, but also ensuring privacy and technological neutrality. The blockchain would prevent indeed TSP to indiscriminately gain and collect sensitive information of the citizens, especially relating to online authentication services – an issue which has already raised the legitimate concerns of The Council of European Professional Informatics Societies (CEPIS) for possible risk of user monitoring, profiling and tracking (Hölbl, 2016).

4. The TrustedChain® network: overview

TrustedChain® is the first permissioned blockchain network of European Trust Service Providers currently in operation. Designed by Ifin Sistemi in partnership with Monax Industries, TrustedChain® is engineered to meet the needs of highly sensitive services, both within public administration and private sector. It only accepts TSP as verifiers of transactions and it leverages their high technical standards required by the law, in order to provide a trustworthy and reliable blockchain-based ecosystem, which ensures long-term preservation of data, along with adequate security, scalability, reliability, continuity of service and law compliance.
TrustedChain® is currently the biggest permissioned blockchain of its kind in Europe, both for quality and number of nodes, as well as for number of transactions.

Leveraging the experience and the long-established market positioning of some TSP in specific sectors, the TrustedChain® eco-system allows to develop applications in different vertical sectors, such as public administration, healthcare, banking and industry (infra § 5), also supporting the use of smart contracts and AI functionalities. Processing data of several Italian public institutions, such as municipalities and regional governments, the network also introduces the blockchain technology in the Italian public administration for the first time.

• From inertial data to "green data": the new ecology of digital services

The TrustedChain® network allows TSP to share and extract value from the data they manage.
So far, the mission of TSP was to ensure digital information to remain accessible and usable over time. Albeit of crucial importance, the digital preservation of TSP has kept data in an inertial condition, since it was not possibile to share them without affecting confidentiality and legitimate interests of their owners.

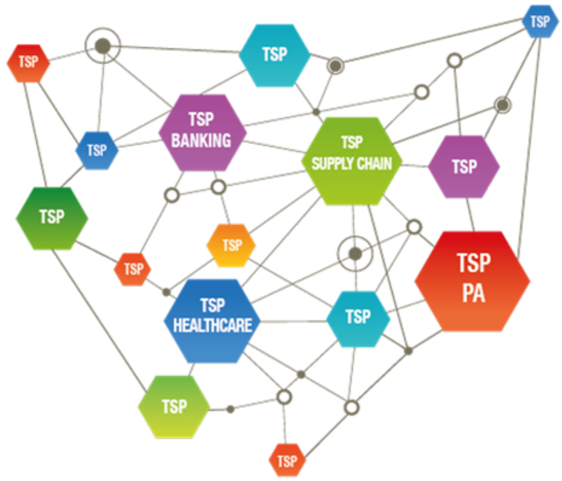


Figure 1: The TrustedChain® Ecosystem

TrustedChain® is conceived as a secure eco-system, which enables all participants to safely share sensitive data and extract value from them for mutual advantage, without compromising confidentiality of transactions: privacy is indeed enforced by-design (Zyskind, Nathan & Pentland 2015a,b), namely automatically and in a decentralised fashion, throughout the engineering process. Thanks to the off-blockchain data storage and the use of blockchain as a trustless access-control manager, data queries and calculations are processed off-chain only and in a completely distributed way (Zyskind, Nathan & Pentland 2015a,b). Thereby, through different layers of control, permission and visibility of data, the blockchain makes possible to safely remove the barrier of sharing data with untrusted sources or even competitors, reducing friction and meeting different market and management needs across many industries. Businesses, for example, may hide sensitive information and only share those data that do not endanger their competitive position in the market – especially when a wide array of unknown stakeholders and competitors are involved.

This ad hoc algorithmic governance ushers in a new ecology of digital transactions and services, based on green data: these are data which are generated, managed and shared between untrusted or unknown participants for different purposes – for example of a commercial, statistical or scientific nature – and create value for the stakeholders involved and the whole ecosystem, but always in the full respect of sector-specific regulations and without compromising confidentiality, privacy, interests and will of data owners.

Green data may also be viewed as opposite to Big Data (Zyskind, Nathan & Pentland 2015b), typically generated by platforms lacking in adequate privacy policy. Especially through ubiquitous computing and IoT applications, "the atomic age of data" (Goodman, 2015) has fueled public concern about security and privacy of digital platforms, since users may be exposed to several threats, such as identification, localisation, monitoring, tracking, surveillance, manipulation, profiling, targeted advertising, data linkage, data breach and even social engineering (Langheinrich, 2001; Ziegeldorf, Morchon & Wehrle, 2013; Zyskind, Nathan & Pentland 2015b).

Thanks to the principle of privacy-by-design, a creative engineering and deployment of green data may boost research, innovation and the development of new business dynamics in different sectors, to the benefits of many stakeholders. The more the data shared in the ecosystem, the bigger the value generated. This triggers a virtuous circle and a network effect, attracting new participants with increasingly variegated and complex combinations of data sharing, and new models of economic incentives as well. AI and machine learning patterns with both reactive, proactive and predictive functionalities can also be used to extract value from data even more effectively.

In this regard, it should be recalled that it is not possible to generate green data with open blockchains such as Bitcoin: green data require off-blockchain heavy computation on private data, namely on data with permissioned visibility; Bitcoin transactions instead are completely visible to the nodes and to those who explore the ledger, and the system cannot properly handle heavy computation (Zyskind, Nathan & Pentland, 2015b).

	bitcoin	Permissioned Networks	TrustedChain®
Trustless Environment	✓	✗	✗
High technical performance	✗	possible	ensured by law
Law Compliance	✗	possible	ensured by law
Consumer protection	✗	possible	ensured by law
Confidentiality of transactions	✗	possible	ensured by law
Business continuity	not guaranteed	not guaranteed	ensured by law
Long-term preservation of data	not guaranteed	not guaranteed	ensured by law
Green data	✗	possible	✓

Figure 2: - Basic features of Bitcoin, permissioned networks and TrustedChain®

5. TrustedChain® main fields of application

TrustedChain® supports applications in sensitive sectors, such as:

- Document storage and archiving - The application of the blockchain technology can have particularly relevant effects on the traditional TSP storage services. The tamper-resistant, non-reputable timestamp enabled by the algorithmic protocols can automatically certify the existence and the exact content of any file at a certain date and time (Swan, 2015), ensuring data integrity, accuracy and reliability, and thus complementing the traditional TSP function of long-term preservation of data. "Rather than simply storing the documents, as is done today, a shared ledger system would record proof of the state of those documents" (Government Office for Science, 2016). Importantly, the proof-of existence can have several applications in the legal field, since it can demonstrate the existence of any digital asset at a certain date and time, without showing its contents, and keeping confidentiality (Swan, 2015).

- *e-Government and public administration* - The blockchain technology can offer immediate advantages for public institutions through different applications: from the resistance to tampering and protection of document integrity, to the automation and effectiveness of tax collection and administrative workflows.
  The blockchain has the potential to transform the delivery of public service, improve governance, reduce fraud and also foster the confidence of citizens in institutions and digital services (Government Office for Science, 2016).

To this aim, TrustedChain® applications include:

- The tamper-resistant, decentralised and efficient management of digital identities and

public records, such as fiscal information, judicial data, information concerning immigration flows, etc. Among many applications of the blockchain technology for public administration, record keeping represents one of the most immediate (Boucher, 2017): it allows for a reduction of redundant data, cost, time and need for infrastructure, and it may lead to a significant saving in public expenditure;
- Interoperability and notarisation of permissioned ledgers developed within public administration: TrustedChain® is compatible with any blockchain framework and it can preserve other ledgers over time;
- Smart contracts and multi-signature transactions: these features may improve the effectiveness of tax collection, and also manage and keep track of both public and private funds, with provable transparency and traceability (Government Office for Science, 2016; Swan, 2015);
- Data cross analysis and AI: they can be used to improve public governance, reporting anomalies or predicting future problems based on machine learning patterns, while always protecting citizens personal information and privacy.

• *Finance and banking* - The blockchain technology can be effectively applied to: reduce cost, time and complexity of the payment, clearing and settlement infrastructures; secure data and transfer of digital assets; gain competitiveness, also through the adoption of new business models and applications, such as smart contracts and multi-signature transactions.

TrustedChain® provides financial services with a trust-by-design platform, overcoming the typical risks of open networks, and ensuring security, confidentiality of data and law compliance. It also supports smart contracts, for the purpose of reducing transaction time, costs and risks, as well as AI applications. While the latter are already being used by banks, they can be significantly enhanced by the integration within the TrustedChain® ecosystem, since it allows data to be shared between untrusted participants. Indeed, AI models can become much more accurate and efficient if they can access the data of several banks within the same system, instead of only one. In turn, a more accurate AI response can lead to a reduction of workflows and hence greater savings (e.g.: banks may detect frauds or identify unworthy borrowers more quickly).

• Healthcare - The health sector typically generates, manages and stores big volumes of sensitive data, often causing understandable concern about security, protection of privacy and anonymity of patients. As a consequence, patients may often be refrained from sharing their clinical data and trials for scientific or statistical purpose. The insufficient consent of patients for data sharing may generate significant social and management costs, since it can adversely affect: the quality of scientific research and statistics, due to lack of updated and/or crossed data records; the adequate understanding of costs and benefits of therapies and treatments, due to under-reporting; the prompt response to particular diseases, such as epidemics (Chamber of Digital Commerce, 2016).

TrustedChain® applications aim at eliminating friction and ensuring privacy, security and systemic trust within e-Health systems.

In particular:

- The algorithmic protocols allow patient identities to be safely verified and tracked;
- Data can be collected, shared and analysed for scientific, statistical or commercial purpose, always protecting the privacy of patients by-design (i.e. green data);
- The procedures to obtain patient consent for data sharing can be automated in a time- and cost-efficient way through smart contracts;
- The exchange of clinical data between medical infrastructures and research institutions can be safely enabled, improving scientific research to the benefit of the entire industry and patients themselves; database can be created for specific problem or purposes (e.g. for transplant) and updated in real-time, without disclosing personal information of patients involved;
- AI applications can be used for automatic diagnosis, medical image processing, prediction of future pathologies, personalised management of care pathways and therapies, and the creation of a broader clinical picture of the patient, including data from wearable devices.

• Industry (and other services) - TrustedChain® aims at simplifying and improving the efficiency of complex industrial workflows, for example through the traceability of products of an entire production chain from raw materials, in so preventing and combating counterfeiting. But the fields of application of TrustedChain® also include insurance and energy sectors.

Smart contracts can be used to automatise and make transactions seamless and more efficient; AI applications can also be deployed to analyse data and support the decision-making phase of workflows, with reactivity but also proactively, pointing out and predicting potential hazards and risks. The technological solutions implemented within TrustedChain® are expected to be a starting point for even further industrial applications, arising from the daily confrontation of developers with the experiences of users.

5. Conclusion

Fully-decentralised blockchains represent one of the many possible models of blockchain governance. Because of its many limits, however, it should not be assumed that such model is always effective for any field of application, or the only true way to deploy the blockchain technology - as it was endowed with an undisputed and superior worth. Permissioned blockchains are often perceived as a suboptimal solution or a major brake on innovation, but that view is rather simplistic. The blockchain must be fit for purpose. Accordingly, technical trade-offs, regulation and the plurality of values of the stakeholders involved should always be carefully evaluated, choosing the best model of blockchain governance which satisfies functional requirements of specific usage areas, and serves sustainability in the long run.

In this context, it must also be recognised that a perfect blockchain governance may not exist in practice. Compromises are possible and necessary in a multi-stakeholder framework: there may be many possible alternatives for action, and the appropriate mix of centralisation and decentralisation should be tailored to specific use cases, applying creativity, multi-disciplinary knowledge and technical skills.

Trust Service Providers can play a fundamental role in the blockchain governance, validating the transactions of highly sensitive sectors and providing an ecosystem in which services can safely thrive. Systemic trust, clearly defined governance, law compliance, adequate technical performance, confidentiality of transactions and long-term preservation of data are indeed essential conditions for blockchain networks to accomplish complex tasks in an effective and reliable way and promote sustainable innovation.

TrustedChain® is the first cutting-edge network of European TSP, which captures the benefits of the blockchain technology and offers a reliable and risk-free infrastructure upon which public administration and private sector can run specific, decentralised applications. The TrustedChain® ecosystem also allows for AI functionalities and data sharing between unknown parties or competitors, giving rise to a new ecology of data, enabled by privacy-preserving computation techniques. This shows that innovation is not only a prerogative of open networks: even permissioned blockchains may have a strong innovative capacity, and the benefits of a relatively centralised governance can thus be significant.

The active involvement of TSP and the implementation of networks such as TrustedChain® may be highly useful to the faster development of blockchain-based services; additional legislation and standardisation at the international level may then facilitate the seamless integration of blockchain services into specific sectors.

References

Allen, D. W. E. (2017). Blockchain Innovation Commons. Available at SSRN: https://ssrn.com/abstract=2919170

Allenby, B.R. (2012). The Theory and Practice of Sustainable Engineering (1st ed.). Upper Saddle River, NJ: Pearson Prentice Hall

Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is The State Still Necessary?. Available at SSRN: http://dx.doi.org/10.2139/ssrn.2709713

Baudrillard, J. & Guillaime, M.(1994). Figures de l'altérité. Paris: Descartes & Cie

Bitnation.co. Governance 2.0. Available at: https://bitnation.co

Blockchain Technologies (2016). What are Blockchain Applications? Use Cases and Industries Utilizing Blockchain Technology. Available at: http://www.blockchaintechnologies.com/blockchain-applications

Boersma, K., Meijer, A., & Wagenaar, P. (2009). Unraveling and Understanding the e-Government Hype. In A. Meijer & al., ICTs, Citizens and Governance: After the Hype! (1st ed., pp. 256-265). IOS Press

Bos, J., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., Wustrow, E.,(2014). Elliptic Curve Cryptography in Practice. In Nicolas Christin & Reihanen Savafi- Naini, (Eds.), Financial Cryptography and Data Security. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers (1st ed., pp. 157-175)

Chamber of Digital Commerce (2016). Smart Contracts: 12 Use Cases for Business & Beyond. Available at https://digitalchamber.org/resources/chamber-reports/

Croman, K., et al. (2016). On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security. (pp. 106-125). Springer Berlin Heidelberg. Available at: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

Curtois, N. (2014). On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies. http://arxiv.org/abs/1405.0534

Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of Blockchain. Available at SSRN: http://dx.doi.org/10.2139/ssrn.2744751

De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. Internet Policy Review, 3(2). DOI: 10.14763/2014.2.286

DuPont, Q. & B. Maurer, (2015). Ledgers and Law in the Blockchain. KR. Available at:
http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/

Earls, A. (2016). Blockchain not a panacea for supply chain traceability, transparency. TechTarget. Available at: http://searchmanufacturingerp.techtarget.com/feature/Blockchain-not-a-panacea-for-supply-chain-traceability-transparency

European Parliament Resolution (2016). European Parliament Resolution of 26 May 2016 On Virtual Currencies (2016/2007(INI)). Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228+0+DOC+XML+V0//EN

Gasser, U., Budish, R., West, S. M., (2015). Multistakeholder as Governance Groups: Observations from Case Studies. Berkman Center Research Publication No. 2015-1. Retrieve from http://ssrn.com/abstract=2549270

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In STOC, vol. 9 (pp. 169–178).

Gervais, A., Karame, G., Capkun, S., & Capkun, V. (2013). Is Bitcoin a Decentralized Currency?. IACR Cryptology ePrint Archive, 2013, (p. 829).

Goodman, E. (2015). The Atomic Age of Data: Policies for the Internet of Things. Available at SSRN: http://ssrn.com/abstract=2605201

Government Office for Science (2016). Distributed Ledger Technology: Beyond Blockchain. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Greenspan, G. (2015). MultiChain Private Blockchain — White Paper. Available at: http://www.multichain.com/download/MultiChain-White-Paper.pdf_____(2016). Understanding zero knowledge blockchains. MultiChain.com. Available at: http://www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/

Guillaume, M. (1984). Crise et Chuchotements, Graduate Institute Publications, 1984. DOI: 10.4000/books.iheid.3357

Guéhenno, J.M. (1993). La fin de la démocratie. Paris: Flammarion.

Hölbl, M. (2016). Position on the Electronic identification and trust services (eIDAS). Council of European Professional Informatics Societies (CEPIS). Available at: http://www.cepis.org/media/Position%20on%20the%20Electronic%20identification%20and%20trust%20services%20(eIDAS).pdf

Ittay E., & Gün Sirer. E., (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. In Nicolas Christin & Reihanen Savafi- Naini (Eds.), Financial Cryptography and Data Security. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers (1st ed., pp. 436-454). Available at: http://www.cs.cornell.edu/~ie53/publications/btcProcArXiv.pdf

Kiviat, T. I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. Duke Law Journal, 65, pp. 569-608. Available at: http://www.the-blockchain.com/docs/Beyond%20Bitcoin-%20Issues%20in%20Regulating%20Blockchain%20Transactions.pdf

Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. Presented at International conference on Ubiquitous Computing. Available at http://cs.gmu.edu/~jpsousa/classes/699/papers/privacy%20Langheinrich.pdf

Lustig, C., & Nardi, B. (2015, January). Algorithmic authority: The case of Bitcoin. In System Sciences (HICSS), 2015 48th Hawaii International Conference on System Science (pp. 743-752). IEEE.

McConaghy, T., et al. (2016). BigchainDB: A Scalable Blockchain Database. Available at: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Monax.io. Explainer | Permissioned Blockchains. Available at https://monax.io/explainers/permissioned_blockchains/
Musiani, F. (2013). Governance By Algorithms. Internet Policy Review, 2 (3). DOI: 10.14763/2013.3.188

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

Paquet, G. (2005). The New Geo-Governance. A Baroque Approach. (1st ed). Ottawa: The University of Ottawa Press.

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services For Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC

Reid, F. & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. Available at: https://arxiv.org/abs/1107.4524

Swan, M. (2015). Blockchain. Blueprint For a New Economy. Sebastopol, CA: O'Reilly

Wright, A. & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available at SSRN: https://ssrn.com/abstract=2580664

Ziegeldorf, J., Morchon, O. & Wehrle, K. (2013). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), (pp. 2728-2742). Available at https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf

Zyskind, G., Nathan, O. & Pentland, A. (2015a). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops (SPW), (pp.180–184). Available at: http://web.media.mit.edu/~guyzys/data/ZNP15.pdf
_____(2015b). Enigma: Decentralized Computation Platform with Guaranteed Privacy. Available at: http://arxiv.org/pdf/1506.03471v1.pdf.

Photo by Héctor J. Rivas on Unsplash

COMMENTARY

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(5)2018

Why and How Blockchain?

Mark D. Wolfskehl[1] Ph.D.
CEO, Blockchain Innovations, Inc.
Correspondence: mark.wolfskehl@binv.us

Received: 19 April 2018 **Accepted:** 20 April 2018 **Published:** 23 April 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
MW [1] wrote this commentary in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

We discuss the current state of blockchain in the technical industry and discuss blockchain's decentralization roots and its inclusion in the world of mainstream corporate technology. We include some technical background and issues in the context of the industry, feasibility, and future directions. We offer speculation as to how blockchain technology may serve various competing agendas. The purpose of this paper is to raise questions more than provide answers - to stimulate thought and discussion - in the context of the technology and its positioning in the centralisation vs. decentralisation spectrum of interests.

Keywords: *trends, analysis, opinion, technical, blockchain*

Blockchain was unleashed on the world in the form of Bitcoin in the hopes of transforming at least the financial sector of the world into a populist haven where anarchy rules and the average person does not have to become beholden to big banks, governments and other institutions for monetary needs.

In 2018 Blockchain is now mainstream where those same big banks, governments and every institution large and small, sees Blockchain as the cure for all its ills. I find this at least somewhat curious. Blockchain certainly does seem to hold potential for decentralisation of technological institutions of all sorts. This is something that would probably fit neatly along the lines of thinking of the original developer of Bitcoin. However, I think the fact that centralised institutions now find blockchain useful deserves a closer look.

Certainly, whenever there is a boom in any sector of the economy greed will rule, and people regardless of ideology will seek to cash in. But however, exciting the promise of Blockchain there is also a side of high cost. The Proof of Work algorithms central to most blockchain implementations extract a huge cost in computing power (this is the "work" of which is spoken), unusual hardware requirements, and energy consumption. Blockchain Innovations, Inc. is currently investigating how we might be able to retain or even increase the level of decentralized security provided by Proof of Work while removing, well, the work. By doing so we hope to allow the owner of the average PC without superhero-level hashing power the ability to participate and contribute to any blockchain without spending unsustainable amounts of money on graphics cards and electric bills.

It is understandable that the hashing power requirements that are currently blocking entry for "the average Joe" are easily met by large institutions. Irony aside though it is curious why such institutions would care about blockchain in the first place. Is your blockchain going to be behind a firewall? Is it going to be managed and controlled by one centralized organisation? When the application is going to be run in a centralized manner anyway, a rational individual would consider the added complexities of a blockchain implementation.

There is also a high cost for "programmer power" to implement blockchain solutions. One designs a complex blockchain solution that is broken down in a decentralized manner, throws large amounts of money at it, unusual hardware into running the software, and expends a lot of energy running a Proof of Work algorithm. In terms of "programmer power" we are not just talking about highly skilled employees who don't come cheap. There will also be a long-time lag from concept to implementation of a very complex solution. And in terms of business, doesn't time = money? The next step then is to run such a solution in a centralized data center by a single organisation. Make sense? In an age where efficient centralised server solutions are available off the shelf and are extremely cheap and easy to customise it does appear at least on the surface to have some aspects of irrationality from the economic perspective.

For those who wish to truly operate in a decentralised manner blockchain certainly make perfect sense. However, it is not my position to argue even that anyone considering a blockchain solution to be run in a centralized manner drop such plans. What I am suggesting is that the trend is curious and deserves some contemplation. Are there deeper reasons at play that are perhaps not immediately obvious?

One possibility is that one can very reasonably differentiate between blockchain as a software systems technology and cryptocurrency as a competitor for government-issued fiat. On the other hand, one might also argue that by filling the technology sphere with blockchain one obscures to oneself the fact that the basis of the technology has to date been almost exclusively in implementing cryptocurrency. However, marketing is marketing. And if the world sees the word "blockchain" more than the word "cryptocurrency" could this be viewed by "the big boys" as a good thing?

An interesting consequence though is that through this trend the number of blockchain projects can only be expected to skyrocket. This affects public projects as much as projects inside the data center, and the adoption rates of both are increasing. But perhaps this is not viewed as a problem? Because another possibility of the conscious and rational variety might be the hope that an application will develop that will take blockchain away from finance.

However, we have another trend in the technology industry today. That is one to make minimal investment and still turn around a product. One might term this the "lowest hanging fruit" approach. This is a short-sighted view that plagues the industry at the same time as the blockchain boom. And it ensures that the overwhelming majority of blockchain projects will remain in the realm of fintech for a long time to come. This in turn is going to cement blockchain's association with cryptocurrency. No significant shift will happen without a willingness to invest the time and money to reinvent (and re-code) from the bottom up.

But there are other possible explanations. Every large corporation today hires programmers. And the best programmers always want to be on top of the hottest technology. And what is the hottest technology today? Blockchain. Could this be why JP Morgan Chase developed a smart contracts system as a fork of Ethereum? It is easy to imagine some genius programmers lurking inside the closed doors begging for a chance to play with Ethereum.

This is pure speculation on my part. However, keeping the high demand developers happy for what must be an infinitesimal investment for a large bank makes perfect sense. What could be the harm? But once one has a successful project it is hard to just throw it away. And we see this in Chase's spinning off of the project now as a separate company.

On another level blockchain currently has a certain "hotness" about it, regardless of how we got here. At this tipping point one might say that the demand is such that people will jump at the opportunity to implement anything. This does require one to take the view that at least at some certain level humans are not rational creatures – not a controversial one to me personally. As we know supply must meet demand. So, I think we are going to be seeing an ongoing trend for a while where people hear the word "blockchain technology" and will immediately think of a place where blockchain must apply. Blockchain sells.

One thing is still curious, and that is that even removed from cryptocurrency the heart of blockchain is still anarchist in nature. Once put out there, it cannot be controlled. That was the point of Bitcoin in the first place. Could there be some hope amongst proponents of centralization that this nature can be changed?

The heart of the Proof of Work implementation of blockchain technology is really a very clever solution to Byzantine consensus. The best explanation I have seen to this effect is in Mastering Bitcoin by Andreas Antonopoulos [1]. However, the desire to have a "hive" of nodes cooperate in unison could also be potentially viewed as the very opposite of anarchy, perhaps even to the point of tyranny.

Does this mean that the nature of blockchain can be changed from an anarchist one, if one understands its true role in distributed systems? Distributed consensus is fundamentally a technology problem. And a solution to distributed consensus is just a tool. All tools can be used for good or for bad. But the type of consensus in Bitcoin – the emergent kind – comes from being fair and even handed. That means that (at least in theory) every node has an equal chance to have a say. So, while the "hive" can coordinate amongst itself, it is very unlikely that one individual can coordinate the hive. However, from this point of view the method of distributed consensus matters a great deal. I think this is the aspect of blockchain that is overlooked the most – for the very understandable reason that it is also the most technical. However, the fact and degree that it matters cannot be understated.

Proof of Stake is an almost drop-in replacement for Proof of Work that is currently being adopted by numerous systems. The very valid motivations previously mentioned of sustainability can easily be seen. However, it is the position of Blockchain Innovations and myself personally that Proof of Stake merely sidesteps the issue and fails to address the core problem of system security. Once a person or entity controls the largest stake can one not take over the network? Proof of Work is still the fairest solution, on a software architecture level, for emergent consensus that is widely available.

Some systems have gone back to older style messaging and leader selection models for obtaining Byzantine consensus. Such solutions are as complicated on a conceptual level as Proof of Work is unsustainable in hardware and energy. It is easy to convince oneself that Proof of Work is fair. It is not particularly dependent on network communication methods, aside from the simple need that all systems are eventually reached. After that a computational problem with random properties takes over the control mechanism in the form of a race. In the case of a protocol that is entirely dependent on a (typically very logically complicated) communications protocol fairness and even handedness is not easy to see at all. Vulnerabilities are highly likely to emerge over time. It could become very likely that even a single individual may take over the network – provided such an individual is extremely smart and insightful into the protocol.

So, we see that there exist hidden possibilities of centralization of the logical type. A warning to those with centralization interests is in order: the ability to take over a network is not without risk. Nobody can say that the takeover will be done by the intended party. The policy of maximal self-interest may still be to play fair.

Proof of Work to date appears to remain the fairest solution. But even Proof of Work is becoming de facto problematic. I have mentioned the sustainability issue a number of times. This can be stated in another manner: barrier to entry. We see that already the hardware and energy requirements in purely economic terms are hard for the "average Joe" to justify. And isn't Joe the one Satoshi Nakamoto originally had in mind to benefit the most from Proof of Work? This is a de facto issue of centralization that transcends the direct application of software architectural methods. Something must be done that addresses the barrier to entry without compromising on fairness. The solution currently under development at Blockchain Innovations addresses this issue along with the computation and energy sustainability issues while retaining the emergent consensus model embodied in Bitcoin.

In the end trends are trends and economics is economics. Making money is the game, and mutual benefit is the gain. If the forces of centralization and the forces of decentralization can approach the same technology and make advances at the same time society comes together. Peoples' fortunes across the spectrum increase. It is certainly preferable that apparently opposing forces compete on the economic playing field, one that is fundamentally peaceful.

Ultimately, what we are seeing is the emergence of an ironically symbiotic relationship in blockchain between those interested in centralization and those interested in decentralization. It is the intention of Blockchain Innovations to foster both "sides" by merely taking the attitude of contribution to the economy. By the same token, we think it is important to keep in mind that to truly be blockchain one needs to stick to the essential elements. So, we intend on the technology side to remain faithful to the principles and implementation aspects of decentralization embodied in the original Proof of Work implementation of Bitcoin. On the organizational level, we remain open and friendly to individuals and organizations regardless of placement on the spectrum of centralization vs. decentralization agenda.

People can hope. But ultimately nobody can truly know how blockchain will transform society in the long term. The exploration is exciting, and ultimately competition via peaceful means in an ever increasingly antagonistic (and so often violent) world is a good thing. We hope to see the advances continue.

References

[1] Antonopoulos, Andreas M., Mastering Bitcoin: Programming the Open Blockchain; Second Edition 2017; O'Reilly Media; Chapter 10: Mining and Consensus.

Photo by Álvaro Serrano on Unsplash

COMMENTARY

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(5)2018

The Return of 'The Nature of the Firm': The Role of the Blockchain

Prateek Goorha[1]
Independent scholar
Correspondence: goorha@sent.com

Received: 30 March 2018 **Accepted:** 31 March 2018 **Published:** 2 April 2018

Competing Interests:
None declared.

Author's contribution:
PG [1] prepared the manuscript in entirety.

Acknowledgements:
Not declared.

Abstract

In this note, I return to Coase (1937), on its 80th anniversary, to assess whether its logic and insight can be reconciled with the blockchain revolution. I argue that, indeed, it can, and propose the existence of a third method of organizing economic activity in a specialised exchange economy, in addition to the two that Coase considered. I call it the cryptographic stigmergy.

If there be such merit in the argument here, let it be dedicated to the memory of Ronald Coase.

Keywords: *Coase; firms; markets; blockchain; transactions; stigmergy*

1.

In this note, on its 80th anniversary, I wish to re-examine the merit of Coase's article, 'The Nature of Firm', rightly considered to be a keystone in economics, for the context of the blockchain economy. A professor once gave me sage advice on tackling Coase along the lines that, if I suspected that Coase may have made some error in logic somewhere, I would be well served to read again. With that caveat in mind, I take this task on perhaps to set his logic right in my own mind on the relevance of that brilliant paper to the emergence of blockchains.

Coase's article, as its title suggests, concerned itself with the task of defining a firm in the context of a market economy. So fundamental a concept needed defining then, because Coase felt that the extant assumptions needed a rethink. He felt that the task was worth his attention because the firm was understood differently by the common man and the economist.

In the intervening years since his article, nothing has altered. However, with the advent of blockchains, an incipient drift in the definition of the firm is increasingly becoming apparent again. The fundamental workhorse for both the blockchain and for Coase is the manner in which they organize transactions. It is a little surprise then that, when the manner in which they are processed is fundamentally altered, so too should the result from a Coasian analysis.

The poster children of blockchain – Bitcoin as a store of financial value and, somewhat more murkily, Ethereum as a store of innovational value — have helped insert the technology firmly into the common lexicon. Its effect on the economic system is, however, less vividly imagined. Enthusiasts of its applications have usually claimed too much for it, including as the messianic harbinger of a libertarian revolution that will obviate the need for government and regulation and remake economies. Detractors have usually missed the mark by even more, claiming that the technology is a flash in the pan and that its applications so far represent little of intrinsic social value.

This note is concerned with Coase's paper, and so these viewpoints matter only so far as they apply to the logic in his paper.

Coase began the paper by setting a standard that few analyses in economics meet: A definition of a firm that is realistic and tractable. And already our task is harder, since a 'blockchain firm' does not really exist, let alone in profusion enough to be used in any test for predictions against reality.

Coase provides the solution to this disadvantage, however. He argued that the economic system in which the firm was resident ought to be the starting point. He articulated the perception of the economic system as being one that, for the most part, still agrees well with our own. It requires no central authority and is directed by the price mechanism so effectively that it essentially operates on auto-pilot. Coase argued that somehow this guidance provided by the price mechanism was suspended within the boundaries of a firm. There, planning seemed to take over. It was this aberrancy, apparent at the time to Coase alone, that drew him to his thesis.

2.

That aberrancy has arguably been engendered again. The economic system has begun to be altered anew by the blockchain in two ways.

First, the boundaries for where the price mechanism is being suspended is being changed, not solely in favor of the market nor solely in favor the Coasian firm.

Second, the diploid system of price and planning is admitting a third in its midst, perhaps best described as cryptographic stigmergy. Stigmergy is the idea that a large group of individuals can interact through identifiable changes in their environment; when that environment is reliably reified in a blockchain, we have cryptographic stigmergy.

Coase asks why it is that the coordination ability of the price mechanism works admirably for market transactions but cannot continue in its function within a firm. He remarks that these are unquestionably different methods for achieving coordination. To these we now have a third: In the space of cryptographic stigmergy, the blockchain provides this coordination mechanism as a feature of its environment.

If this is true, we must put this new entry to the same test that Coase devised for the firm. Conceding that the degree to which the price mechanism is superseded varies, Coase proceeded by asking why there is an organization within a firm by an entrepreneur or manager at all when the price mechanism already exists for that purpose? Citing someone else, he asks why the firm must become a co-equal unit with other entities in the economic system that is then guided by the price mechanism. We, too, must ask why there is an organization by cryptographic stigmergy, so that we might better see whether there are differences between its modus operandi and those of the other two candidates.

The first reason that Coase considers is one that he quickly dismisses. The desire to lord it over others in the setting of a firm, or to hold some preference to be commanded about cannot, he surmises, be the reason for a firm's existence. I am not quite as sanguine about the infeasibility of this rationale in relation to cryptographic stigmergy. The desire to be 'one's own master' is certainly high on the list of stated reasons for those who are involved in this space. Ironically, the test for whether Coase was right (and, I repeat, by default, he is) lies in the reason given by those who choose cryptographic stigmergy as a method of organizing economic activity over joining a firm, when both are equally feasible.

Coase then proffers his favored and famous explanation. An organization within a firm is preferred when there is a cost of using the price mechanism. These costs, that have since been immortalized as transactions costs, are those of actually discovering what the relevant prices are and the costs of contracting with a variety of different entities that would have been involved in a purely price-directed production process. The firm stands in as a proxy for all those contracts that otherwise must be written, and, in exchange for this convenience, a factor of production volunteers to be directed by an entrepreneur within its boundaries. To these two costs he added a third: The distortionary costs of regulation that favor 'alternative methods of organization in a specialized exchange economy.

3.

Several advances in contract theory in the preceding 80 years have served to formally restate and model what Coase intuited in his article on why it is that the price mechanism constitutes a relative disadvantage to the firm. Kernels of the ideas on asymmetric information, differences in risk preferences, holdup and contractual incompleteness, at the very least, are all to be found in his article.

Nothing dares alter Coasian logic, but the space of cryptographic stigmergy does add nuance to his argument. Indeed, there remains a cost of price discovery associated with the market, and, indeed, the rationale for a firm based on this fact and others also remains. However, the blockchain technology has certain key features that inarguably change the game.

Blockchain technology is usually defined as a cryptographically-secure decentralized ledger that serves as a consensus mechanism based on protocols that require acquiring costly stakes in the system. There are, however, some additional key features that enable it to stand as the mechanism for cryptographic stigmergy. Some of these make it closer in essence to the price mechanism, though others make it seem more akin to a firm; this combination of features makes it all the more evident that the cryptographic stigmergy defines a space for coordinated production in between those of the price mechanism and the firm.

First among these is that the technology chains blocks of verified transactions ad infinitum, in the process giving it an infinite memory. In this respect, the blockchain holds the potential for providing more informative signals as the basis for transactions than can price, since price is memoryless for the purposes of organization. This feature distinguishes it from the price mechanism, but it also distinguishes it, albeit to a lesser degree, from the Coasian firm. The latter, admittedly, exists by virtue of a preference for longer-term contracts, but also requires unquestioning direction by the entrepreneur within some unspecified, vague 'limits'.

A second key feature, more in line with a market guided solely by the price-mechanism, is that the blockchain is essentially open access. Participation in a market remains far more open than does any current reification of blockchain technology, or indeed any that is likely to occur in the foreseeable future. However, the blockchain provides a wide spread in this respect: It can be adopted by firms for enterprise applications; by pools of firms for collaboration and retained as the basis for broad decentralized collaboration over new ideas.

A third feature of the blockchain is perhaps one that is easy to overlook. It is simply that the blockchain is portable. Blockchains compactify transactions very effectively.

For the purposes of organization this is not an insignificant benefit, especially when we consider that a frequent problem that is cited as being of crucial importance is the prohibitive cost of contractual specificity. A key feature of the environment that enables cryptographic stigmergy is that its technology provides a compact signal in the present that carries with it valuable information on the past.

The final feature is particularly interesting and enables the previous three to function. The costs that motivate organization of economic activity in market-based transacting are ameliorated, if not entirely suspended, within the boundaries of a firm. The blockchain, however, does not suspend their impact. Instead, it seeks to expressly internalize at least some part of the transactions costs to increase its overall value. The cryptographic nature of the stigmergy involved in the blockchain is in large part that the costs of verifying transactions are internalized to the members of its specialized exchange economy, with a view to enhancing overall stability. Coase's message was that the existence of transactions costs justifies alternate methods of organization. Blockchains take this message more keenly than do firms; they do not seek to avoid them, but instead try to leverage them to make alternate methods of organization less appealing.

4.

The cryptographic stigmergy holds the potential to fundamentally alter the boundaries of the Coasian firm, as well as lift some of the burden of organization off the price mechanism. It does not, however, usher in a revolution of the nature that would serve to invalidate Coase (1937).

A blockchain does not obviate the need for the price mechanism; indeed, the price mechanism remains the superstructure that permits coordination across the cryptographic stigmergic space. A blockchain does not obviate the need for the Coasian firm either. Because they are fully state-dependent and tractable, blockchains can operationalize smart contracts effectively, and possibly even a wider variety of complete contracts. They cannot, however, operationalize all contracts, especially the incomplete contracts that firms, as well as informal transactional relationships, routinely contend with. Such transactions are organized in an environment that is marked by ambiguity arising from an incomplete mapping across the states that it occupies, and, consequently, the prospect of renegotiation and reliance on third-party arbitration.

Coase does, however, give us a glimpse for what we might expect to see when Coasian firms attempt to coexist with the cryptographic stigmergy. Firms, he reminds us, should be expected to become larger as the costs of organization rise more slowly in the number of transactions they conduct. Technologies, significantly those that are rooted in Moore's Law and Metcalfe's Law, are enabling this dynamic for a number of modern firms well beyond the rudimentary telecommunication revolution that Coase based his observations on then. Yet, he arguably presaged platform economies when he remarked that '(i)nventions which tend to bring factors of production nearer together, by lessening spatial distribution, tend to increase the size of the firm.' Generally, his logic suggests a simple rule of thumb. If the costs incurred by a blockchain application to take over all of a firm's activities are higher than those incurred by the firm, the blockchain application would subsume the firm only if it can replicate all of what the firm does at a cost that is lower than the cost incurred by the firm, by at least as much as it would cost the blockchain to rely on the price mechanism. This latter cost can be substantial, possibly even prohibitively so, if incomplete contracts are simply not amenable to tractable blockchain application. So, if it is cheaper for a blockchain application to farm out some of its activities to the price mechanism or to firms, then we should be left with a situation where activities are divided across the three organizational mechanisms on an equi-marginal basis.

References

Coase, R. (1937). The Nature of the Firm. Economica, 4(16), new series, 386-405


Photo by Patrick Hendry on Unsplash

CRITICAL REVIEW

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(6)2018

Utility of the Blockchain for Climate Mitigation

Delton B. Chen Ph.D[1]
Center for Regenerative Community Solutions, New Jersey, USA
Correspondence: deltonchen@crcsolutions.org
Received: 25 March 2018 **Accepted:** 23 April 2018 **Published:** 26 April 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
DC [1] acknowledges project management support of the Center for Regenerative Community Solutions, advice provided by EconoVision and the help of volunteers.

Abstract

The blockchain is the enigmatic technology that gave birth to Bitcoin and the cryptocurrency movement. By fate or by good fortune, carbon markets and cryptocurrencies face common problems: a need to find consensus on data, and a need to trade value between distrustful strangers. Could the blockchain ledger enable a consensus on carbon budgets, and deliver value for carbon mitigation services? Could blockchain technologies help to resolve the climate crisis? To answer these questions, we need to examine the opportunities for decentralized ledgers in carbon and energy markets. Here we show that the blockchain offers a unique opportunity to improve accountability in carbon markets and to develop renewable energy micro-grids, but for the blockchain to reach its full potential—to be the game changer—it should be combined with macro-economic policies and macro-prudential regulatory frameworks that can finance a multi-trillion-dollar transition.

Keywords: *Blockchain, cryptocurrency, climate change, mitigation, carbon offset, carbon credit, decentralised ledger, central bank, macro-economic, macro-prudential*

1. Introduction

1.1 Blockchain Ledger

Since the genesis of Bitcoin (BTC) in January 2009, cryptocurrency trading has grown into a global market that consistently trades US$10 to 40 billion-equivalent per day (based on data from [1] for February to March, 2018). Bitcoin and other cryptocurrencies have been popularized for their ability to provide peer-to-peer financial transactions without a bank. Underpinning these cryptocurrencies is the blockchain distributed ledger technology (DLT). In simple terms, the blockchain refers to a digital ledger for people who wish to share and agree on the same information, but who don't want to rely on a centralised authority.

The blockchain ledger relies on a consensus mechanism to address a logical problem called the Byzantine Generals Problem [2] that involves sharing information amongst untrusting actors. The main developer of the blockchain ledger, Satoshi Nakamoto, designed a proof-of-work solution that is Byzantine Fault Tolerant (BFT) [3] [4]. In practice, the likelihood that bad actors could collude to undermine the blockchain ledger is believed negligibly small, and so the ledger and the data it contains are often described as 'immutable'.

Enterprise solutions that are based on blockchain DLTs are attractive to consumers, businesses and institutions because DLTs offer a way to achieve data consensus and accountability across entire operations. The potential advantages of DLTs include reduced administrative costs, reduced fraud and improved data tracking: allowing enterprises to operate more reliably and allowing managers to make informed decisions. One such example is the Australian Securities Exchange (ASX), which is replacing its Clearing House Electronic Subregister System (CHESS) with a new blockchain registry that will operate over a permissioned network [5].

Open-source blockchain standards are being developed to assist and accelerate the mass adoption of blockchain solutions—such as smart contracts that are interoperable with devices and other financial systems. These standards are being developed by various groups, including the Enterprise Ethereum Alliance and the Hyperledger Project.

1.2 Energy Demand of Distributed Ledgers

A well-known feature of the Bitcoin network is that its proof-of-work solution forces a deliberate use of computer processing to solve an encrypted puzzle, and this is to coordinate consensus amongst computers, to generate new Bitcoins, and to secure the network. This deliberate computer processing creates significant demand for electricity. As of January 2018, the digital mining of Bitcoins consumed more electricity than Portugal (49.8 TWh/yr), and the demand for electricity is rising [6].

Although the electricity consumption of the Bitcoin network is substantial, we should also consider that the Internet consumed 200-300 TWh of electricity in 2017 [7]—and this demand for electricity is also rising steadily. To put this into a broader perspective, the Internet is now comparable to aviation as a source of carbon emissions [8]. This is a stark reminder that the digital economy involves a trade-off with the environment. Driving this trend in energy use is a massive amount of new data being created by new digital devices.

Newer versions of the blockchain consensus mechanism are being developed in an attempt to reduce computer processing and electricity consumption by public DLTs, and one candidate is a proof-of-stake solution. Whatever solutions are adopted for public DLTs, the key challenge is to find an efficient consensus mechanism that can control the scarcity of a cryptocurrency when cryptocurrency mining is needed to finance the network.

The electricity demand of the blockchain consensus mechanism is much less of an issue for commercial solutions that operate on permissioned private networks. For example, Microsoft's Coco Framework replaces the proof-of-work of the Ethereum consortium network with 'trusted enclaves', greatly reducing latency and electricity demand. The Coco Framework also addresses other enterprise issues, such as scalability, data confidentiality and consortium governance. Coco illustrates the great administrative potential of blockchain DLTs over permissioned networks.

1.3 The Climate Crisis

Human activities are having a negative impact on the planetary ecosystem, and the climate is especially sensitive to man-made greenhouse gases. The negative consequences of climate change include angry weather, acidic oceans, and rising sea levels [9]. A major risk to the whole climate system is that the Arctic's ice structure is destabilizing with rapid ice melt, warming of seawater, and the mixing of cold Arctic air with warm air from southern latitudes. The Arctic is susceptible to warming feedbacks, including falling albedo with lost sea ice and the release of soil carbon to the atmosphere when permafrost thaws [10]. In February of 2018, daily temperatures in the Arctic remained 20°C above the average for longer than a week [11]—which illustrates the dramatic rate of change.

The climate crisis is created by a market failure in carbon emissions, and it persists as a failure to introduce carbon pricing to stay below 1.5 to 2.0°C of global warming. These temperature change limits—1.5 to 2.0°C—are the ambition of the 2015 Paris Climate Agreement [13], and they are recommended to limit the risks and the impacts of climate change. These limits are needed because ecosystems and civilization are highly sensitive to changes in average surface temperature. For example, most of the world's coral reefs are expected to be 'bleached' dead by +2.0°C of global warming [14]. Professor Veerabhadran Ramanathan, an expert in climate science at the University of California University, warned that climate change could even pose an existential risk to humanity [12].

Nations are working to reduce the carbon intensity of their Gross Domestic Product (GDP), but the 'elephant in the room' is economic growth. Economic growth, as measured by total GDP, increases demand for fossil energy and so growth drives greater carbon emissions [15]. Total GDP grew at an impressive 3.7% in 2017 [16], and records show that GDP has been growing at roughly 2 to 5% p.a. since the end of World War II [17]. Adrian Raftery and his colleagues undertook a trend analysis that takes into account economic growth, and they found that our chances of staying under 2.0°C are slim, with only a 5-in-100 likelihood of success [15]. Global warming this century is currently headed towards about 3.2°C by 2100, and there is a 5% chance of exceeding 4.9°C, which implies a significant risk of catastrophic climate change [15].

The neoclassical response to climate change is to implement an ideal carbon tax, which is defined by maximum welfare: the point where the tax balances the avoided damages. Some economists advocate hedging against the systemic risks of climate change by further increasing carbon taxes [21] above the ideal tax, and by adjusting investment decisions [20]. To realize the 2015 Paris ambition, the carbon tax would need to be implemented globally, and would need to rise higher than the ideal carbon tax. The High-Level Commission on Carbon Prices—chaired by Joseph Stieglitz and Nicholas Stern—estimates that this higher carbon tax rate would be at least US$40–80 per tonne of CO2 by 2020, and US$50–100 per tonne of CO2 by 2030 [22]. Professor William Nordhaus, a climate economist at Yale University, wrote in 2016 that staying below 2.5°C would require a new global policy [18]. There is clearly a need to introduce stronger carbon pricing into the world economy.

2. Emerging Blockchain Solutions

According to the UNFCCC, blockchain technologies can help address the climate crisis by improving accountability, transparency and efficiency of the following [23]:

1. Carbon stock-taking for low-carbon projects and the Nationally Determined Contributions (NDCs) of parties to the 2015 Paris Climate Agreement;
2. Carbon offset trading in carbon markets in relation to legal compliance and voluntary offsetting;
3. Peer-to-peer energy trading in decentralized clean energy markets; and
4. Climate finance in terms of old and new business practices.

Another potential blockchain application, which has yet to be widely discussed or addressed, is:

5. the delivery of scalable climate finance for the macro-economic and macro-prudential management of the low-carbon transition.

The success of the 2015 Paris Climate Agreement will depend on functioning carbon and energy markets—but there are caveats. The main caveat is that marginal improvements in markets will not solve the climate crisis. A major problem is that global energy demand will grow with projected economic growth (refer Section 1.2) and so new economic policies will be needed to limit global fossil fuel consumption and global carbon emissions. To put some meat on the bones of this discussion, we will discuss the above five applications by giving some examples.

2.1. Carbon Stocktaking

A curious feature of carbon markets is that the carbon is often portrayed as a commodity. The carbon that is abated from industry or sequestered into forests is not a commodity, because this carbon is not physically transported between buyers and sellers. Carbon markets are mostly trading services, and the service is recorded as a carbon offset/credit. A single carbon offset represents the service of preventing one metric tonne of carbon dioxide equivalent (CO2-e) from entering the atmosphere.

Low-carbon projects receive carbon offsets/credits as revenue for reducing carbon emissions or for sequestering carbon. The carbon amounts should be measured, reported and verified, and then monitored in case of leakage. These administrative processes are vulnerable to freeriding. For example, in 2015 researchers at the Stockholm Environment Institute found that a staggering 0.6 billion metric tonnes of CO2-e was misallocated under the Kyoto Protocol [24]. Interpol has reported on how cartels have exploited the carbon market with fraud and tax evasion scams [25]. Carbon sequestration projects based on forest management face unique technical and political challenges along their supply chain, and indigenous communities who depend on forests for their livelihood are often vulnerable to exploitation and human rights abuses [26].

The diamond trade offers an example of how blockchain technologies could be used to improve accountability. De Beers—the world's largest diamond producer—is inviting traders to register their diamonds on a blockchain ledger to record each diamond's authenticity and ethical origins. The approach requires data verification at each point in the supply chain. A blockchain ledger for carbon stocktaking will similarly require that supply chain is monitored and recorded. IBM is currently working on a blockchain enterprise solution with Energy-Blockchain Labs, and their aim is to streamline China's carbon market. In theory, a similar approach could be used to record the carbon stock take of entire nations—helping to deliver on the Paris Climate Agreement.

2.2. Carbon Offset Trading

The compliance market for carbon emissions is dogged by carbon caps below the ambition of the Paris Agreement, and by carbon prices below the social cost of carbon. More stringent laws are needed to raise carbon prices and to reduce carbon emissions. The European Commission has a legislative proposal to tighten the EU emissions trading scheme after 2020 [27], and other governments may follow their lead.

The public may buy carbon offsets in the voluntary carbon market. An online carbon trade exchange developed by CTX (ctxglobal.com) is helpful by ensuring that voluntary purchases are hassle free but selling carbon offsets to the public is like trying to convince the public to voluntarily pay higher taxes. Currently the voluntary carbon market is over-supplied by carbon offsets for this reason.

Some blockchain innovations are occurring in carbon offset markets. One example is Climate Coin Foundation, who plan to use a cryptocurrency—called Climate Coin—to crowd-fund a new platform that will represent carbon offsets with tradable tokens. Another example is a group called Nori, who plan to issue tokens for carbon that will be removed from the atmosphere. No doubt other start-ups will innovate in this space, but their success will depend on a rising price for carbon offsets over the coming years and decades.

2.3. Electricity Markets

The decentralization of electricity supply could be one of the most disruptive outcomes of a low-carbon transition. To reduce carbon emissions, commercial and residential consumers may prefer to buy their electricity from renewable sources using the town grid or a local micro-grid. Blockchain ledgers can be used to manage the decentralized power sharing, battery storage, feed-in tariffs, and other financial incentives on these grids. Three examples are (1) LO3 Energy's project called Brooklyn Microgrid; (2) Power Ledger's platform for monetizing surplus energy; and (3) TenneT's pilot home energy network. Solara is a start-up that will integrate data encryption technology directly into solar PV hardware, and this will improve the reliability of data. This list is by no means exhaustive, and other blockchain applications will likely emerge, especially when electric vehicles put greater demand on the electricity grid as they replace the existing fleet of petrol and diesel vehicles.

2.4. Green Token Finance

Green public tokens (cryptocurrencies) are part of a grassroots environmental movement, and they are traded in a living laboratory of people who share common interests. The aim is to crowd fund a project, or to increase trade in a green token. Some examples are Carbon Coin (carboncoin.cc) and Solar Coin (solarcoin.org). Carbon Coin may be supporting a forestry project but its governance is opaque. Solar Coin is issued to citizens who generate electricity with solar PV. These green tokens are promoted with a climate-related mission statement, but the tokens' supply and price are not coupled to carbon metrics, and so it is unclear if they actually help to reduce carbon emissions. Official economic policies may be needed to give green tokens their long-term price stability and environmental purpose. Green public tokens are evidently a nascent innovation that could be better designed to provide more transparency, accountability and tangible results.

2.5. The New Economy

The economy is expected to more than double in size between now and 2050 [28], and if this growth is unmanaged and dirty, then it will add significant new demand for coal, oil and natural gas [29]. Dirty growth is a continuation of the growth pattern that began in the 1950's—a pattern that Professor Will Steffen and his colleagues call 'the great acceleration' [30]. Professor Tim Jackson, at Surry University, is adamant that that a new macro-economic policy is needed to provide sustainable growth over the long-term [31].

What kind of macro-economic policy do we need to address the climate crisis? On one hand, there are conventional fiscal policies, such as carbon taxes and cap-and-trade— 'sticks'—and on the other hand there are unconventional green funds, green quantitative easing (QE) and green bond purchases— 'carrots'. It is the author's own opinion that a complete carrot-and-stick approach is missing, and that central banks should be involved in a global program of providing monetary stimulus to fill the policy void with scalable climate finance.

A recent report shows that central banks have accumulated about US$20 trillion in total assets [32]. This is a significant portion of global wealth, and it suggests that central banks have the capacity to purchase a significant amount of carbon offsets in the voluntary market but missing is a clear mandate for central banks to finance such purchases. New central bank monetary policies could be developed to create more demand for carbon offsets, and these policies should also be used to encourage the private sector to invest in low-carbon projects [33].

To fill the central bank policy void, a Central Bank Digital Currency (CBDC) could be developed, so that the central banks can price climate risk into the global financial system by trading the CBDC with national fiat currencies [33]. Such a CBDC could be developed using distributed ledger technologies (DLT) and permissioned networks between central banks. Central banks were quick to utilize the blockchain to develop CBDCs for inter-banking trade [34], and two examples are Project Ubin [35] and Utility Settlement Coin [36].

With regards to climate risk, the Financial Stability Board for the G20 is conversing with financial industries [37], central banks, and the insurance industry [38]. In April 2018, eight central banks will be meeting in Amsterdam to discuss climate related risk [39]. These activities suggest that central banks are indeed looking for new policies to manage climate risk.

With the right policies, central banks could shape the low-carbon transition by providing macro-prudential governance of climate risk [33]. Such governance should be preemptive because a failure to act preemptively has irreversible long-term consequences. The Fukushima Daiichi nuclear disaster—triggered by a tsunami on 11 March 2011—is a painful reminder of why risk management is important. According to a Bloomberg report [40], the power plant operators, TEPCO, did not respond to a risk assessment concerning extreme tsunami wave heights and advice on emergency power. The take-home message is that certain risks need to be managed preventatively, and the cost of this prevention is analogous to an insurance premium.

3. Conclusion

The blockchain is a technology that can help establish consensus within society over information and value, and it will likely play an important role in improving the accountability and transparency of carbon markets and energy markets. It is advised here that the blockchain technology is simply not enough to deliver on the ambitions of the 2015 Paris Climate Agreement, and new macro-economic and macro-prudential policies are also needed to manage the economy for rapid decarbonization—at the rate needed to achieve the Paris Agreement. There is a window-of-opportunity for experts in various fields—including central bankers, economists, policy makers, lawyers, scientists and blockchain developers—to collaborate on the solutions for the New Economy.

Humanity has accumulated incredible technical knowledge since the start of the Industrial Age, but the silo effect of people working in their specialized fields poses a problem. Addressing the climate crisis will require new inter-disciplinary collaborations, because a new economy will need a toolbox of radical policies and reliable financial tools that can manage the low-carbon transition.

References

[1] *[Accessed 20 March 2018] https://coinmarketcap.com/*

[2] *Lamport, L., R. Shostak and M. Pease, (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4 (3): 382-401*

[3] *Nakamoto, S. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 5 March 2014. Released 24 May, 2009, Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf.*

[4] *Nakamoto, S. (2008). Private email. The Mail Archive. Thu, 13 Nov 2008 [Accessed 20 March 2018] https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html*

[5] *[Accessed 20 March 2018] http://fortune.com/2017/12/07/blockchain-technology-australian-securities-exchange-asx/*

[6] *Bitcoin Energy Consumption Index (2018). [Accessed 20 March 2018] https://digiconomist.net/bitcoin-energy-consumption*

[7] *The Guardian (2017) 'Tsunami of data' could consume one fifth of global electricity by 2025. Guardian Environment Network. [Accessed 20 March 2018] https://www.theguardian.com/environment/2017/dec/11/tsunami-of-data-could-consume-fifth-global-electricity-by-2025*

[8] *[Accessed 20 March 2018] https://www.theguardian.com/environment/2015/sep/25/server-data-centre-emissions-air-travel-web-google-facebook-greenhouse-gas*

[9] *Hansen, J., Sato, M., Hearty, P., Ruedy, R., Kelley, M., Masson-Delmotte, V., Russell, G., et al. (2016). Ice melt, sea level rise and superstorms: evidence from paleoclimate data, climate modeling, and modern observations that 2 °C global warming could be dangerous. Atmos. Chem. Phys., 16: 3761-3812.*

[10] *Schuur, E. A., McGuire, A. D., Schädel, C., Grosse,G., Harden, J. W., Hayes, D. J., Hugelius, G., Koven, C. D., et al. (2015) . Climate change and the permafrost carbon feedback. Nature, 520 (7546): 171-179.*

[11] *Watts, J. (2018). Arctic warming: scientists alarmed by 'crazy' temperature rises. The Guardian, 28 February 2018. [Accessed 20 March 2018] https://www.theguardian.com/environment/2018/feb/27/arctic-warming-scientists-alarmed-by-crazy-temperature-rises*

[12] *Xu, Y., and Ramanathan, V. (2017). Well below 2 °C: Mitigation strategies for avoiding dangerous to catastrophic climate changes. PNAS, 114 (39): 10315-10323.*

[13] *UNFCCC, 2015. Adoption of the Paris Agreement, 21st Conference of the Parties, Paris: United Nations. Report No. FCCC/CP/2015/L.9/Rev.1 [Accessed 12 September 2017] http://unfccc.int/resource/docs/2015/cop21/eng/l09r01.pdf.*

[14] *European Geosciences Union. (2016, April 21). 1.5 C vs 2 C global warming: New study shows why half a degree matters. ScienceDaily. [Accessed March 25, 2018] www.sciencedaily.com/releases/2016/04/160421085218.htm*

[15] *Raftery, A.E., Zimmer, A., Frierson, D.M., Startz, R. and Liu, P., 2017. Less than 2°C warming by 2100 unlikely. Nature Climate Change (31 July 2017)*

[16] *IMF (2018) World Economic Outlook Update, January 2018 [Accessed 11 January 2018] https://www.imf.org/en/Publications/WEO/Issues/2018/01/11/world-economic-outlook-update-january-2018*

[17] *World Bank (2018). GDP growth (annual %). World Bank national accounts data, and OECD National Accounts data files. [Accessed 20 March 2018]*

https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG

[18] Nordhaus, W. D., 2016. 'Projections and uncertainties about climate change in an era of minimal climate policies', Cowels Foundation Discussion Paper No. 2057. New Haven, CT: Yale University.

[19] Aglietta, M., & Espagne, E., 2016. 'Climate and Finance Systemic Risks, More Than an Analogy? The Climate Fragility Hypothesis', Working Paper CEPII, No 2016-10 – April, pp. 30.

[20] Dietz, S., C. Gollier, and L. Kessler, 2018. The climate beta. Journal of Environmental Economics and Management, 87: 258-274.

[21] Weitzman, M.L. (2010). "Risk-adjusted gamma discounting." Journal of Environmental Economics and Management 60(1): 1–13.

[22] High-Level Commission on Carbon Prices (2017). Report of the High-Level Commission on Carbon Prices. Washington, DC: World Bank.

[23] [Accessed 20 March 2018] http://newsroom.unfccc.int/climate-action/how-blockchain-technology-could-boost-climate-action/

[24] [Accessed 20 March 2018] https://www.sei-international.org/sei-in-the-media/3207-kyoto-protocols-carbon-credit-scheme-increased-emissions-by-600m-tonnes

[25] [Accessed 20 March 2018] https://www.interpol.int/Media/Files/Crime-areas/Environmental-crime/Guide-to-Carbon-Trading-Crime-2013

[26] [Accessed 20 March 2018] http://www.redd-monitor.org/2018/01/25/human-rights-and-environmental-organisations-urge-finland-to-stop-funding-the-kenya-forest-service-following-human-rights-abuses-of-indigenous-sengwer-people/

[27] [Accessed 20 March 2018] http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/595926/EPRS_BRI(2017)595926_EN.pdf

[28] [Accessed 20 March 2018] https://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html

[29] [Accessed 20 March 2018] http://news.exxonmobil.com/press-release/exxonmobil-releases-energy-carbon-summary-and-outlook-energy

[30] [Accessed 20 March 2018] http://journals.sagepub.com/doi/abs/10.1177/2053019614564785?journalCode=anra

[31] Jackson, T. (2017). Prosperity Without Growth - Foundations for the Economy of Tomorrow. London: Routledge.

[32] [Accessed 20 March 2018] https://www.zerohedge.com/news/2018-03-13/last-breakout

[33] Chen, D. B. (in press). Central Banks and Blockchains: The Case for Managing Climate Risk with a Positive Carbon Price. In: Transforming climate finance and green investment with blockchains. Elsevier. Alastair Marke, Ed., Chapter 9.

[34] Grym, A., Heikkinen, P., Kauko, K., and Takala, K. (2017). Central bank digital currency. Bank of Finland, BoF Economics Review, May 2017, (p.10).

[35] MAS, 2017. 'The future is here | Project Ubin: SGD on Distributed Ledger', Monetary Authority of Singapore, Deloitte, pp. 44.
[Accessed 25 August 2017] http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial- Centre/Project-Ubin.aspx

[36] [Accessed 20 March 2018] https://www.coindesk.com/hsbc-barclays-join-utility-settlement-coin-as-bank-blockchain-test-enters-final-phase/

[37] [Accessed 20 March 2018] https://www.fsb-tcfd.org/

[38] University of Cambridge Institute for Sustainability Leadership (CISL). (2017). Insurable cities: The ClimateWise Principles Independent Review 2017. Cambridge, UK: Cambridge Institute for Sustainability Leadership.
[Accessed 20 March 2018] https://www.cisl.cam.ac.uk/business-action/sustainable-finance/climatewise/principles

[39] [Accessed 20 March 2018] http://www.straitstimes.com/business/banking/mas-7-other-central-banks-form-green-focused-network

[40] [Accessed 20 March 2018] https://www.bloomberg.co.jp/news/articles/2011-03-16/LI467Z07SXKY01

Photo by rawpixel on Unsplash

ESSAY

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(6)2018

Why do we need Tokenomics?

Stylianos Kampakis[1] PhD
University College London, Centre for Blockchain Technologies, UK
Correspondence: stylianos.kampakis@gmail.com
Received: 28 April 2018 **Accepted:** 1 March 2018 **Published:** 2 March 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
SK [1] prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Not declared.

Abstract

Initial Coin Offerings (ICOs) have revolutionised the way startups are funded. Furthermore, besides their use in an ICO, tokens unlock many possibilities within the context of the artificial economies that are being set up through blockchain: from incentivisation to automatic balancing of the economy. In spite of these developments, there is still no commonly accepted theoretical framework for analysing token economies and ICOs. This presents a unique challenge to the scientific community.

Keywords: *: ico, initial coin offerings, ICOs, token economy, tokenomics*

1. A different landscape

A long time has passed since 1776, when Adam Smith defined political economy in his monumental work "The Wealth of Nations". Since then economics as a scientific discipline has gone a long way with different schools of thought having shaped policy, public administration and society. However, up until now, there was one common assumptions behind all schools of thought: money is the default medium of exchange for goods and services.

However, Adam Smith, John Maynard Keynes and Milton Friedmand would find themselves in a completely different world now. Blockchain technology has allowed the development of the Initial Coin Offering and as of writing there is more than $5.6 billion that has been raised by ICOs1. Each start-up that runs an ICO is unique. However, there is one thing common between all ICOs. This is the use of a token as a currency.

There are three different kinds of tokens:

1) Equity tokens
2) Security tokens
3) Utility tokens

Equity tokens and security tokens are simply an extension of the concept of share or asset-ownership to the blockchain. However, it is utility tokens that offer a completely new proposition.
Utility tokens are tokens that are simply redeemable within a start-up's closed economy and are exchanged for goods and services. And this is where we observe the first major difference to what economics as a discipline has dealt with since its inception.

2. Some examples

The use of blockchain-based tokens allows the creation of new kinds of economies, completely customisable and adaptive, while at the same time ensuring security and transparency without a central authority. There are many possibilities, and in this article, we are going to see three different examples:

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

Some use cases are going to be presented here.

2.1 Improved incentivisation schemes

Incentivising people to do something is never an easy task. In traditional economics, the assumption was that people act as rational economic agents. However, in the last few years economics have been greatly influenced by psychology and the work of people like the noble laureates Daniel Kahneman and Richard Thaler.
The work of Daniel Kahneman and Amos Tversky convinced us that humans are not always making decisions in a rational manner through their work in prospect theory 2. Their work demonstrated that in decisions that involve probabilities and uncertainty (which is the case for many real-world scenarios), humans tend to operate in a different way to what they would have done if they were rational agents.

Richard Thaler 3 extended some of the conclusions of this work to public policy making. In his popular book "Nudge", he explained how a government could use the cognitive biases that humans are using in decision making, in order to improve societal and economic outcomes.

Behavioural economics is a fascinating field, but the possibilities automatically increase when it is seen through the lens of blockchain technology. Through the use of tokens, it becomes possible to incentivise different agents through the production of tokens for particular actions.

For example, a user can be incentivised to purchase a product, or perform an action such as recycling. A company can be incentivised for compliance. Users can be incentivised for forming collective action. The possibilities are endless.

2.2 Automatic balancing of an economy

Economies go through cycles where inflation, deflation and other economic indicators fluctuate. Central banks have an indirect control over the economy through the use of interest rates, bonds and other means.

Token economies of a certain scale are not much different. However, there are two main advantages that blockchain offers:

1) Detailed data over transactions.
2) Automatic controls through the use of smart-contracts

What this means is that measures such as inflation can automatically be calculated on the spot. Safeguards against the economy, such as against speculative attacks or rapidly rising inflation, can be placed through smart contracts. Furthermore, because these measures are enforced through smart contracts, decision making is automated, transparent and available to the public. This can make token economies more robust, while also improving trust.

Indeed, a very interesting question is what would happen if central banks and governments were able to integrate blockchain within their current monetary systems.

3. So, why tokenomics?

So, to answer the original question posed in the beginning of the article: "why we need tokenomics"? It has become common knowledge that blockchain opens up many different possibilities. However, while tokens are a huge part of it, tokenomics is still a discipline that has not been studied in depth. A google scholar search for "token economy blockchain" returns only 1860 results.

Furthermore, the majority of ICO white papers are not using any kind of formal analysis of their economic model. For example, a model that has showed up in many ICOs, is the issuance of a limited number of tokens, which are gradually burnt as they are being used. This limits supply over time, which (if the demand is not reduced) will increase the price of the token.

While this might sound lucrative to the short-term investor, it does not explain how the model is sustainable in the long run. Indeed, ICOs is a new invention, so we don't have any examples of start-ups that followed this model and had sustainable growth for 5+ years.

However, a proper theory of token economies would allow us to understand which models work best and are sustainable. This would also help improve the credibility of ICOs as a method of raising money, calming criticism and concerns about speculative bubbles.

All this makes it clear that the vast possibilities opened up by formalising token economies is still unexplored. The science of economics has given us powerful insights into how the laws of real world economies work. What we, as the scientific blockchain community, need to do, is spend more time and resources in understanding how to transfer learnings from traditional economics into token economies and how to create new economic models and theories that exploit the possibilities offered by blockchain.

References

[1] http://uk.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1

[2] Tversky, Amos; Kahneman, Daniel (1992). "Advances in prospect theory: Cumulative representation of uncertainty". Journal of Risk and Uncertainty. 5 (4): 297–323. doi:10.1007/BF00122574. ISSN 0895-5646

[3] Thaler, Richard H., and Cass R. Sunstein. Nudge: Improving decisions about health, wealth, and happiness. New Haven, CT Yales University Press, 1999.

Photo by Toa Heftiba on Unsplash

FOR AUTHORS

The JBBA is an open access, externally peer reviewed, scientific journal devoted to Distributed Ledger Technologies, Blockchain Technology & Cryptocurrencies. The journal offers a wide ranging and comprehensive coverage of all facets of Blockchain technology and Distributed Ledger Ecosystems. We welcome manuscripts reporting Blockchain and DLT research projects, scientific methods, case studies, analysis, reviews and practical use cases of emerging distributed ledger technologies and new innovations including sound descriptive work. All submissions should be in English. The editor reserves the right to reject without review. Manuscript queries should be addressed to:

Editorial@thejbba.com

Open access policy:

The JBBA follows a fully open access policy for all articles published in the journal. Published articles can be disseminated freely and instantly to the widest possible audience, without barriers to access. Authors are free to reproduce and distribute their work at will, for example by placing it on their institution's website. This enables increase article citations and impact because of easier availability and results in enhanced literature searching.

The JBBA is published 4-6 times per year and will provide a forum for authors to share their knowledge, skills, experiences and creative work across a wide range of industries and technologies in which Blockchain is being deployed.

We will publish: (Max. word count = 5,000 words)

Original Scientific Research (Qualitative, Quantitative)
Randomised Control Trials
Systematic Reviews
Meta-analysis
Conference Research Abstracts
Comparative studies
Case Studies & Essays
Book Reviews
PhD/MSc thesis & Dissertations
Critical reviews and Analysis
Interviews/ Opinions of Key Influencers/ Thought Leaders
Editorial
Commentary on latest issues and trends in blockchain & DLT

We may also include selected mix of articles published on our website. Interviews/ opinions are not peer reviewed but all content must be approved by the handling editor to assess suitablility for publication. Should you wish to be interviewed by us, please email to:

Editorial@thejbba.com

Editor-in-chief has overall responsibility for the content, production and strategic direction of the JBBA.

The JBBA ISSN Number (Online): ISSN 2516-3957

The JBBA ISSN Number (Print): ISSN 2516-3949

Step-by-step guide to manuscript submission:

1. Author submits the article via JBBA Scholastica site
2. The article will undergo quick initial screening by the Managing/ Associate Editor-in-Chief. If they feel that the article is inappropriate for the journal for a reason that can be quickly ascertained, such as the subject matter being too far from the scope of the journal, the authors will normally be informed within 1-2 weeks of submission.
3. For all other submissions, we will first seek to gauge the level of interest that the paper will have, on the assumption that it is correct and well written. This will normally mean sending the paper out to the editor for "quick opinions", after which its suitability will be discussed by the Associate Editors-in-Chief.
4. The paper will then be sent for review. Post review, there are 3 possible outcomes:

- Accepted (will be allocated for publication)
- Rejected
- Revise and submit

5. You will be informed of the review outcome by the Managing Editor.
6. The final decision for all manuscripts is taken by the Editor-in-Chief. The handling editor will make a recommendation – sometimes a tentative one – and this will be discussed. In cases of doubt, more quick opinions will usually be sought.
7. Some stages of the above process may occasionally be bypassed if the content is so close to the expertise of one or more of the editors that extra external information is clearly not necessary for a fair decision to be made.

Article Processing Charge:

If your article is accepted for publication, we will ask you to pay the Article Processing Charge (APC) of **£585** (£485 for members of the British Blockchain Association). The APC covers the cost of administration, copy editing, formatting, layout, online hosting, archiving, digital object identifier, journal marketing, designing, print publication and print distribution. Article processing charges will enable full, immediate, and continued open access for all work published in the JBBA. This allows unrestricted access; to authors, through the widest possible dissemination of their work; and to the blockchain community in general, through facilitation of information availability and scientific advancement of distributed ledger technologies and allied disciplines.

Waiver policy:

We acknowledge that some authors may be suffering form financial hardships making it difficult for them to pay the APC. The JBBA offers full waiver to authors in **exceptional circumstances**, on request. No payment information is requested before an article is reviewed and accepted, so the ability to pay **do not** affect the editorial decisions at the JBBA. If you believe your request for an APC waiver should be considered on the grounds of exceptional financial circumstances, please write to the managing editor explaining your grounds for request. All such requests will be considered on a **case-by-case basis** by the Editorial Board.

We offer **full APC waiver** to authors that permanently reside in the following low-income countries:
Afghanistan, Benin, Burkina Faso, Burundi, Central African Republic, Chad, Comoros, Congo, Dem. Rep., Eritrea, Ethiopia, Gambia, Guinea, Guinea-Bissau, Haiti, Liberia, Madagascar, Malawi, Mali, Mozambique, Nepal, Niger, Rwanda, Senegal, Sierra Leone, Somalia, South Sudan, Tanzania, Togo, Uganda and Zimbabwe.

APC is waived for **full time students** pursuing a postgraduate degree from a recognised institution/ university in one of the following countries:

Guyana, Republic of Moldova ,Angola, Haiti , Rwanda, Bangladesh, Honduras, Samoa, Belize, Iraq, Sao Tome and Principe, Benin, Kiribati, Senegal, Bhutan, Kiribati, Seychelles, Bolivia (Plurinational State of), Kyrgyzstan, Sierra Leone, Burkina Faso, Lao People's Democratic Republic , Solomon Islands, Burundi, Lesotho, Somalia, Cabo Verde, Liberia, Cambodia, Madagascar, Sri Lanka, Cameroon, Malawi, St. Helena, Central African Republic , Malawi, Sudan, Chad, Mali, Suriname, Comoros, Marshall Islands, Swaziland, Comoros, Marshall Islands, Swaziland, Congo, Mauritania, Tajikistan, Cook Islands, Micronesia (Federated States of), Timor-Leste, Côte d'Ivoire, Mongolia, Togo, Democratic People's Republic of Korea, Morocco, Tokelau, Democratic Republic of Congo, Mozambique, Tonga, Djibouti, Myanmar, Turkmenistan, El Salvador, Namibia, Tuvalu, Equatorial Guinea, Nauru, Uganda, Eritrea, Nepal, United Republic of Tanzania, Ethiopia, Nicaragua, Uzbekistan, Fiji, Niger, Vanuatu, Gabon, Nigeria, Vietnam, Gambia, Niue, West Bank and Gaza Strip, Ghana, Palau, Yemen, Guatemala, Papua New Guinea, Zambia, Guinea, Refugee Camps (UNHCR) Zimbabwe and Guinea-Bissau.

Digital Archiving Policy:

All articles will be archived at the British Library and subsequently deposited at the Agency for the legal Deposit Libraries (ALDL), which acts on behalf of Bodleian Library Oxford University, the Cambridge University Library, National Library of Scotland, National Library of Wales and Trinity College Dublin.

Plagiarism Policy:

We have a very stringent plagiarism policy in place and all articles are screened on Turnitin for detection of plagiarism. This allows the highest possible level of scholarly integrity, transparency and rigorous quality control in contents published by the JBBA.

General Guidance for Authors:

The editors request that all articles shall be submitted via Scholasticahq portal and must include an abstract. We prefer text attachments in Microsoft Word, Times New Roman, font size 12, double spacing except for references at the end of the paper, which should be single space.

Please provide your name, title, post-nominal, full address, and e-mail in all correspondence. The JBBA does not publish the work that has been or will be published elsewhere. The text of accepted manuscripts can sometimes be edited to enhance communication between author and reader. Submission implies that the work is not being considered for publication elsewhere and that it has been approved by all authors. Original research articles should not exceed 10 A4 size pages (c. 750 words per page, excluding Tables and Figures).

Author names and contact information are provided during the submission process. The person who submits the paper via Scholastica is the corresponding author and an active email address is needed.) The first author or primary author is the person who conducted most of the work described in the paper, and is usually the person who drafted the manuscript. The "senior author " is usually the last person named, and is generally the one who directed or oversaw the project. The names of the "contributing authors" appear between the primary and senior authors, and the order should reflect their relative contribution to the work. By completing the submission, you automatically agree to the statement that the manuscript has not been published elsewhere and that it has not been submitted simultaneously for publication elsewhere. Authors who fail to adhere to this condition will be charged with all costs which JBBA incurs, and their papers will not be published.

Manuscripts should be structured as follows:

Title (short and concise, plus a proposal for a 'running head'), Names of authors, Addresses of authors, Abstract (max 300 words), Key words (max ten), Introduction, Methods, Results, Discussion, Acknowledgements, References, Tables, Figure captions, Figures and Supplemental Material. The abstract should reflect both content and emphasis of the paper. The introduction should be restricted to scope, purpose, and the rationale of the study. Limit the information on methods to what is essential to judge whether the findings are valid.

The link below provides useful instructions on how to write an academic/ scholarly article:

https://canvas.hull.ac.uk/courses/371/pages/academic-writing-style

References:

References in the text should be in order of publication, e.g. (Dawson & Grick 2005, Minton et al. 2007). In the reference list the literature cited should follow Vancouver style referencing i.e, in alphabetical order by the first word of the family name (e.g. van Eerden under V). Please refer to the following examples (not actual papers; for demo purposes only) of citation formats for journals, conferences, books, electronic media, and magazine & newspaper articles. Here is a guidance document on how to use Vancouver style referencing:
https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/library/public/vancouver.pdf

1. Journal Articles

Foster, M.K., "Supply chain management using public blockchains ", Journal of Operations Management, 26(1), 2012, 457–467.

2. Conference Articles

George, S., 'Effects of Quantum computing on Cryptographic Hash function', Proceedings of the third annual meeting of the International Society for Mathematics, Atlanta, Georgia, 2016, 44-49.

3. Books

Merkel, W. and Albright, T.C., Practical Management Science (2nd ed.), Brooks/Cole, Pacific Grove, CA, 2017.
Jones, D.J., Smith, F. and Watson, T.P. (eds), Artificial Intelligence Reconsidered (2nd ed.), Wiley, New York, 2013..

4. Electronic Media

Stephen, B.B., "Norms, models and identities on Blockchain," The Journal of Science Online, 20(10), 2016, **http://jalt-publications.org/tlt/files/75/oct/index.html.**

5. Magazine & Newspaper Articles

Henry, F.A., III., "Is blockchain the panacea for all?," Time, April 9, 2016, 28-31.

Listing sources of information at the end of a paper is an important part of professional scholarship and writing. It is highly suggested that all references should be checked if they are complete and there should be no missing or uncited references. The references should be listed in the alphabetic order of the last name of the first author. Refer to the author's last name and published year in the parenthesis, as in (Cox and King, 2006) except at the beginning of a sentence: "Cox and King (2006) demonstrated . . ." Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished". Papers that have been accepted for publication should be cited as "in press". Capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation.

**JBBA Publication Ethics & duties of the Authors, Reviewers, Editors and publishers: **

Duties of Editors

Articles will be evaluated exclusively on the basis of their Blockchain/ Distributed Ledger technologies/ Cryptocurrencies interest and their relevance to the scope of the journal.
Articles under consideration will be kept confidential: that is, it will not be disclosed to anyone other than those involved in the evaluation process and in the administration of the journal. Editors may submit their own papers to the journal, but if they do so, then all information about the processing of those papers will be hidden from their view and they will have no part in the decision process. Moreover, it is the policy of JBBA to set a slightly higher bar for acceptance for papers submitted by editorial board members.
Editors who have a significant conflict of interest

connected with a paper will declare it to the other editors and will avoid participating in the decision process.

Duties of Authors

Authors should submit original research work only (except if it this is clearly not the intention of the article – as might be the case, for example, with a survey paper, interview, analysis, commentary). Any results that are not due to the authors should be clearly cited. Copying or paraphrasing substantial parts of another paper without attribution is unacceptable, as is any other form of plagiarism.

No paper should be submitted to JBBA that is already published elsewhere or is being considered for publication by another journal.

Those named as authors of a paper should have made a substantial contribution to the paper, or to a more general project of which the paper is a part, and anybody who has made such a contribution should be offered authorship.

Authors who discover important errors in their articles, whether published or under consideration for publication, should notify the journal promptly.

Duties of Reviewers

Reviewers asked for quick opinions are expected to be objective and to provide them promptly. Should they have a conflict of interest, or should they lack the expertise to make a judgment with confidence, they should make this clear to the editors and should decline to review the paper.

More detailed manuscripts may take longer to review. For such papers an initial deadline will be set by the handling editor: if it is felt by the reviewer to be unrealistic, then he or she should agree an alternative with the editor. Since a paper that reaches this stage of the reviewing process will normally have been judged to be interesting enough to publish, the focus of the more detailed report should be the correctness of the paper and the quality of its writing. However, opinions about its quality and interest are also welcomed.

Reviewers are expected to keep confidential the information that the paper has been submitted to JBBA, except that if the paper is rejected and the reviewer receives it again to evaluate for another journal, then the information that the paper has been rejected by JBBA may be shared (confidentially) with the editorial board of the other journal.

In some cases, it is not reasonable to expect a reviewer to check the correctness of a paper down to the last detail. In such cases, editors may be satisfied with indirect evidence that a paper is likely to be correct. (For example, it may be that the general outline of the argument is convincing, but that the technical details involved in converting the outline into a complete proof are very complicated.) Thus, publication in JBBA should not be considered an absolute guarantee of correctness, just as in practice it is not a guarantee for any other journal. Readers who discover important errors in JBBA papers are strongly encouraged to report them to the journal: as stated above, if we are made aware of an error, we will add a prominent notification of the error to the editorial introduction to the paper.

If an author subsequently corrects an error and posts a revised version of the paper to the JBBA, the version of record of the paper will remain as the previously accepted version. However, a prominent link to the corrected version will be added to the editorial introduction.

JBBA does not normally copy-edit articles. We therefore ask our reviewers to point out minor errors such as spelling mistakes as well as more important mathematical slips. Should these be very numerous, then a more general statement to the effect that the paper should be thoroughly checked for small errors will be sufficient.

Authors who discover important errors in their articles, whether published or under consideration for publication, should notify the journal promptly.

Duties of the Publisher:

The JBBA is committed to the permanent availability and preservation of scholarly research and ensures accessibility by maintaining our own digital archive. Articles in JBBA are published under a Creative Commons CC-BY licence and will be free to read in perpetuity.

Journal Sponsors, Academic Partners and Advertisement

The JBBA welcomes academic sponsors/ partners and advertisements for the print edition. Please visit the British Blockchain Association website for more information

To advertise in the JBBA, please contact:

Email: Editorial@thejbba.com

Marketing & Communications Department
The JBBA
The British Blockchain Association
Kemp House 152 - 160 City Road
London, United Kingdom
EC1V 2NX