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

VOLUME 2 | ISSUE 2 | ISSN PRINT: 2516-3949
OCTOBER 2019

The British Blockchain Association
Advocating Evidence Based Blockchain

BUILDING QUANTUM RESISTANT BLOCKCHAINS

2nd Blockchain International Scientific Conference, 11 March 2020

ACADEMIC PARTNERS

Ulster University
SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
CEBB | Centre for Evidence-Based Blockchain
Edinburgh Napier UNIVERSITY
The Open University

The British Blockchain Association

Advocating Evidence Based Blockchain

2nd Blockchain International Scientific Conference

#ISC2020

11 March 2020 | Edinburgh Napier University

WHY ATTEND ISC 2020?

Network with some of the Most Eminent Blockchain Scholars

Meeting point Conference of Blockchain Industry & Academia

International Recognition of your work by Blockchain Scientific Community

Prizes for Best Abstract, Project & Oral Presentations

Connect with Enterprises & Institutions looking for Blockchain innovators

Publish your work in The JBBA

Pitch your ideas and research to Policy Makers and Enterpreneurs

CALL FOR PAPERS

Researchers, academicians, technologists, blockchain developers, policy makers and other stakeholders are welcome to submit their original research papers, pilot projects and case studies to ISC 2020

For more information visit

www.britishblockchainassociation.org

TABLE OF CONTENTS

CEBB | Centre for Evidence-Based Blockchain

FOUNDING MEMBERS

RMIT Blockchain Innovation Hub

The British Blockchain Association
Advocating Evidence Based Blockchain

Edinburgh Napier University

SUSS Singapore University of Social Sciences

uB Université de Bourgogne

The Open University

Ulster University

ABOUT CEBB

A neutral, decentralised, global coalition of leading Blockchain research institutions and academics

Setting benchmarks and frameworks to support governments, businesses and policymakers in making evidence-based decisions

A collective voice on the advancement of Evidence-Based standards in Blockchain and Distributed Ledgers

Academic "Think Tank" of thought leaders and researchers in Blockchain

Establishing internationally agreed standards on postgraduate Blockchain education curriculum

Support organisations in setting up their own local EBB chapter with support from CEBB

Promotion of research, call for papers and dissemination of scholarly content within the CEBB network

Facilitate joint initiatives, workshops, journal clubs, and other academic activities with CEBB members

Collaboration in projects, case studies, applied and theoretical research to avoid duplication and streamline resources

Exclusive, close-knit networking opportunities and connection with peers to build evidence-based guidelines for stakeholder organisations

---

JOIN CEBB

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

DISCLAIMER

Publication in this journal of scientific, technical and literary material is open to all authors and readers. While every effort has been made to ensure articles published are free from typing, proof reading and formatting errors at the time of going to press, the publisher will be glad to be notified of any errors or omissions brought to our attention after the journal is published in the print format. Articles should not be taken to represent the policy or opinion of the British Blockchain Association, unless this is specifically stated. The publisher, affiliates of the British Blockchain Association, reviewers and editors assume no responsibility for any claims, instructions, methods or recommendations contained in the manuscripts. This publication is not a substitute for professional advice. The contents herein are correct at the time of printing and may be subject to change.

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

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

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

DOAJ DIRECTORY OF OPEN ACCESS JOURNALS Google Scholar

Articles are indexed in **Semantic Scholar, Microsoft Academic** and available at online repositories at some of the most prestigious Universities, worldwide.

The British Blockchain Association is a Publisher Member of Portico, CrossRef and CPDUK

Crossref CPD MEMBER The CPD Certification Service PORTICO

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

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

Online publication:
The articles published in this issue can be viewed Open Access on the JBBA website: 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.

The JBBA is a publisher member of Reviewer Credit

REVIEWER CREDITS Registered Journal

Distribution

Print copies of the journal are sent worldwide to selected university libraries, policymakers, government officials, fin-tech organisations, eminent scholars, and major conferences. To request a print copy, please visit the journal website for more details.

Photo by Annie Spratt on Unsplash

EDITORIAL

As an Associate Editor-in-Chief of The JBBA, it gives me great pleasure to author the editorial of the 4th Issue of the journal. The papers that were accepted for publication in this issue are the following:

'The Contractual Cryptoeconomy: An Arrow of Time for Economics', by Prateek Goorha
'Cryptocurrency Investing Examined', by Prof Jim Kyung-Soo Liew, Ph.D. of The Johns Hopkins University
'Singapore's Open Digital Token Offering Embrace: Context & Consequences', by Prof David Lee of Stanford University and Robert Greene of Singapore University of Social Sciences (SUSS)
'A Blockchain Infrastructure for Transportation in Low Income Country Cities, and Beyond' by Simon Herko
'Blockchain Investigations - Beyond the 'Money', by Simon Dyson of NHS Digital
'A Review of fast-growing Blockchain Hubs in Asia' By Caroline Lim of SUSS, and
'Transitioning to a Hyperledger Fabric Quantum-Resistant Classical Hybrid Public Key Infrastructure' by Rob Campbell of Capitol Technology University

These research papers combine a savant blend of exploratory skills, intellectual curiosity, innovative thinking and scientific rigour. In this sense, we are delighted to publish cutting-edge research that lies at the deeper level of investigative science, beyond mere surface phenomena and the often decried hype, to outline and demonstrate the true benefits of this revolutionary technology for the industry and society at large. The journal has become a global platform for academics and scientists, who wish to work together constructively and make decisions based on the best available evidence.

The selection process for these publications has systematically relied on evidence-based practices and double-blind peer-review. Subject matter experts with a track record of excellence in scientific research provided us with their structured reviews. These reviews formed the basis of the final editorial decision made by the Editor-in-Chief. The review board assessed the submissions according to several well-defined criteria to decide whether the research was effectively pushing back the boundaries of knowledge. This ensured that we establish how the technology could be used beyond the initial (and much popularised) incentive layers of cryptocurrency protocols and financial services, so as to benefit the academic community, industry leaders and society at large. The high-quality research of today will fulfil the transformative potential of the technology and will lead to the new architectures, the new interfaces and higher decentralisation forces of tomorrow, within public and private organisations. Moreover, we now have the opportunity to enhance the evidence-based approach to policy design and policy recommendations.

The JBBA is now read in over 150 countries; it is available in the online repositories at the most prestigious universities worldwide, and is decisively advancing the strategic agenda of evidence-based practices in the field of blockchain and distributed ledger technologies.

Lastly, I would like to thank our Editor-in-Chief, Dr Naseem Naqvi FRCP FBBA who entrusted me more than a year and a half ago with this noble mission of being an Associate EIC for the journal. His devotion, relentless efforts, passion and enthusiasm, are an integral part of what makes The JBBA a tremendously successful endeavour. Other heartfelt thanks go to all the reviewers, fellow editors, authors, The JBBA and the BBA staff; the global blockchain community would be a much smaller place without you.

I hope you find the contents of the journal enjoyable and beneficial to yourself and your institution. Please send us your comments to help strengthen our efforts.

Sincerely,

Marc Pilkington PhD FBBA
Associate Editor in Chief

ENGAGE WITH
THE BRITISH BLOCKCHAIN ASSOCIATION
AND THE JBBA

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

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

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

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

Follow us on Medium to receive exclusive content and stories from the JBBA

Connect with the BBA's Linkedin organisation profile and Follow us to receive real-time official updates

EDITORIAL BOARD

TESTIMONIALS FROM AUTHORS AND READERS

"The JBBA has an outstandingly streamlined submissions process, the reviewers comments have been constructive and valuable, and it is outstandingly well produced, presented and promulgated. It is in my opinion the leading journal for blockchain research and I expect it to maintain that distinction under the direction of its forward-looking leadership team.

Dr Brendan Markey-Towler PhD, University of Queensland, Australia"

"It is really important for a future world to be built around peer-review and publishing in the JBBA is one good way of getting your view-points out there and to be shared by experts.

Professor Dr. Bill Buchanan OBE PhD, Edinburgh Napier University, Scotland"

"The JBBA has my appreciation and respect for having a technical understanding and the fortitude for publishing an article addressing a controversial and poorly understood topic. I say without hesitation that JBBA has no equal in the world of scientific Peer-Review Blockchain Research.

Professor Rob Campbell, Capitol Technology University, USA"

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

Dr. Prateek Goorha PhD, Blockchain Researcher and Economist"

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

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

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

Dr. Delton B. Chen PhD, Global4C, USA"

> This is a very professionally presented journal.
>
> *Peter Robinson, Blockchain Researcher & Applied Cryptographer, PegaSys, ConsenSys*

> Very professional and efficient handling of the process, including a well-designed hard copy of the journal. Highly recommend its content to the new scientific field blockchain is creating as a combination of CS, Math and Law. Great work!
>
> *Simon Schwerin MSc, BigChain DB and Xain Foundation, Germany*

> JBBA has quickly become the leading peer-reviewed journal about the fastest growing area of research today. The journal will continue to play a central role in advancing blockchain and distributed ledger technologies.
>
> *John Bond, Senior Publishing Consultant, Riverwinds Consulting, USA*

> I had the honour of being an author in the JBBA. It is one of the best efforts promoting serious blockchain research, worldwide. If you are a researcher, you should definitely consider submitting your blockchain research to the JBBA.
>
> *Dr. Stylianos Kampakis PhD, UCL Centre for Blockchain Technologies, UK*

> I would like to think of the JBBA as an engine of knowledge and innovation, supporting blockchain industry, innovation and stimulate debate.
>
> *Dr. Marcella Atzori PhD, EU Parliament & EU Commission Blockchain Expert, Italy*

> The overarching mission of the JBBA is to advance the common monologue within the Blockchain technology community. JBBA is a leading practitioners journal for blockchain technology experts.
>
> *Professor Dr. Kevin Curran PhD, Ulster University, Northern Ireland*

> The articles in the JBBA explain how blockchain has the potential to help solve economic, social, cultural and humanitarian issues. If you want to be prepared for the digital age, you need to read the JBBA. Its articles allowed me to identify problems, find solutions and come up with opportunities regarding blockchain and smart contracts.
>
> *Professor Dr. Eric Vermeulen, Tilburg University, The Netherlands*

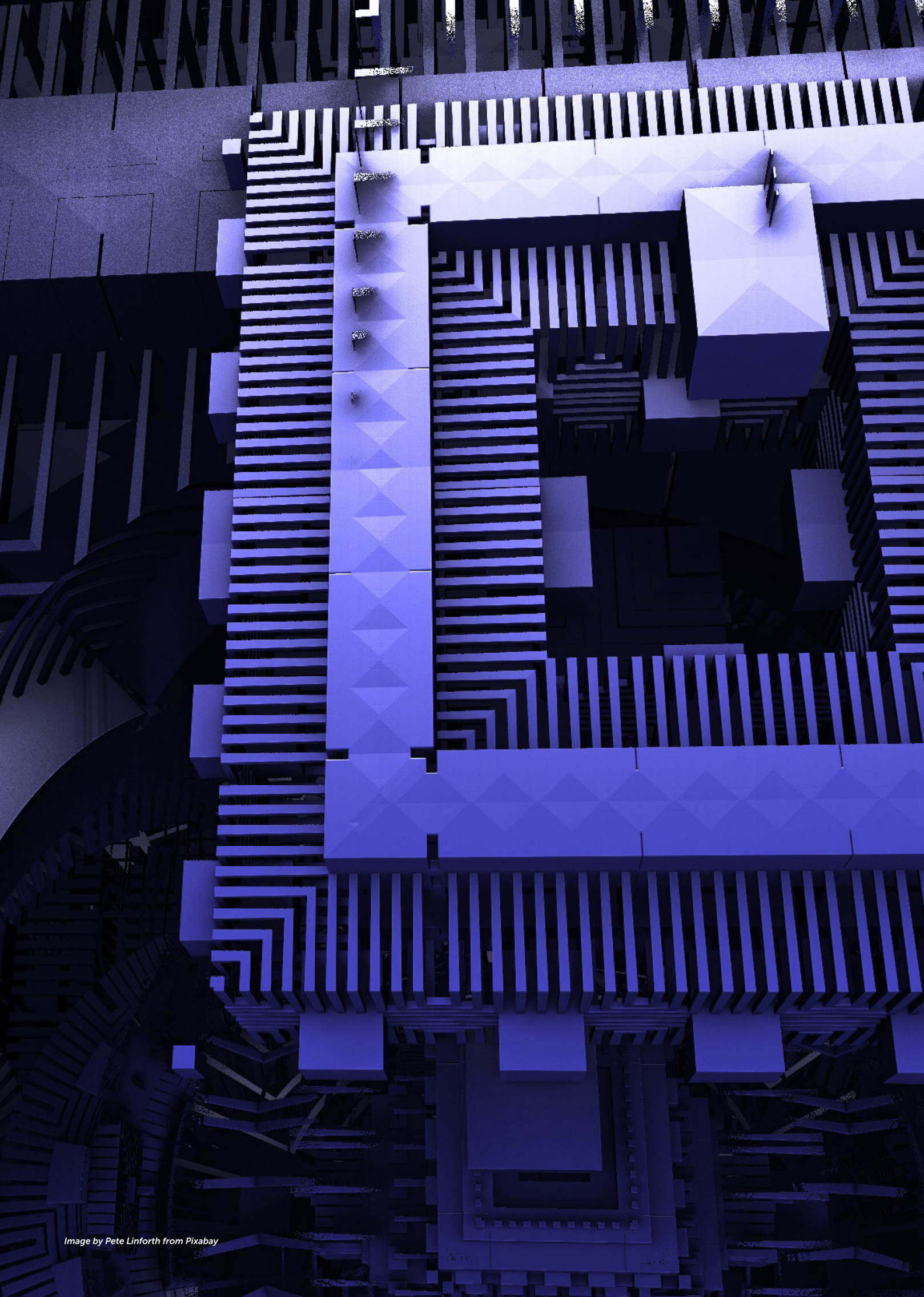


Image by Pete Linforth from Pixabay

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(4)2019

Transitioning to a Hyperledger Fabric Hybrid Quantum Resistant-Classical Public Key Infrastructure

Robert E. Campbell Sr.
Capitol Technology University, Laurel, USA
Correspondence: rc@medcybersecurity.com
Received: 13 June 2019 **Accepted:** 26 July 2019 **Published:** 31 July 2019

Abstract

Hyperledger Fabric (HLF) is a permissioned, blockchain designed by IBM and uses Public Key Infrastructure (PKI), for digital signatures, and digital identities (X.509 certificates), which are critical to the operational security of its network. On 24 January 2019, Aetna, Anthem, Health Care Service Corporation, PNC Bank, and IBM announced a collaboration to establish a blockchain-based ecosystem for the healthcare industry [1]. Quantum computing poses a devastating impact on PKI and estimates of its large-scale commercial arrival should not be underestimated and cannot be predicted. The HIPAA (Health Insurance Portability and Accountability Act) and General Data Protection Regulation (GDPR), requires "reasonable" measures to be taken to protect Protected Health Information (PHI), and Personally Identifiable Information (PII). However, HLF's ecosystem is not post-quantum resistant, and all data that is transmitted over its network is vulnerable to immediate or later decryption by large scale quantum computers. This research presents independent evaluation and testing of the National Institute of Standards and Technology (NIST), based Second Round Candidate Post-Quantum Cryptography (PQC), lattice-based digital signature scheme qTESLA. The second-round submission is much improved, however; its algorithm characteristics and parameters are such that it is unlikely to be a quantum-resistant "as is," pure "plug-and-play" function and replacement for HLF's PKI. This work also proposes that qTESLA's public keys be used to create a quantum-resistant-classical hybrid PKI near-term replacement.

Keywords: *Hyperledger Fabric, PKI, HIPAA, GDPR, distributed ledger, post-quantum cryptography, qTESLA, Ring Learning with Errors, cybersecurity, enterprise blockchains*

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

1. Introduction

An X.509 PKI is a security architecture that uses cryptographic mechanisms to support functions such as email protection, web server authentication, signature generation, and validation. It is a specification upon which applications like Secure Multipurpose Internet Mail Extensions (S/MIME) and Transport Layer Security (TLS) are based. It also can be defined as a collection of methods, rules, policies, and roles that are required to generate, manage, provide, employ, and revoke digital certificates; it is also responsible for the management of public-key encryption. A PKI ensures the secure transfer of data over various network infrastructures, such as Intranet and Internet architectures. HLF's Enterprise Blockchain, and in general the secure communications, critical infrastructure, banking, and Internet commerce depends upon the security and reliability of PKI cryptography. Cryptographic encryption and signature algorithms are used to ensure confidentially, integrity, and authenticity of messages, data, and information. PKI is used to bind identities, and public-keys and Fabric uses Certificate Authorities (CA), as the primary trusted party that uses digital signature algorithms to sign certificates of trust. The architecture, deployment, and operation of HLF impact the blockchain network's cybersecurity risks and determine the controls best able to mitigate those risks. Key considerations include the ability of untrusted or unauthorized persons to participate in the network; and the strength of the encryption protocols. Advances in quantum computing are threatening today's global encryption standards, including PKI [2]. There is an immediate need to develop, deploy, and migrate the consortium's blockchain ecosystem to a hybrid safe PQC. PQC is

cryptosystems which run on classical computers and are considered to resistant to quantum computing attacks. There are significant uncertainties associated with PQC, such as, the possibility of new quantum algorithms being developed which would cause new attacks. Also, new PQC algorithms are not thoroughly tested and analyzed. It takes years to understand their security in a classical computing environment. This work evaluates HLF's blockchain post-quantum computing vulnerabilities and threats given global regulatory requirements and provides valuable second-round qTESLA independent testing and evaluation data and aids in the NIST Post-Quantum Cryptography Standardization Process [3]. Further, the author encourages additional independent testing, verification, and validation of qTESLA as one of the most practical hybrid quantum-resistant PKI systems.

2. Implications in this Work

Without plans for quantum-resistant cryptography and security, all data and information, including encrypted, that is transmitted today, and tomorrow is vulnerable. This would violate all known regulatory requirements for data privacy and security. HIPAA enacted in 1996 and is United States legislation that provides security and data protection for medical information [4]. GDPR requires in the case of a personal data breach notification not later than 72 hours after having become aware of it [5]. Both GDPR and HIPAA levies hefty fines and penalties due to non-compliance. GDPR non-compliance with various provisions of the GDPR shall be fined according to the gravest infringement, which can be Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher [6]. HIPAA violations of penalties and fines for noncompliance are also based on the level of perceived negligence. These fines can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for each violation [7]. It takes years of study and analysis of quantum-resistant cryptography algorithms before governments and industry can trust their security. Given the nature and the far-reaching implications of the legal and financial obligations of both these laws, it is essential to have plans and strategies to address and mitigate vulnerabilities and threats that may lead to data breaches and non-compliance. Permissioned blockchains are not immune to cyber-attacks, and further exploration of the quantum-resistant cryptography is a necessity, and, a consensus between industry and regulators regarding the appropriate cybersecurity standards to apply to blockchain solutions in the healthcare, financial and GDPR covered services industry. An honest discussion and principles approach to cybersecurity regulation all in mitigating cybersecurity risk in permissioned blockchains while allowing the technology to continue to evolve through innovation.

Failure to comply with HIPAA, GDRP, and other regulating authorities can result in stiff penalties. Fines will increase with the volume of data or the number of records exposed or breached, and the amount of neglect. The lowest fines begin with a breach when the rules are not known, and by exercising reasonable diligence, would not have known the provisions were violated. At the other end of the spectrum are fines levied where a breach is due to negligence and not corrected appropriately.

We need a coordinated strategy and approach with specific recommendations and policies for academia, policymakers, and industry participants regarding and promoting the development of secure blockchain technologies and applications through viable cybersecurity standards. The enterprise blockchain cybersecurity risks must be understood, and risk management plans along with policies for HLF and enterprise blockchain, in general, must have policies that are by regulating authorities.

3. Significance of the Findings

IBM simultaneously is a leading developer of enterprise-grade blockchains and quantum computers. In 2018, Harriet Green, chairman, and CEO of IBM Asia Pacific, stated: "IBM sees quantum computing going mainstream within five years" [8]. Currently, there is not a specific strategy to mitigate the threat of quantum computers, and as such, all known data security and privacy laws will be violated. There are significant regulatory responsibilities of its participants that own, create, modify, store, or transmit regulated data and information. Enterprise-grade blockchains must enact holistic approaches to cybersecurity across applications, infrastructure, and processes. Cybersecurity must defend against attacks, but also maintain control of data content. This research illuminates the need for new policies to be developed for those entities whose data is regulated. To the author's knowledge, no cybersecurity policy addresses regulated data on enterprise blockchains. A cybersecurity policy outlines the assets that need protection and the threats to those assets and the rules and controls for protecting them. The policy should inform all approved users of their responsibilities to protect information about those assets. Policy management, reporting, and administration will be essential for organisations inputting their data on blockchains. Participants will need to be able to report enterprise-wide on everything users have done with regulated content to satisfy compliance requirements.

HLF's PKI system of trust is broken with the arrival of large-scale quantum computing, and all PII and PHI are at risk with no known plans to mitigate. HIPAA, GDPR, FINRA, and all known data and privacy laws that will be violated. The author has independently

tested, verified, and validated qTESLA's much improved Second Round Submission to NIST Post-Quantum Cryptography Standardization Process and has proposed a hybrid quantum-resistant PKI system for replacement in HLF. The test result yields smaller key sizes; however; given today's standards and applications in use only qTESLA's public key is recommended for use in a hybrid PKI solution. qTESLA's public-key is an adequate replacement for the current ECDSA public-key. In HLF's PKI, it is the public key that is used most often and qTESLA's second submission offers an acceptable size that could reinforce a mix of the most practical quantum-resistant digital signature scheme with current ECDSA algorithms.

Given what is at risk for the blockchain implementors and its users, reasonable measures must be taken to mitigate the threat of data privacy and security. To safeguard data on a blockchain platform, the participants must be able to control who has access to their data and under what circumstances. Blockchain networks must be able to provide reasonable measures and safeguards that adhere to privacy regulations such as HIPAA, FINRA, and GDPR.

4. HLF and PKI and Membership Services Technology

IBM offers Cryptographic PKI Services that allow users to establish a PKI infrastructure and serve as a certificate authority for internal and external users, issuing and administering digital certificates. It supports the delivery of certificates through the Secure Sockets Layer (SSL) for use with applications that are accessed from a web browser or web server. It includes delivery of certificates that support the Internet Protocol Security standard (IPSEC) for use with VPN applications and delivery of certificates that support Secure Multipurpose Internet Mail Extensions (S/MIME), for use with email applications. All these functions are essential but critically vulnerable.

Fabric is a private, blockchain technology that uses smart contracts, and participants or members manage its transactions. The members of the network enroll through a "trusted" Membership Service Provider (MSP) [9]. The blockchain is advertised as an implementation of distributed ledger technology (DLT) that delivers enterprise-ready network security, scalability, confidentiality, and performance, in modular blockchain architecture.

The MSP issues, cryptography, protocols, encryption, signature keys and issues and validates certificates and user authentication to clients and peers. HLF's PKI consists of Digital Certificates, Public and Private Keys, and Certificate Authorities (CA) which issues digital certificates to parties, who then use them to authenticate messages. A CA's Certificate Revocation List (CRL) is a reference for the certificates that are no longer valid. PKI is used to generate certificates which are tied to organizations, network components, and end-users or client applications. The MSP dispenses X.509 certificates that can be used to identify components as belonging to an organization. Certificates issued by CAs can also be used to sign transactions to indicate that an organization endorses the transaction result and is a necessary precondition of it being accepted onto the ledger. These X.509 certificates are used in client application transaction proposals and smart contract transaction responses to digitally sign transactions. Its digital certificate is compliant with the X.509 standard and holds the attributes relating to the holder of the certificate. The holder's public key is distributed within the certificate, and the private signing key is not.

The public-keys and private-keys are made available and act as an authentication "anchor," and the private keys are used to produce digital signatures. Recipients of digitally signed messages can validate and authenticate the received message by checking that the attached signature is valid with the use of the public key. Digital identities are cryptographically validated digital certificates that comply with X.509 standard and are issued by a Certificate Authority (CA). HLF uses a list of self-signed (X.509) certificates to constitute the root of trust and a list of self-signed (X.509) certificates to form the root of trust. A CA dispenses certificates that are digitally signed by the CA and bind together the actor with the actor's public key. The above services are critical to the operation of a secure enterprise blockchain, and there must be plans and strategies in place that provide reasonable measures to adhere to regulatory policies.

5. Post-Quantum Computing Impact on HLF PKI

PQC algorithms must provide security against both classical and quantum computing attacks. Their performance is measured on classical computers and considerations are made for the potential of "drop-in replacements," which infers compatibility and interoperability with existing systems. Also, essential requirements must include resistance to side-channel attacks and misuse.

Cryptography in HLF is used in many applications where secure communication is needed. The primary use and role are signature generation, verification, and authentication where algorithms are used to establish confidentiality, integrity, and authenticity of messages sent during communication. Public-key cryptography is used where each participant has a private key and a public key. In a public-key signature cryptosystem, the signer has a private signing key that can be used to sign messages and must keep this key secure. The public key, which is visible to anyone, can be used to verify that the signature is authentic and, if the signature

scheme is secure, then repudiation is achieved and only the signer could have generated the signature. PKIs are used to bind identities to the public keys, where Certificate Authorities (CAs) play an essential role. A CA is a commonly trusted party that uses digital signature algorithms to author certificates consist of a public key and information of its owner. The security of public-key cryptography and ultimately, the private key is based on cryptography that can no longer be considered safe because of the emerging quantum computing threat. HLF relies on a PKI, which is based upon Elliptic Curve Cryptography (ECC), and it is critically vulnerable to quantum computing [10]. Specifically, the cryptography that secures web browsers (TLS), certificates, software updates, virtual private networks (IPsec), secure email (S/MIME) and many other applications are no longer safe in the PQC era [11]. Reasonable blockchain enterprise cybersecurity measures require extensive planning and testing for transition and migration to post-quantum resistant cryptography.

It is unlikely that the current PQC algorithms under review will function "as is" and will require modifications such as hybrid quantum resistant-classical PKI systems. Hybrid systems will likely be the way forward in the near term, given the uncertainties and complexities of the current crop of PQC algorithms. Current cryptographic libraries will provide support for post-quantum digital signature algorithms in PKI but will require some modifications and testing in large-scale scenarios.

In this paper, the author investigates the use of hybrid digital signature schemes, specifically qTESLA. Much testing needs to be done in real-world scenarios involving digital signatures and PKI. Protecting against quantum attacks will require changes that designers and implementers will have to accommodate. Cryptographic primitives may need to be a replaced, and protocol-level modifications may be necessary to provide new primitives. It is a complex and lengthy undertaking to migrate to a new quantum-resistant PKI. Other issues such as constrained devices, compatibility, performance characteristics, and Internet of Things (IoT) must also be considered. Currently, HLF uses the Elliptic Curve Digital Signature Algorithm, which is used for many functions such as digital signatures and TLS protocol handshakes.

6. Elliptic Curve Cryptography in HLF

Elliptic curve cryptography is a class of public-key cryptosystem which assumes that finding the elliptic curve discrete algorithm is not possible in a "reasonable" amount of time. Public key cryptography does not require any shared secret between the communicating parties. The security of elliptic curve or asymmetric cryptographic schemes relies on the believed hardness of solving "hard problems," such as integer factorization and the computation of discrete logarithms in finite fields or groups of points on an elliptic curve. The ECDSA algorithm relies critically on generating a random private key used for signing messages and a corresponding public key used for checking the signature. The bit security of this algorithm depends on the ability to compute a point multiplication and the inability to calculate the multiplicand given the original and product points. Decades ago, these were "hard problems," due to several factors such as the current state of computing power, and the time it would take for a classical computer to solve these problems. Other factors come into play, such as the length of cryptanalysis and the lack of known techniques that ensured the problems remained hard. However, the technology of computing power, cryptanalysis, and side-channel analysis always threaten the existing cryptographic standards given enough time. It can be noted that many real-world cryptographic vulnerabilities do not stem from solely a weakness in the underlying algorithms, but often from implementation flaws such as side-channel attacks, errors in software or code design flaws. An example is the vulnerabilities ECDSA signature implementation, is the property of weak randomness used during signature generation, which can compromise the long-term signing key.

The HLF CA provides features such as, registration of identities, or connects to Lightweight Directory Access Protocol (LDAP) as the user registry, issuance of Enrollment Certificates (ECerts), certificate renewal and revocation. HLF's ECDSA offers the following key size options:

Table 1. Algorithms used to generate X.509 certificates and keys are not secure [12]

Size	ASN1 OID	Signature Algorithm
256	prime256v1	ecdsa-with-SHA256
384	secp384r1	ecdsa-with-SHA384
521	secp521r1	ecdsa-with-SHA512

The approved security strengths for U.S. federal applications are 128, 192, and 256 bits. Note that a security strength of fewer than 128 bits is no longer approved because quantum algorithms reduce the bit security to 64 bits (see table 2). NIST Special Publication 800-57 Part 1 Revision 4: Recommended for Key Management, as shown in Table 2 [13]. Table 2 shows that Rivest, Shamir, and Adleman (RSA) and ECC based PKI have zero bits of security and AES requires larger keys. This table illustrates the vulnerability and single point failure, of the fully trusted CA and X509 standard based on ECC. The quantum computing threat collapses the RSA, ECC, and HLF's PKI.

Table 2. Comparison of conventional and quantum security levels of typical ciphers [14]

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

7. Evaluation of qTESLA's Second Round Submission to NIST

The National Institute of Standards and Technology (NIST) is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new public-key cryptography standards will specify one or more additional digital signature, public-key encryption algorithms. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers. The author tracked with NIST in identifying three broad aspects of evaluation criteria that would be used to compare candidate algorithms throughout the NIST PQC Standardization Process. The three elements are 1) security, 2) cost and performance, and 3) algorithm and implementation characteristics. Security is the most crucial factor when evaluating candidate post-quantum algorithms. Cost as the second-most important criterion when assessing candidate algorithms. In this case, cost includes computational efficiency and memory requirements. After security, the performance was the next most important criterion in selecting the second-round candidates [3].

qTESLA is a lattice-based signature scheme which uses the assumption that RLWE distributions are indistinguishable from random. The public key in qTESLA is, roughly speaking, a sample of an RLWE distribution. The signer keeps secret information about this sample and uses that information along with a hash function to produce signatures. Signature verification involves some simple arithmetic within the chosen ring, and then the recomputation of a hash function. qTESLA has reasonably good performance parameters that are comparable to the other lattice-based signature schemes. The submitters of qTESLA have claimed a tight security proof for the schemes in the quantum random oracle model. It was noticed that a bug in the security proof requires an adjustment of the parameters (which reduces the efficiency of the scheme). Furthermore, the security argument assumes (among other things) conjecture about the distribution of random elements in the ring. Considering that the conjecture does do not seem to fit the form of a typical security assumption, and more analysis will need to be conducted in the second round.

This section, tests, evaluates and analyzes qTESLA's second-round submission modifications in the lattice-based digital signature scheme category to NIST's post-quantum standardization project. This second-round submission is based on the hardness of the decisional Ring Learning With Errors (R- LWE) problem. qTESLA utilizes two approaches for parameter generation that includes heuristic and provably- secure. The heuristic approach is optimized for efficiency and key size, and the provably- secure is targeted to highly sensitive or classified transactions. A new feature added in the second-round submission is a key compression technique that produces a noticeable reduction in the public key size. The vendor refers to this technique as "public key splitting," and is significant because it is the public key that is used most often in typical transactions. qTESLA has submitted twelve parameter sets targeting various security levels. However, this work focuses on submissions that include public-key reduction and the most efficient submissions as the most practical hybrid (classical and quantum-resistant) PKI near-term algorithm solution [14].

8. Basic signature scheme

Informal descriptions of the algorithms that give rise to the signature scheme qTESLA are shown in Algorithms 1, 2, and 3. These algorithms require two basic terms, namely, B-short and well-rounded, which are defined below.

Let q, L_E , L_S , E, S, B, and d be system parameters that denote the modulus, the bound constant for error polynomials, the bound constant for the secret polynomial, two rejection bounds used during signing and verification that are related to L_E and L_S , the bound for the random polynomial at signing, and the rounding value, respectively. An integer polynomial y is B-short if each coefficient is at most B in absolute value. An integer polynomial w well-rounded if w is $(\lfloor q/2 \rfloor - E)$-short and $[w]_L$ is $(2^{d-1} - E)$-short.

In Algorithms 1-3, the hash oracle H(•) maps to H, where H denotes the set of polynomials $c \in R$ with coefficients in $\{-1, 0, 1\}$ with exactly h nonzero entries.

Algorithm 2 is described as a non-deterministic algorithm. This property implies that different randomness is required for each signature. This design feature is proposed as added to prevent some implementation attacks and protect against some fault attacks [13].

Algorithm 1 Informal description of the key generation

Require: -

Ensure: Secret key $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$, and public key $pk = (a_1, ..., a_k, t_1, ..., t_k)$

- $a_1, ..., a_k \leftarrow R_q$ ring elements.
- Choose $s \in R$ with entries from D_σ. Repeat step if the h largest entries of s sum to at least L_S .
- For $i = 1, ..., k$: Choose $e_i \in R$ with entries from D_σ. Repeat step at iteration i if the h largest entries of e_i sum to at least L_E.
- For $i = 1, ..., k$: Compute $t_i \leftarrow a_i s + e_i \in Rq$.
- Return $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$ and $pk = (a_1, ..., a_k, t_1, ..., t_k)$

Algorithm 2 Informal description of the signature generation

Require: Message m, secret key $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$

Ensure: Signature (z, c)

- Choose y uniformly at random among B-short polynomials in Rq.
- $c \leftarrow H([a1y]M , ..., [aky]M , m)$.
- Compute $z \leftarrow y + sc$.
- If z is not $(B - S)$-short then retry at step 1.
- For $i = 1, ..., k$: If $a_i y - e_i c$ is not well-rounded then retry at step 1.
- Return (z, c).

Algorithm 3 Informal description of the signature verification

Require: Message m, public key $pk = (a_1, ..., a_k, t_1, ..., t_k)$, and signature (z, c)

Ensure: "accept" or "reject" signature

- If z is not $(B - S)$-short then return reject.
- For i = 1, ..., k: Compute $wi \leftarrow aiz - tic \in Rq$.
- If $c \neq H([w1]M , ..., [wk]M , m)$ then return reject.
- Return accept.

9. New features

qTESLA utilizes two approaches for parameter generation, the first approach, referred to as "heuristic qTESLA," follows a heuristic parameter generation and the second approach, referred to as "provably secure qTESLA," follows a provably secure parameter generation according to existing security reductions. New in this submission is mitigation steps to address the implementation attacks as research shows the vulnerabilities of lattice-based signature schemes such as qTESLA [16]. The second and third new feature is the AVX2-optimized implementations for the parameter sets qTESLA-I, qTESLA-III, and qTESLA-V, and their variants with smaller public keys, called "public key splitting," for qTESLA-I-s, qTESLA-III-s, and qTESLA-V-s respectively. qTESLA's AVX2-optimized implementations submission included an Intel Advanced Vector Extensions 2 (AVX2) submission which significantly improved performance. The author performed experiments with qTESLA's AVX2 optimized implementation, and the results are included in this paper. The public key splitting submission is a variant that addresses public key size, which is significant because the public key size is regarded as more important than the secret key size because the former needs to be transmitted more frequently [14].

10. Mitigation of implementation attacks

Side-channel cryptanalysis considers attackers trying to take advantage of the physical interactions of cryptographic devices to achieve recovery of the secret key. In some cases, computational faults are intentionally inserted to obtain faulty values for the key recovery. Fault injections or attacks are also used to obtain information leakage under the faulty environment. These implementations-specific attacks are more efficient than the best-known cryptanalytic attacks. They are therefore generally more powerful than classical cryptanalysis and are a serious class of attacks that must be addressed. These attacks exploit timing or power consumption, electromagnetic emanation, that is correlated to some secret information during the execution of a cryptographic scheme and protection against this attack is a minimum-security requirement for standardized cryptographic implementation. qTESLA attempts to address the exploit timing leakage, power consumption, electromagnetic emanation, and cache attacks by adding constant-time execution to secure against side-channel analysis. qTESLA 's approach indicates that it is in every signing operation, it injects "fresh randomness," that will make it resilient to a catastrophic failure of the Random Number Generator (RNG) protecting against fault analysis attacks [14]. The verification and validity of the previous statements are not in the scope of this paper and will most likely require more independent tests and analysis.

11. Performance of second-round qTESLA algorithms analysis

To evaluate the performance of the provided implementations written in portable C, the author ran benchmarking suite on one machine powered by an Intel® Core™ i7-6500 CPU @ 2.50 GHz x 4 (Skylake) processor, 16 GB of RAM, 500 GB hard drive,

GNOME:3.28.2, running Ubuntu 18.04.2 LTS. For compilation, GCC version 7.3.0 was used in all tests. The vendor proposed twelve parameter sets which were derived according to two approaches (i) following a "heuristic" parameter generation, and (ii) following a "provably-secure" parameter generation according to a security reduction. The proposed parameter sets are displayed in Table 3, together with their targeted security category.

The results for the optimized implementations are summarized in Tables 4, and 5, respectively. The results for AVX2 implementations are given in Tables 6, and 7, respectively. Additionally, the reference implementations are summarized in Tables 8, and 9, respectively. Results for the median and average (in parenthesis) are rounded to the nearest 102 cycles. Signing is performed on a message of 59 bytes.

Table 3. Parameter sets and their targeted security [14]

Heuristic	Provably secure	Security category
qTESLA-I, qTESLA-I-s	qTESLA-p-I	NIST's category 1
qTESLA-II, qTESLA-II-s	-	NIST's category 2
qTESLA-III, qTESLA-III-s	qTESLA-p-III	NIST's category 3
qTESLA-V, qTESLA-V-s	-	NIST's category 5
qTESLA-V-size, qTESLA-V-size-s	-	NIST's category 5

Table 4. Second Round Optimized Implementation tests for 5000 iterations.

Scheme	keygen	sign	verify	total (sign + verify)
qTESLA-II	4410.7 (4963.6)	931.7 (1226.1)	232.8 (236.5)	1164.5 (1462.6)
qTESLA-II-s	4004.0 (4818.7)	981.5 (1281.4)	232.7 (235.1)	1214.2 (1516.5)
qTESLA-V-size	17177.0 (20416.5)	2161.4 (2812.1)	511.6 (514.2)	2673.0 (3326.3)
qTesla-V-size-s	17201.1 (20340.2)	2341.4 (2972.4)	516.8 (523.1)	2858.2 (3495.5)

Table 5. Second Round Optimized Implementation Key Sizes in Bytes

Scheme	Public Key	Secret Key	Signature
qTESLA-II	2336	931.7	232.8
qTESLA-II-s	800	3136	2432
qTESLA-V-size	5024	3520	4640
qTesla-V-size-s	1952	6592	5216

This work is a follow-on to qTESLA's NIST first-round submission, and the evaluation focuses on the "new" and improved features submitted in its second-round NIST submission. This second-round submission includes an expanded category of parameters in which the author examined the most practical based on

Table 6. Second Round AVX2 Implementation

Scheme	keygen	sign	verify	total (sign + verify)
qTESLA-I	903.2 (940.9)	206.4 (268.2)	55.1 (55.8)	261.5 (324)
qTesla-I-s	928.5 (952.4)	214.9 (276.6)	54.8 (55.9)	269.7 (332.2)
qTESLA-III	2373.5 (2677.0)	273.5 (343.5)	110.4 (111.3)	383.9 (454.8)
qTESLA-III-s	2366.8 (2713.6)	291.4 (374.2)	110.0 (112.4)	401.4 (486.6)
qTESLA-V	12577.2 (14472.8)	734.1 (951.3)	254.9 (256.0)	989.0 (1207.3)

Table 7. Second Round AVX2 Implementation Key Sizes in Bytes

Scheme	Public Key	Secret Key	Signature
qTESLA-I	1504	1216	1376
qTesla-I-s	480	2240	1568
qTESLA-III	3104	2368	2848
qTESLA-III-s	1056	4416	3232
qTESLA-V	6432	4672	5920
qTesla-V-s	1952	6592	5216

Table 8. Second Round Reference Implementation

Scheme	keygen	sign	verify	total (sign + verify)
qTESLA-I	920.3 (971.5)	314.4 (425.6)	71.5 (72.6)	385.9 (498.2)
qTESLA-I-s	926.4 (968.5)	334.2 (438.1)	73.3 (74.2)	481.7 (512.3)
qTESLA-p-I	4130.2 (4316.4)	1990.4 (2605.6)	561.2 (567.9)	2551.6 (3173.5)
qTESLA-II	4466.0 (5047.9)	1536.6 (2027.2)	372.3 (375.7)	1908.9 (2402.9)
qTESLA-II-s	4452.1 (5047.0)	1647.3 (2213.9)	385.5 (386.5)	2032.8 (2600.4)
qTESLA-III	2395.5 (2669.8)	433.9 (580.0)	143.0 (145.2)	576.9 (725.2)
qTESLA-III-s	2410.5 (2735.2)	471.9 (610.8)	150.9 (153.6)	622.8 (764.4)
qTESLA-p-III	21043.7 (21569.7)	5414.6 (7247.6)	1517.4 (1529.4)	6932.0 (8776.4)
qTESLA-V	12224.6 (14221.3)	1349.6 (1775.1)	325.9 (329.1)	1675.5 (2104.2)
qTESLA-V-s	12644.5 (14433.8)	1439.4 (1856.3)	335.4 (336.8)	1774.8 (2193.1)
qTESLA-V-size	17357.1 (20838.9)	3653.8 (4769.2)	825.2 (830.5)	4479.0 5599.7
qTESLA-V-size-s	17859.4 (21204.1)	3824.2 (5044.1)	851.3 (847.3)	4675.5 (5891.4)

performance improvements. The most significant enhancements noted, is in the speed of key generation and the size of the public keys. Techniques, such as the AVX2 and Public key splitting, yields a dramatic

improvement over the previous submissions. The public key splitting offers acceptable sizes for various NIST security category levels, While, these implementations are not provably secure as defined by NIST, meaning the algorithms may not be approved for top secret information and operations, however; they may prove useful for less critical data and processes.

Table 9: Second Round Reference Implementation Key Sizes in Bytes.

Scheme	Public Key	Secret Key	Signature
qTESLA-I	1504	1216	1376
qTESLA-I-s	480	2240	1568
qTESLA-p-I	14880	5184	2592
qTESLA-II	2336	1600	2144
qTESLA-II-s	800	3136	2432
qTESLA-III	3104	2368	2848
qTESLA-III-s	1056	4416	3232
qTESLA-V	6432	4672	5920
qTESLA-V-s	2336	8768	6688
qTESLA-V-size	5024	3520	4640
qTesla-V-size-s	1952	6592	5216

12. Optimized implementations

All comparisons are made about qTESLA's first-round NIST submission where possible, due to the fact there are new submissions and comparisons cannot be made. The optimized implementation for key sizes shows qTESLA-II vs. qTESLA-II-s shows 78.5% public-key reduction; however; there is an increase in the secret key and signature size of 236.5 % and 944.6 % respectively. Submissions for qTESLA-V-size vs. qTESLA-V-size-s shows 61.1 % public-key reduction, while there is an increase in the secret key and signature size of 87.2 % and 12.4 % respectively. (See Table 5).

12.1. AVX2 implementation

The AVX2 implementation for key generation, signing, and verification is shown in Table 6 and is compared to the new AVX2 and public-key reduction. The tests show that there is a slight increase in key generation time, signature and verification time for all categories of submission when using the public-key reduction techniques, however; these improvements are dramatic compared to the respective timing in all categories in qTESLA's first submission [2]. (See Table 6). The AVX2 implementation for key sizes shows qTESLA-I vs. qTESLA-I-s shows 68.1 % public-key reduction; however; there is an increase in the secret key and signature size of 84.2 % and 13.9 % respectively. Submissions for qTESLA-III vs. qTESLA-III-s shows 65.9 % public-key reduction, while there is an increase in the secret key and signature size of 86.5 % and 13.4 % respectively. Finally, in this category, qTESLA-V vs. qTESLA-V-s shows 69.6 % public-key reduction, while there is an increase in the secret key and signature size of 86.5 % and 41.0 % respectively, See Table 7.

12.2. Reference implementation

The last category examined is Reference implementation, which has 12 parameters. Since many of these parameters are new, direct comparison to the previous submission cannot be made. However; the author notes overall, there is a significant reduction in key generation, signing, and verification times compared to the first-round submission. The following is a comparison of the first-round submission to the second-round submission. For example, for key generation, signing, and verification CPU cycles qTESLA-I reduced key generation cycle time by 26.4 % but increased 5.7 % signing, decreased 12.1 % verification respectively. qTESLA-p-I showed key generation cycle reduction of 23.0 %, but the 152 % increase in signing, an increase of 34.1 % verification. qTESLA-p-III showed a decrease of 16.3 % key generation, but increase signing 71.6 %, and a reduction of 28.3 % verification time (See Table 8 and [2]). The test results of the Reference implementation key sizes in bytes are in Table 9. The following observations can be made from a comparison of the first-round submission with the second-round submission; The most dramatic improvement comes with the public key splitting function, while test results show there is a corresponding increase in secret key size and signature. For example, for the public key of qTESLA-I-s vs. qTESLA-I decreased by 68.0%, but the secret key increased by 84.2 %, and the signature increased by 13.9 %. qTESLA-III-s vs. qTESLA-III show a reduction of 65.9 %, but an increase in the secret key size of 86.4 %, and an increase in the signature size by 13.4 %. Please see Table 9 for further comparisons.

13. Recommendations for Blockchain Implementors

HLF implementors should develop and provide a strategy or roadmap for maintaining the confidentiality, integrity, and availability of private keys and stringent cybersecurity controls to combat the quantum computing threat. Also, implementers should review their current cryptographic standards to make sure they are up to date, and that infrastructure and support exist to update when new NIST standards become available rapidly. Immediate work should begin to test and benchmark the most promising PQC candidates that could be integrated into its blockchain with interoperability and compatibility in mind. The X.509v3 standard allows for algorithm flexibility in that the Object Identifier (OID) defines the formats of public keys. Adding a new cipher OID is needed to extend X.509, but what is also required is for software will be able to comprehend and process the new OID. Currently, there are no known CAs issuing certificates for quantum-safe public keys exist, and no CAs is

signing their certificates with a quantum-safe signature algorithm.

Strong blockchain network security requires the roles and responsibilities of each type of participant to be clearly defined and enforced following regulatory guidelines. It is essential to qualify, quantify, and document cybersecurity risks posed by each type of participant. It is also essential to anticipate and understand the security consequences of participants leaving and entering the network over time. Blockchain developers should anticipate and understand these threats resulting before committing regulated data to the blockchain. There should be plans for penetration testing that are similar to traditional networks using various attack scenarios and vectors, document the development process and obtain independent audits of the design and development process.

Therefore, there is an urgent requirement to develop and deploy plans to accommodate the most practical hybrid PQC algorithms that are working towards global standardization. The successful transition and migration to PQC will require significant time and effort given the complexities involved. Further, researchers should examine hybrid solutions where both classical cryptography algorithms and PQC algorithms working together to mitigate the uncertainties in the pace and development of quantum computers and the reliability of candidate PQC under the global standards community.

13.1. Recommendations for Healthcare and GDPR Covered Entities

HLF and other permissioned blockchains present unique opportunities and vulnerabilities in managing cybersecurity risks. As the healthcare industry, financial services, and GDPR covered industry begin to experiment with and commit to pilots, these entities need to understand that the risks are appropriately identified, and this is a risk management plan. This risk management plan is required for regulated data, and there must be one for enterprise blockchains. Therefore, beyond the hype of any new technology, a thorough cybersecurity program remains vital, and all parties need to conduct due diligence to protecting the network and participating organizations from cyber threats. Also, the participation of multiple entities, each with their on-ramps into the enterprise blockchain, is a potential source of vulnerability.

Ask blockchain vendors about their quantum-safe features to protect data that is under regulatory guidance

- Query software-as-a-service or third-party platform providers about their embedded cryptographic methods and plans for an ecosystem-level solution to protect organizations and maintain contractual obligations.
- Determine how to implement best the GDPR principle of "the right to be forgotten."
- What is the ability to detect, correct fraudulent, malicious, or erroneous records?
- It is unclear which organization will be considered as the data controller and processor within the Fabric and enterprise blockchains, especially when they cross international borders.
- Create new quantum-proof policies, methods, and procedures aligned to use cases/requirements. Update asset inventory with newly implemented cryptographic details.

Healthcare, GDPR, and financial entities must not think that there are no risks associated with blockchain enterprise blockchain networks and must ask for documented risk management strategies to protect regulated data. As the HLF blockchain ecosystem becomes more diverse and grows in popularity, vendors, users, and implementors must be aware of possible cyber-attack. While blockchains offer unique structures and provide cybersecurity capabilities that are not present in today's networks, reasonable measures must be taken. The cybersecurity risk must be evaluated, documented, and its implications considered when regulated, businesses policymakers, and institutions commit protected data to any enterprise blockchain.

14. Conclusions and Future Work

This work has shown that HLF, enterprise blockchains, and current global PKI that relies on the PKI X.509 standard to ensure secure communication between various network participants are utterly vulnerable to the quantum computing threat. Falsified certificates destroy the trust, integrity, confidentiality, and non-repudiation in the entire blockchain and can have enormous consequences if measurements are not taken. It has been shown that quantum computers break ECC on which PKI depends and therefore exposes its implementers and users to potentially massive fines for non-compliance and security incidents with GDPR, FINRA and HIPAA laws. Enterprise Blockchains such as HLF are being adopted in many industries that have regulatory controls over the data. For example; GDPR regulates European Union citizens' data with the potential of massive fines irrespective of the location or headquarters of the blockchain implementation location. Financial and PII data privacy and information is becoming more heavily regulated, especially on Wall Street and in the state of New York and California. In the United States, healthcare data privacy is a significant issue with the

increase in cyber-attacks, and the resulting lawsuits, fines, and penalties levied on violators.

The author argues that blockchain technology has the potential to address the documented issues of legacy health and financial information technology systems, such as interoperability, data access, speed, and privacy and the ability to adapt to changing programs. However; out-of-date cryptographic standards will be broken and will not forestall any adversaries from breaking their encryption and gaining access to highly regulated data and information. Development and deployment plans need to be developed to accommodate the most practical hybrid PQC algorithms that are working towards global standardization. Also, blockchain cybersecurity policy is required to govern acceptable use and should include standards, procedures, and guidelines.

Cybersecurity should begin with an assessment that includes current security policies, identification of objectives, review of requirements, and determination of existing vulnerabilities. It is imperative to begin the development of "Policy Recommendations for Enterprise Blockchains" because covered entities must know that placing their data on permissioned blockchains does not and cannot negate risks and obligations. All must understand the risks before committing regulated data, because it is required, and it is also prudent in protecting PHI, PII, GDPR, and FINRA regulated data and information. An evidence-based approach is needed to mitigate and adhere to cybersecurity regulation. All aspects must be considered such as geographic boundaries, jurisdictions and a thorough understanding of the impact of widespread governance of global regulators

As cyber threats to the HIPAA and GDPR and covered financial entities continue to grow in dedication and sophistication permissioned blockchains can contribute to add "new and advanced cybersecurity techniques" and can be a valuable tool in mitigating those threats if the risks are understood and mitigated. Permissioned blockchains offer significant cybersecurity capabilities, share some of the same cyber risks that affect other IT systems, and have unique characteristics, all of which merit further evaluation by regulators and industry. The author encourages new conversations about the cybersecurity benefits of blockchain systems and ways to promote appropriate government policies.

Finally, this research does not indicate any of NIST Second Round candidate algorithms will be a simple "drop-in replacement," and it may require additional NIST rounds and years of follow-on research, analysis and testing for a suitable "drop-in replacement," can be identified or developed. Therefore, the author believes that qTESLA offers a possible near-term "Hybrid Quantum Resistant-Classical Public Key Infrastructure," a solution with a significant reduction in its public key size. As discussed, it is the public key that is exposed and used the most in today's PKI systems, and it is possible to modify the X.509 certificate standard to accommodate this new PQC algorithm that would only provide the public key that would be much more resistant to implementation and quantum computing attacks. Additional work and testing are needed in large scale real-world scenarios to ensure there are no significant issues with incorporating PQC PKI X.509 certificates on an industrial scale. Potential problems that need to be examined are latency, overhead, and the ability for software, hardware, and other constrained devices to interoperate such as, smartphones, smart cards, and IoT. Regardless of the estimated time of arrival of large-scale quantum computers, cybersecurity should be a primary concern to enterprises and healthcare organizations because they cannot afford to have their private communications and data decrypted even if it is ten years away.

References:

[1] J. Emond, "IBM Newsroom," 24 January 2019. [Online]. Available: https://newsroom.ibm.com/2019-01-24-Aetna-Anthem-Health-Care-Service-Corporation-PNC-Bank-and-IBM-announce-collaboration-to-establish-blockchain-based-ecosystem-for-the-healthcare-industry. [Accessed 16 May 2019].

[2] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," The Journal of the British Blockchain Association, vol. 2, no. 1, pp. 17-24, 2019.

[3] NIST, "Second PQC Standardization Conference," 22 August 2019. [Online]. Available: https://www.nist.gov/news-events/events/2019/08/second-pqc-standardization-conference. [Accessed 16 May 2019].

[4] NIST, "Second PQC Standardization Conference," 22 August 2019. [Online]. Available: https://www.nist.gov/news-events/events/2019/08/second-pqc-standardization-conference. [Accessed 16 May 2019].

[5] E. Commission, "2018 reform of EU data protection rules," [Online]. Available: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. [Accessed 16 May 2019].

[6] G. EU.org, "Fines and Penalties," [Online]. Available: https://www.gdpreu.org/compliance/fines-and-penalties/. [Accessed 16 May 2019]

[7] D. o. H. a. H. S. Office for Civil Rights, "Federal Registry," [Online]. Available: https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-95. [Accessed 16 May 2019].

[8] "CNBC interview: Harriet Green, Chairman and CEO

of IBM Asia Pacific," , . [Online]. Available: https://www.cnbc.com/2018/03/30/ibm-sees-quantum-computing-going-mainstream-within-five-years.html. [Accessed 11 7 2019].

[9] A. M. V. V. K., Z. M. Jøsang, "The Impact of Quantum Computing on Present Cryptography," Arxiv, 31 March 2018. [Online]. Available: https://arxiv.org/pdf/1804.00200. [Accessed 16 May 2019].

[10] H. U. M. M. S. D. Bindel Nina, "Transitioning to a Quantum-Resistant Public Key Infrastructure," PQCrypto-BHMS17, 2017. [Online]. Available: https://s3.amazonaws.com/files.douglas.stebila.ca/files/research/papers/PQCrypto-BHMS17.pdf. [Accessed 16 May 2019].

[11] Hyperledger, "Fabric CA User's Guide," [Online]. Available: https://hyperledger-fabric-ca.readthedocs.io/en/latest/users-guide.html#table-of-contents. [Accessed 11 6 2019].

[12] "NIST Special Publications - NIST Computer Security ..., ",. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html. [Accessed 7 1 2019].

[13] L.. Chen, S. P. Jordan, Y.-K.. Liu, D.. Moody, R. C. Peralta, R. A. Perlner and D. C. Smith-Tone, "Report on Post-Quantum Cryptography | NIST," , 2016. [Online]. Available: https://nist.gov/publications/report-post-quantum-cryptography. [Accessed 30 12 2018].

[14] N. Bindel, "Submission to NIST's post-quantum project (2nd round)," 2019. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions. [Accessed 11 6 2019].

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
RC wants to thank his PhD supervisor Dr. Ian McAndrew, Dean of doctoral programs, Capitol Technology University, for his dedication, encouragement and expert guidenace in this research.

Photo by Vladimir Solomyani on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(1)2019

The Contractual Cryptoeconomy: An Arrow of Time for Economics

Prateek Goorha
Independent Scholar, Greater Boston, USA
Correspondence: goorha@sent.com
Received: 11 March 2019 **Accepted:** 18 April 2019 **Published:** 2 May 2019

Abstract

We consider the potential blockchains have for building a framework for all manner of contracts that can characterize an economy using the unifying idea of control over their duration. Such a contractual cryptoeconomy (CCE) would accommodate a broader variety of contracts than smart contracts, which are suitable for a relatively small portion of the set of all feasible contracts. We proceed by examining the idea of a contract's natural life as a common feature shared across all contracts, be they incomplete or complete. This simplifying idea suggests why providing flexibility over a contract's duration on a blockchain – through innovations such as HTLCs — is necessary to increasing the variety of contracts that can be feasibly represented. We also assess participation in a CCE that features blockchains with differing degrees of security. We do so by focusing on how the value of a contract is related directly to its natural life for both its immediate participants and, through externalities across the CCE, to a wider set of users. A key idea provides the overall impetus: When contracts rely on third-party intermediation, at least some contractual surplus is dissipated in arbiter rent, making the quality of third-party arbitration as important as its scale. By contrast, blockchains create contractual mechanisms that act as Coasian exchanges that can internalize this arbiter rent. However, crucially, the degree to which their use requires forgoing contractual complexity and absorbing the cost of externalities can determine the relative benefits provided by a CCE.

Keywords: *Arbiter Rent; Contracts; Duration; HTLCs; Blockchains; Thomas Jefferson; Economic Arrow of Time; Coasian exchange; Contractual Cryptoeconomy*

1. Introduction

'The Earth belongs, in usufruct, to the living.' - Thomas Jefferson [1].

While its specific focus is blockchains, the impetus for this article came from Thomas Jefferson's observation cited above. It is extracted from a letter he wrote to James Madison in 1789, impelled by his belief that a contract's length should be set at a fixed period.

Jefferson's actuarial skills had enabled him to calculate that – owing to the average life span of individuals then – by the end of that period one of the parties would likely have died. Contracts, he proposed, should be rescinded every 19 years. The clock should, in other words, be reset so that the usufruct of contracts can more correctly reflect their true creators and beneficiaries. It is on the nature of this link between the usufruct of a contract on the one hand and its duration on the other that we shall focus our attention on in this paper; it is, we shall see, key to the class of contracts that can be feasibly represented on a blockchain.

Yet there is also a second aspect of Jefferson's thought process that is worth appreciating: The idea that this usufruct is at risk of being delimited and squandered, and that a mandated reset of some kind is the only tool at hand to prevent this undesirable eventuality. Is a resetting of the clock necessary to realign usufruct across blockchains too, and can such a tool feasibly even exist for blockchains without necessarily violating its immutability characteristics? In relation to this idea we shall also consider a particular source of risk to a contractual cryptoeconomy (CCE) that emanates from the externalities between its different blockchain instantiations, and even between the CCE and the traditional economy based on legacy contractual mechanisms.

It is clear that Jefferson believed that successors to a contract should not be forcibly shackled to the actions of its predecessors, and that events from a time in the past should not take hostage those who create

events at a time in the future. Given the linear and immutable nature of blockchains, does a CCE not meet this standard? We shall see how an appreciation of contractual variety, and developing mechanisms for a CCE to accommodate them, suggests quite the opposite.

Jefferson understood moral hazard all too well. On placing a hard duration on contracts, he wrote in his letter:

'This would put lenders, and the borrowers also, on their guard. By reducing too, the faculty of borrowing within its natural limits, it would bridle the spirit of war, to which too free a course has been procured by the inattention of money lenders to this law of nature, that succeeding generations are not responsible for the preceding.' [1]

His thinking inspires considering the following broader question: Do all contracts have some notion of a natural life in common? Perhaps more generally: What is the foundational role of time in transactions and contracts? Is it to provide an absolute and final verdict, like some digital super-precise photo-finish line in a race? Or is to serve as the permissive referee who taps an unseen wristwatch significantly, merely to encourage a dawdling participant to adopt a somewhat swifter pace of progress?

These are sweeping questions, but here we shall examine these issues more narrowly in the context of blockchains, for which a key characteristic is precisely that of the inherent immutability of transactions they enable alongside an impartial adherence to a linear process that features time-stamping as a tool to appeal to time as the ultimate impartial arbiter.

When time is connected with a sequence of transactions – say as with an uncomplicated supply chain or assembly line – the linearity of a secure blockchain can trivially be used to reliably and usefully bolster the operations with verifiability. However, a large swath of research in economics examines the myriad of situations where such linearity isn't quite so obvious. Often sequential investments are not fully specifiable ex ante, which is to say that there is no obvious chain to follow for contracting parties. In several cases such incompleteness is actually desirable to both parties in a contract, for example when the nature of incompleteness is itself a basis for setting expectations yet leaving room for creativity around a shared goal. And, frequently, the sequence should become terminable ex post to protect the value of an investment, as in cases where recontracting becomes necessary; in such cases, the prospect of recontracting limits the ability of the inefficient ex post allocation to endure.[i]

For blockchains to be a genuinely useful tool for contracting – and actualize a CCE – would seem then to depend not merely on their ability to serve as the proverbially dispassionate 'arrow of time', but also to enable guiding such an arrow's direction tractably when a contractual application requires it. This is to say that a CCE needs an 'economic arrow of time' that appeals to time as the arbiter, but in a manner better suited to maximizing contractual usufruct.

2. The Contractual Cryptoeconomy

While constitutions, transnational pacts, purchase agreements and employment contracts can all be seen as forms of 'contracts', they have several obvious and several subtle differences that justify their examination within the purlieus of separate fields of study. Indeed, whether a constitution can be considered a (social) contract in any real and useful sense is hardly an uncontentious idea. [2] provides several useful references and a general discussion, and, interestingly, also considers their applicability within the context of piratical constitutional contracts. See, also, [3].

Economists, for example, have long studied the difference between a complete contract and an incomplete contract. The incompleteness stems from the fact that a vast majority of contracts in the real world cannot be made fully contingent on a specifiable state of the world. Smart contracts, by contrast, are premised on fully specifiable states of the world and are, in this respect, an interesting example of complete contracts. For incomplete contracts, moral hazard is a prime motivator. In other words, incomplete contracts focus on ownership of productive assets because their use can often not be fully specified ex ante, nor can it frequently be monitored. It has been argued that such incomplete contracts could, in theory, be made equivalent to complete contracts provided only that the parties are averse to risk and we assume that they can at least provide a probability distribution for future outcomes, even if they cannot predict exact features of the possible future states of the world. This works, provided we have access to an incentive compatible mechanism that motivates the parties to declare the state that does eventuate truthfully. [4]

It is not, therefore, hard to understand why incomplete contracts are ubiquitous in the real world. For a discussion of the difference between complete and incomplete contracts in the context of blockchains, see [5], [6] and [7].

Abstracting from differences between the variety of applications of contracts and their broad types, here we wish to focus thought on an essential similarity observed by the third president: the idea of a natural life. Time – its duration; its ability to be reset; its impending horizon – is central to all contracts, and it is this shared basis of a 'progression across a series

of transactions', each linked in some direct or indirect manner to time, that makes their association with blockchains an interesting subject to consider.

2.1 Internalizing Arbiter Rent

Blockchains operate on the essential principle of time-stamping a batch of transactions and permit the possibility of doing so immutably, verifiably and in a decentralized manner; crucially, depending on features of their particular instantiation, the degree to which these features are secured from sabotage varies. This lends them to be particularly useful for at least two functions: providing a reliable infrastructure for broadly accessible capital markets and serving as a basis for reifying and securing property rights.

It has long been recognized in the development literature that a government's ability has to credibly secure property rights and encourage well-functioning financial markets are key to its capacity to signal its commitment to private-sector investment, especially of the variety that is accretive to longer-term growth. (See, as examples, [8] and [9].)

Between these two functions, there is little doubt that weak property rights do more insidious damage to growth prospects than weak financial markets. [10] However, it has been shown time and again that the temptation for governments to spurn this advice and turn to rapacious rent-seeking activities remains a real threat to stunting economic growth and development prospects. On this point, [11] is particularly convincing.

This broader observation is important for the context of contracts, since third-party arbitration is key not just to a contract's enforceability but to the overall set of contracts that can eventuate in an economy. This function of arbitration, enforcement and verification that governments provide – primarily through their legal code and system of courts – yields them valuable economic rent, which we can see as 'arbiter rent'.

For a contractual space based on blockchains, however, the economic value that is represented by the arbiter rent is internalized within the same system that employs actors on the decentralized network to function as independent and neutral verifiers. Traditional arbiter rent, in this broad sense at least, is reimagined by blockchains. It is retained within the transactional parameters defined by the contractual space a blockchain's design implements. It is not, however, retained entirely within a given contract directly.

To see this point, contrast the contracts that rely on third-party verification provided by institutions with those contracts that entirely dispose of them, operating purely on the basis of trust between parties.
When third-party arbitration is essential, the general institutional quality (see, for example, [12]) and the reliability and efficiency of courts (as argued in [13]) becomes paramount to the extent that a contract can generate surplus. The potential for regulatory distortions resulting in higher arbiter rent and lower contractual surplus for the participants looms large over the market.

Since institutions also provide the broader context to societal trust, or 'social capital' between contracting agents, it is hard to separate the effects of each. However, it has been shown that, even controlling for such endogeneity, social capital still plays a very strong role in enabling beneficial contracts; [14] provides a discussion on the relative role that social capital plays in financial contracts in the context of southern versus northern Italy. Frequently such trust-based contracts are used by those who would otherwise be priced out of any feasible arbiter-enforced contract for a service that entails some form of direct or indirect arbiter rent. As such, 'trust' provides a useful social benefit for contracting.

More generally, the ability to remove the extractive influence of arbiter rent reduces the inframarginal cost and enables greater contractual surplus.

The trouble, of course, is that contracts that are strongly reliant on trust can only operate within the narrow swath of applications where prosocial behaviours and norms among the participants are socially embedded, which is to say, ordinarily only within extended families and smaller communities. [15] proposes a modelling framework to see the role of social capital for informal contractual enforcement in a network. The network connections themselves serve as a collateral that can be used for borrowing between participants in the network.

Contracts that are enabled by blockchains derive their basis from a third source. Neither do they directly rely on social capital – derived from interpersonal trust – nor do they need institutions that provide third-party verification and arbitration – premised upon state sanction. Instead, they replace both with a system based on a consensus protocol for their users that requires no intrinsic trust among its participants, but that creates a reliable contractual space where transactions can be made strongly verifiable.

Contracts operating on a blockchain are designed to internalize the arbiter rent, thereby creating a dedicated economic space – the 'contractual cryptoeconomy' – which is more broadly accessible than those contracts that rely entirely on social capital and less costly than those that rely on third-party arbitration.
Naturally, this is the macro-view for a theoretical motivation for the CCE. In practice, there are significant problems that make it unclear whether a

CCE can indeed satisfactorily accommodate all other forms of contracts.

Consider, for example, that competing blockchain applications can be built ad nauseam without any costless manner to distinguish between their relative quality of implementation ex ante. Centralized third-party arbitration mechanisms, on the other hand, are usually maintained under a system that grants monopoly power over the arbiter's function to the state that defines the contract's jurisdiction. In theory, such proliferation can curtail the extent of the internalization of arbiter rent. Contractual surplus faces the risk of being dissipated when contracts are allocated inefficiently between the legacy contractual environment based on courts as the ultimate third-party arbiter and the contractual blockchain economy. On the other hand, proliferation might also generate positive externalities for the CCE. Much depends on whether we can make variegated blockchain implementations compatible and convergent to theoretical ideals of a contracting platform: interoperability between blockchains certainly permits such compatibility in a technical sense, though it only characterizes a fraction of all feasible implementations of blockchains. We shall develop these points further with the help of a simple model later on.

2.2 Flexibility in Contractual Time

Since the prior description of all relevant states that may affect a contract is either infeasible or impractically expensive, contracts are routinely left incomplete, without fully state-contingent clauses. Incompleteness in contracts may exist for other reasons as well, some of which are unavoidable and some deliberate.

Consider the case of a bilateral externality, for example, where the parties engage in a contract without prior information on the size of the externality that might be generated by the scale of the primary activity that one of the relevant parties engages in, and can therefore not effectively set appropriate terms. [16] Conversely, consider the case of crafting a contract to optimize on the choice of providing contractual flexibility in the terms of the contract ex ante as opposed to making them more rigid. With flexible terms established ex ante, the parties have more freedom to adjust their behavior ex post, once they have better information on how to make the division of surplus more agreeable to both parties. At the cost of some loss of control, flexibility in contractual terms can incentivize creativity, make individual initiative more likely to affect surplus, motivate the selection of more suitable projects, and so forth. This suggests that there may be a strong role for deliberate incompleteness in contracts as a tool to set the expectations for the parties involved. [17] Smart contracts, in such cases, would obviously be suboptimal.

Given the large variety of contracts in the real world that are best described as incomplete, it is worth considering the Jeffersonian idea of deliberate recontracting (in other words, the proviso of a horizon for contracts) for the particular context of contractual implementations on a blockchain.

Blockchains have potential as a theoretical construct for recreating consensual outcomes across a decentralized market structure to leverage the value that is inherent in aggregating distributed information efficiently. For economics this is nothing short of revolutionary, for the very obvious reason that we can now imagine a third alternative to the dichotomy that underpins the 'market versus organization' dilemma (or firms versus institutions) that [18] outlined. Blockchains permit market orderings for value-generation that suspend both the invisible hand of the price mechanism of markets and the direct guiding hand of hierarchies in organizations; [19] terms this third mechanism a 'cryptographic stigmergy'.

The fact that they are immutable, time-dependent databases that can be made exceedingly censorship resistant makes the market and social orderings that public blockchains enable especially durable. However, blockchains are not amenable to providing nuanced consideration of incentives and are, as a consequence, less suitable for tackling contractual complexity that such orderings must routinely grapple with. In this respect, scaling solutions for blockchains that introduce layers upon a foundational blockchain consensus protocol, and then erect a network upon it that can flexibly represent nuance that contractual incentives contain are noteworthy.

Consider the idea of a hashed time-locked contract (HTLC), which illustrates the connection between providing some degree of control over time and the types of contracts that it makes possible. An HTLC is a particular kind of smart contract that has been developed for the scalable transactional layer – the Lightning Network – built on top of the underlying Bitcoin blockchain[ii]. [20] The Lightning Network enables the creation of task-specific payment channels off-chain that permit the aggregation of several transactions that can be mapped onto fewer transactions on the base layer, thereby lowering the average transactional cost. In the limit, only two transactions on the more expensive and slower base layer suffice for a multitude of transactions on any given payment channel: the initial transaction that funds the payment channel shared by two or more agents in a 'multisig' account, and a final transaction that updates the status of accounts after the payment channel is closed off. This effectively loosens the dependency of a multi-transactional contractual relationship on the immutable time-stamping feature of the underlying Bitcoin blockchain. Transactions proceed by a process

of sequential consensus over mutually preferred states that, once agreed to, simultaneously also invalidate deprecated states by instituting a penalty comprising the loss of all staked funds should the previous state be surreptitiously used to close off the payment channel and published to the blockchain.

The network aspect of the Lightning Network permits several 'hops' across any of its nodes with open payment channels. This allows any participant to effect payments to anyone else on the network much more swiftly and cost-effectively than is possible with the base Bitcoin layer. Moreover, the open nature of the network creates a contestable market for transactions. This is important since it ensures that competitive market pressures influence the terms of all new contracts, and the terms that pertain to the division of the surplus that the contract can entail.

For our context, these developments are significant for two compelling reasons.

First, more specifically, HTLCs make the significance of a natural expiry for a contract in eliciting efficient contractual investments clearer to apprehend. An HTLC operates by first creating the hash of a secret. The secret must be revealed by the recipient in order to access some funds at stake. If the hash is kept private, we have a more constrained and state-contingent contract between a buyer and a seller. If the hash is made public, we can then imagine a tournament between a buyer and a pool of sellers who competitively exert efforts to discover the secret. An HTLC also involves an interplay between a definite time at which the contract expires and the ability to adjust the terms of the contract to the demands of a specific context by decrementing this duration sequentially. An HTLC, therefore, places emphasis on publicly specifying a 'fixed duration' before the contract's outcome becomes inviolably published to the Bitcoin blockchain, thereby ending the contract and forcing a reset.

While this reset afforded by the base layer is Jeffersonian in spirit, the HTLC permits context to provide variability in the duration itself. This is because an HTLC also features a method to introduce a 'flexible horizon' as a method to motivate and negotiate efforts that help generate contractual usufruct in the shadow of the Bitcoin blockchain. As such, HTLCs are designed and can be developed further to capture a broader swath of contracts in practice.

Second, and more broadly, note that the Lightning Network could, in theory, permit defining any arbitrary architecture for some given contractual mechanism as a subgraph of its overall network structure. In particular, it becomes feasible to specify not just any set of nodes that are involved within a transaction, but also the order in which they are involved from the time it is initiated to the time it is completed. Therefore, HTLCs can be seen as an organic and dynamic method to define a nexus of contracts that determines the boundary of a traditional firm, and it uses the underlying Bitcoin blockchain as the third-party arbiter for a wider set of contracts that inhere to traditional firms.

While this setup seems to have effectively created the precursors to decentralizing a firm on a scaling solution for blockchains, it remains far from certain that it rings in the demise of traditional firms. Issues pertaining to residual control over productive and complementary assets, management of teams, the assumption of risks, the delegation of authority across agents, and so forth are complex contractual issues that will require further developments, very likely relying on a suite of suitable technologies working seamlessly to integrate not just blockchains, but other types of ledger technologies as well.

3. The Economic Arrow of Time

The prospective role of time-stamping processes that can then be marched immutably through time looms large over applications that are considered for blockchains. There is something attractive about relying on time as an arbiter.

Of course, this view is rather limiting in its capacity for the nuanced insight needed for dealing with contractual variety in the real world. It is indeed true that some physical processes feature an 'arrow of time': closed systems with increasing entropy concretely indicate an irreversible and directional arrow through time. Most famous among these is the thermodynamic arrow of time implied by the Second Law of Thermodynamics. Other processes, however, are characterized by a 'time-reversal invariance', in that they do permit possibilities for a reversal of the process. [21] It is, therefore, even at a rather general level, infeasible to rely on the inviolability of some implied arrow of time as the essential shared foundation for real world applications. In the context of blockchains, while the law is routinely taken to unleash the value of transactional immutability, it can very well also be taken to suggest the level of difficulty required to successfully sabotage precisely that feature.

For instance, a supply chain, from initial input to final output, may appear to represent a process very conducive to the arrow of time analogy. Yet, the value of any such arrow shrinks markedly when we are interested in more than merely describing the process of sequentially linking units into a chain. By concentrating emphasis on the curation of information, a supply chain on a blockchain sets aside several interesting and important contractual issues, implicitly assuming that they can all be considered complete.[iii] This delimits the usefulness of blockchains by relegating a host of

incomplete contractual transformations that affect the potential usufruct of the supply chain. By contrast, when we begin to consider aspects of the various contracts that exist between entities on a supply chain, the emphasis shifts from one of an inexorable and rigid arrow of time, to one that can be guided – perhaps better seen to be a distinct 'economic arrow of time'.

In a standard contract in economics (where the principal is risk neutral and the agent is risk averse) the prospect of renegotiating a contract serves to give the contract precisely this characteristic of time-reversal invariance. When an agent must select costly effort that is unobservable by the principal over the course of a contract and, simultaneously, must also commit to not renegotiating, she exposes herself to a degree of risk. To elicit the optimal level of effort through any form of assurance of a payoff that corresponds with the higher-level of effort, the principal would need to distinguish between agents who would select suboptimal levels of effort from those who select the optimal level; instantly, we shift the focus of the problem to one of resolving adverse selection rather than a strict sequential progression through the contractual parameters.

3.2 Aspects of time

Contracts that feature degrees of state dependency and propensities for renegotiation underscore the relevance of two aspects of time that are related but subtly different in their effects: 'timing' and 'duration'.

It is broadly understood that timing is integral to the very rationale for a range of contracts. The sequence and ordering of investment decisions that are stipulated by a contract can determine the amount of contractual surplus generated. One of the key messages of transaction cost economics is that timing is key to ameliorating a variety of opportunistic behaviors that are inspired by appropriable quasi-rents; timing is, indeed, central to motivating efficient investments, reducing a range of social externalities and, of course, in setting the overall boundaries of a firm with respect to the market. A key difference between a simple state-dependent smart contract and an HTLC is that the latter permits a method to algorithmically delimit the appropriable quasi-rents involved in a contract.

Contracts can also vary widely in their duration. Constitutions usually have far more enduring lives while several securities contracts can have extremely short lives. Thus, a provision for flexibility over both aspects of time that affect the contractual horizon is both necessary and appropriate for any generic contractual template.
The idea of a contractual duration has been examined at some length in the literature. [22] and [23], for example, suggest that, broadly, contract length depends on the level of uncertainty the investment represents and the cost of renegotiation. Short-term contracts with the option of renegotiation have been contrasted with longer-term contracts. For example, [24] suggests that, in the absence of a commitment to refrain from renegotiation, a buyer and seller will prefer engaging in a sequence of short-term contracts. (See also [25], which contains useful references.) [26] demonstrates the efficiency of short-term contracts over the long run and [27] suggests that even spot contracts can be efficient when inter-temporal smoothing concerns are not a consideration.

Concerns with sequential short-term contracts arise when pertinent information over incentives and behaviour is revealed asymmetrically and in a manner that is correlated over time so that bargaining power shifts squarely towards one party to the detriment of the other. Here, smart contracts that also strongly guarantee anonymity of the participants ex ante would incentivize undertaking a sequence of shorter-horizon contracts, thereby avoiding introducing undesirable divisions of surplus owing to the asymmetric revelation of private knowledge. [28] develops a class of contracts for the Lightning Network, called 'discreet log contracts', that provide anonymity as a feature while also reducing the scope of malfeasance by the third-party nodes that act as intermediaries.

3.2 Phases in a contract's natural life

Regardless of the nuance over aspects of time within a contract's natural life, most contracts are usually seen dichotomously – a contract either exists or it does not, whether in prospect or in fact, and whether it is tacit or explicit. However, consider that most contracts exist within contextual environments that impinge upon them and lead them through 'states' of validities over the duration of their existence. Generally, we can call these states of a contract over its natural life its 'phases' and enumerate at least three: acceptability, vulnerability and termination.

Quite simply, when an extant contract accords with the intention of its participants it can be said to have acceptable validity; when, over its life, it is susceptible to being either terminated or unacceptable (at risk of renegotiation) then it can be said to have a vulnerable validity. The contract's natural life can thus be parsed into phases that describe stages of its existence, and we can subsequently consider the transitions of the contract through these phases over its duration.

While fluid transitions between phases that might exist within a contract are not explicitly considered in the literature, the general issue is recognized as one that is significant in its social welfare implications. For instance, [29], which focuses on contrasting ex ante dispute resolution arrangements with ex post dispute

resolution; while ex ante arrangements enhance joint surplus, they tend not to be legally enforced.

Our consideration of a contract's natural life here is not meant as a sensationalist departure from the literature on contracts, but to draw attention to the fact that several aspects of a contract, such as its prospect for renegotiation, uncertainty, moral hazard, and adverse selection, can usefully be seen as being internal to the contract and manifested as transitions across its phases. HTLCs provide a very promising first step towards resolving such issues for contracts on the blockchain, but they are hardly flexible enough to accommodate complex transactions, multi-layered contracts, complicated property rights, and a host of other issues.

Contracts are often generic templates. They might be drawn up to be applicable across a multitude of transactions, with only limited consideration for specific circumstances, or they might be drawn up and made inviolable through the passage of time or across its applications in a given period. Several examples can be offered in support of this observation of a social, political and economic nature: primogeniture, constitutions and union-negotiated employment contracts, for instance, are contracts that, perforce, do not specify all feasible states explicitly, but their incompleteness for a particular context or contingency (intentionally or not) completely defines their phases. This restates the result in [25], but for a different reason: there the observation is that incompleteness on account of transaction costs need not be relevant so long as payoffs are known. Here, incompleteness can never be entirely eradicated even if payoffs are known so long as parties to a contract 'care' about the transitions of the contract over its phases in its duration, and that the phases are finite and foreseen. It is, of course, feasible that the phases in the duration are a mechanism relevant to the contracting parties since it retrieves information relevant for payoffs.

4. Externalities in a CCE

Recall that [18] argued that there is an inherent 'cost to discover market prices,' and that firms are motivated by the ability to suspend using the price mechanism of the market to coordinate production, permitting the firm's manager instead to direct the coordination of resources. Similarly, a blockchain can be seen as a 'Coasian exchange': Participants are brought together through an ecosystem that acts as a mechanism for the coordination of activities organically, and which is motivated by the 'cost of discovery for the market value of consensus'.

Arguably, the Lightning Network, as a second-layer scaling solution for Bitcoin, can be seen as an effort to encourage the Coasian exchange dynamics of the underlying layer by undertaking an 'intervention' to ameliorate the negative externalities from congestion on the base layer.

Intrinsic to these relative costs of discovery (those for the market prices versus those for the market value of consensus) are several externalities, positive and negative, that a contractual blockchain economy represents relative to the traditional economy.[iv] These externalities may inhere in the social resource costs for securing a blockchain implementation's consensus protocol. They may arise from the information costs imposed by implementations of blockchains with less desirable characteristics or the lack of interoperability between the more desirable ones.[v] They may even pertain to the developments upon it that alter its value proposition.

There is a broad source of externalities that the regulation of cryptocurrencies imposes upon this relative cost consideration. Broadly, this source inheres to the difference between the market for ideas as opposed to the market for goods. Externalities are a common basis for excessive regulatory intervention in the market for goods, especially when contrasted with a reluctance to apply similar regulatory predispositions in the market of ideas. It was Coase again ([30] and [31]) who articulated why a definitive treatment of this issue was essential to any real consideration of externalities affecting production in markets. The notion, frequently heard, that software ought to be treated by the government as speech makes this point quite clear.

4.1 A traditional modeling framework on realigning externalities

Let us briefly consider this issue of externalities as they pertain to participation in the CCE. We use a simple framework that should be instantly familiar to students of public economics.

We might imagine that the economy comprises some secure blockchain υ with a market price of p^{υ}, and other blockchain instantiations conducive to hosting contracts. We can think of this ecosystem collectively as our contractual blockchain economy, Υ.

The point is to imagine a scenario where participation in υ provides a net external value to other participants across Υ, and that it is only partially accounted for by the participants within the secure blockchain. To capture the idea that other participants in the blockchain economy experience varying degrees of externality effects from υ, the nature of which can also be multidimensional, we only need assume that the joint probability distribution $P(V,E)$ is known to all who participate in Υ, where participation in Υ yields a private benefit of V to the individual and, simultaneously, it

inspires a net positive externality of value, E. In terms of our Jeffersonian premise, E can be seen to represent that part of the contractual usufructs in υ that are not directly internalized by its participants.

It is useful to see why this joint probability distribution would make sense for ϒ. Information is inherently distributed, and so the secured and decentralized economic orderings enabled by υ entails more of a gain to those who are more marginalized by any of the distributively inefficient economic orderings that are more centralized and less secure than υ.[vi]

To fix ideas further, let us capture the social marginal cost that the security of υ entails on the ϒ ecosystem with s. This permits us to define a net social gain in the blockchain-enabled economic system; for an individual in ϒ, participation in υ yields a net social gain of $\kappa=(V+E-s)$.

All new entrants to ϒ face p^{ν} for access to the most secure blockchain. Naturally, if p^{ν} exceeds the entrant's reservation price she does not participate in υ. As such, a recognition of the presence of the net positive externality makes it advantageous for ϒ to institute a method to provide a social subsidy for all entrants to υ. In the case of the secure blockchain, the magnitude of this 'subsidy' can be seen as the social resource cost, R, of securing υ, and it can be written as

$$R = \int_{p^{\nu}} \int_{0} \kappa(P(V,E))dV\,dE\,,$$

where the value that a participant receives begins at p^{ν} without an upper bound whereas the externality from a given participant ranges from zero without an upper bound.

If ϒ were to efficiently select a price for υ we would have:

$$\partial R/\partial p\upsilon = -\int_{0} \kappa(P(V,E))dE = 0.$$

This suggests that the efficient price for υ is

$$\widetilde{p^{\nu}} = \alpha\left(E/_{\widetilde{p^{\nu}}}\right) - s,$$

where $\alpha\left(E/_{\widetilde{p^{\nu}}}\right)$ represents the average externalities applicable at the efficient price; thus, the social marginal cost is equal to the social marginal gain.

In words, even an efficient price consideration for υ can do no better than lump in relevant nuances in average externalities. Those in ϒ for whom the private benefit and net externality is below the social marginal cost participate in υ (V is higher than $\widetilde{p^{\nu}}$); those for whom it is higher do not participate (V is lower than $\widetilde{p^{\nu}}$. This is undesirable, of course, because the former comprises the group of participants in υ who create fewer net positive ϒ-wide externalities and the latter group would have been participants who would be more likely to generate such positive externalities to ϒ.

It is quite obvious that any ability to price discriminate between these groups would be an immediate source for an increase in the net social externality gain from market outcomes.

In our context we can imagine higher layers on the secure blockchain υ to concern themselves with increasing the transaction throughput of υ's base settlement layer. This naturally serves as a screening mechanism between those participants who are interested in the security and immutability of the value of the data on υ through time and those who are interested, more proximately, with securing frequent transactions at low cost, which we can capture with the variable ς.

This latter group would then have a joint probability distribution of $P^{\varsigma}(V,E)$, whereas and the former group would have $(P^{\varsigma})\tilde{}(V,E)$. The social resource cost, R, of securing υ, now becomes

$$R = \int_{p^{\nu}} \int_{0} \kappa\widehat{P^{\varsigma}}(V,E).\,dV\,dE + \int_{p^{\nu}} \int_{0} \kappa(P^{\varsigma}(V,E))dV\,dE$$

With the cost of access to the higher transactional layer as l, the efficient price for participants solely in the settlement layer abides the same condition:

$$\widetilde{p^{\nu}} = \alpha(E/\widetilde{p^{\nu}}) - s$$

whereas, for the groups on the transactional layer, the price abides:

$$s + l = \widetilde{p^{\nu}_{\varsigma}} + \alpha_{\varsigma}(E/\widetilde{p^{\nu}})\,.$$

The price for the group participating in the transactional layer is lower than that for the group on the base layer and the net positive externalities are higher through discrimination. Specifically, the ability to sort the participants in this manner permits participation in the base layer to exclude those for whom E was lower but V was higher, and include them in the transactional layer instead.

There is a technical limit for the number of transactional layers that are likely to be built on υ as well as a practical limit on the need for such layers. At a general level, this causes a degree of pooling of the participants across the two groups and creates limits to the ratcheting effect that curators of such layers might develop merely to price discriminate on the basis of ς more and more perfectly. See [32], who initially developed this idea in the context of a two-period incentive contract with asymmetric information on observed performance.

5. Concluding Remarks

With Jefferson's observation as the overarching impetus, we have examined the issue of a natural life for contracts as a feature they all share. Contracts do not, however, last forever, and the notion of their stability is only relevant when seen from the perspective of their vulnerability to partial failure; in other words, how contracts behave over the course of their entire life deserves attention. Blockchains draw attention to this overarching fact. They hold the potential to develop a platform, with features of a Coasian exchange, that permits the use of an economic arrow of time that can accommodate a genuine contractual blockchain economy.

The Jeffersonian standpoint of favouring the living is an acknowledgment[vii] that the contractual enabling of the usufruct is premised upon a period that comes to a close. Logically, this period can be examined as a duration with a definite commencement and expiration, but with varying states of validity as economic rent from a relationship varies over the course of the duration of the contract; the contract then can be seen to have conditional probabilities for these validities over its duration. When contractual usufruct is lost through the course of a contract's natural life, the Jeffersonian solution of recontracting makes patent sense. However, when an economic arrow of time can be appealed to that can service complete as well as incomplete contracts, recontracting does not have to be the default solution. The linear transformations that blockchains accommodate so well provide a strong basis for contractual mechanism design; the organic networks that fluidly emerge from the evolving patterns of contractual usufructs that higher-layer scaling solutions provide suggest that a much wider variety of incomplete contracts can be accommodated as well. Together this gives us a strong basis for a contractual blockchain economy.

Admittedly there is a long way to go before the contractual blockchain economy can be seen as a real alternative – indeed, one that is to be preferred in an era of technologies that favor distributed information – to the traditional economy. However, the fact that several of the necessary components exist in theory and practice even today is a real source for optimism.

References:

[1] T. Jefferson "Letter to James Madison", The Founders' Constitution, vol. 1, chapter 2, document 23, University of Chicago Press. http://press-pubs.uchicago.edu/founders/documents/v1ch2s23. Html, 1789.

[2] P.T. Leeson, "The Calculus of Piratical Consent: The Myth of the Myth of Social Contract", Public Choice, vol. 139, no. 3/4, pp. 443-459, 2009.

[3] D.D. Heckathorn and S.M. Maser "Bargaining and Constitutional Contracts", American Journal of Political Science, vol. 31, no. 1, pp. 142-168, 1987.

[4] E. Maskin and J. Tirole, "Unforeseen Contingencies and Incomplete Contracts", Review of Economic Studies, vol. 66, no. 1 (special issue on contracts), pp. 83-114, 1999.

[5] P. Goorha, "Blockchains as Implementable Mechanisms: Crypto-Ricardian Rent and a Crypto-Coase Theorem", Journal of the British Blockchain Association, Volume 1, Issue 2, Available: 10.31585/jbba-1-2-(4)2018., 2018a.

[6] P. Goorha, "A Comprehensive Contracting Solution Using Blockchains," SSRN Working Paper, Available: http://dx.doi.org/10.2139/ssrn.3237076 , 2018b.

[7] J.S. Gans (2019) 'The Fine Print in Smart Contracts,' SSRN Working Paper, Available: http://dx.doi.org/10.2139/ssrn.3309709, 2019.

[8] D. North, Institutions, Institutional Change and Economic Performance, Cambridge University Press, 1990.

[9] D. Rodrik, "Promises, Promises: Credible Policy Reform via Signalling", The Economic Journal, vol. 99, no. 397, pp. 756–772, 1989.

[10] S. Johnson, J. McMillan and C. Woodruff, "Property Rights and Finance", American Economic Review, vol. 92, no. 5, pp. 1335–1356, 2002.

[11] A. Shleifer and R. Vishny, The Grabbing Hand: Government Pathologies and Their Cures, Harvard University Press, 2002.

[12] D. Acemoglu, D. and S. Johnson "Unbundling Institutions", The Journal of Political Economy, vol., no. 5, pp. 949-995, 2005.

[13] A. Shleifer, "Efficient Regulation", Regulation vs. Litigation, ed. Daniel Kessler, NBER and University of Chicago Press, pp. 27-43, 2010.

[14] L. Guiso, P. Sapienza and L. Zingales, "The Role of Social Capital in Financial Development", The American Economic Review, vol. 94, no. 3, pp. 526-556, 2004.

[15] D. Karlan, M. Mobius, T. Rosenblat and A. Szeidl, "Trust and Social Collateral", Quarterly Journal of Economics, vol. 124, no. 3, pp. 1307-361, 2009.

[16] R. Pitchford and C.M. Snyder, "Coming to the Nuisance: An Economic Analysis from an Incomplete Contracts Perspective", Journal of Law, Economics and Organization, vol. 19, pp. 491-516, 2003.

[17] O. Hart and J. Moore, "Contracts as Reference Points", Quarterly Journal of Economics, vol. 123, pp. 1-48, 2008.

[18] R.H. Coase, "The Nature of the Firm", Economica, vol. 4, pp. 386-405, 1937.

[19] P. Goorha, "The Return of 'The Nature of the Firm': The Role of the Blockchain", Journal of the British Blockchain Association, volume 1, no. 1, Available: 10.31585/jbba-1-1-(2)2018, 2018c.

[20] J. Poon and T. Dryja "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", Available: https://lightning.network/lightning-network-paper.pdf, 2016.

[21] B. Roberts, "When We Do (and Do Not) Have a Classical Arrow of Time", Philosophy of Science, vol. 80, no. 5, pp. 1112-1124, 2013.

[22] J. Gray, "On Indexation and Contract Length", Journal of Political Economy, vol. 86, no. 1, pp. 1-18, 1978.

[23] S. B. Vroman, "Inflation Uncertainty and Contract Duration", Review of Economics and Statistics, vol. 71, no. 4, pp. 677-681, 1989.

[24] O. Hart and J. Tirole "Contract Renegotiation and Coasian Dynamics", Review of Economic Studies, vol. 55, no. 4, pp. 509-540, 1988.

[25] M. Dewatripont, "Renegotiation and Information Revelation over Time: The Case of Optimal Labor Contracts", Quarterly Journal of Economics, vol. 104, no. 3, pp. 589–619, 1989.

[26] P. Rey and B. Salanie, "Long-Term, Short-Term and Renegotiation: On the Value of Commitment in Contracting", Econometrica, vol. 58, pp. 597-619, 1990.

[27] D. Fudenberg, B. Holmstrom, and P. Milgrom "Short-term Contracts and Long-Term Agency Relationships", Journal of Economic Theory, vol. 51, pp. 1-31, 1990.

[28] T. Dryja, "Discreet Log Contracts", undated working paper, MIT Digital Currency Initiative, last accessed: February, 2019.

[29] S. Shavell, "Alternative Dispute Resolution: An Economic Analysis", Journal of Legal Studies, vol. 24, no. 1, pp. 1–28, 1995.

[30] R.H. Coase, "The Market for Goods and the Market for Ideas", American Economic Review, vol.64, no. 2, pp. 384–391, 1974.

[31] R.H. Coase, "Advertising and Free Speech", The Journal of Legal Studies, vol. 6, no. 1, pp. 1-34, 1977.

[32] J. Laffont and J. Tirole "The Dynamics of Incentive Contracts", Econometrica, vol. 56, no. 5, pp. 1153–1175, 1988.

[i] Note that, when such inefficiencies are the source of rent for one of the parties in a contract, recontracting is undesirable to her, even if recontracting may lead to a Pareto improvement for the contract.

[ii] Recall that the base layer of Bitcoin was the first blockchain application and was created with the intention to serve as a digital payment system for networks that obviated the need for third-party intermediation. Bitcoin secures its transactions through the use of a consensus algorithm based on the idea of incontestable proof of work done; it is operationalized by nodes on the network called miners who must invest in costly dedicated computer hardware and energy to competitively solve cryptographic puzzles in order to earn the right to batch transactions into a block that then gets appended to the Bitcoin blockchain. This provides the miner a payoff comprising a fixed number of bitcoins and a smaller variable transaction fee, while enabling all participants on the network to verify the accuracy of the overall ledger of transactions independently.

[iii] For instance, along each stage of a supply chain that features a typical two-sided market, incentives provided by the reference platform linking both sides of the market may well change.

[iv] Naturally, there are several externalities that pertain to the mechanisms of a given blockchain implementation as well. These may include externalities imposed by the activities of a single node that affects the entire network, such as when it engages in transactions that increase the latency across the entire network and ties up a disproportionate share of resources. However, we are more interested here in considering externalities directly relevant to the broader contractual blockchain economy.

[v] A key benefit of contracts on interoperable blockchains is in reducing the costs of complexity in describing outcomes that pertain to a contract. For example, the nature of investments that parties make at time 2, once the contract has been put into operation at time 1, is often seen as being sufficiently complex to make them effectively beyond being independently verified by any third-party, such as a court. Blockchain interoperability can assuage this concern by folding in more and more aspects of an incomplete contract within the ambit of what can be feasibly verified publicly by a 'trusted third-party'. Such aspects can pertain to the nature of the investments, but also to the realized state of the world ex post.

[vi] Mutatis mutandis, this can be seen to extend beyond the contractual blockchain economy to the traditional economy as well.

[vii] The author readily admits that Jefferson's observation

was more profound than what is made of it for the purpose of this paper!

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
None declared.

Photo by Swapnil Bapat on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(3)2019

Singapore's Open Digital Token Offering Embrace: Context & Consequences

Robert W. Greene[1], David Lee Kuo Chuen[1,2]
[1]Singapore University of Social Sciences, Singapore
[2]Stanford University Distributed Trust Initiative, USA
Correspondence: rwg1819@gmail.com
Received: 17 May 2019 **Accepted:** 4 June 2019 **Published:** 28 June 2019

Abstract

The overall global public's ability to purchase some portion of a digital token project's initial batch of tokens is the defining feature of an open digital token offering. Using a dataset that differentiates this token distribution model from other varieties – a distinction often underemphasised in regional analyses of digital token sale trends – this research estimates 2017-18 open digital token offering activity by jurisdiction, finding that Singapore-registered projects accounted for 21 percent of Q3/Q4 2018 dollar-volume, more than any other country. Conversely, by late 2018, previous hubs of this distribution model represented a much smaller share. Reasons for Singapore's rise as a global hub of the open digital token offering are explored, with a particular focus on examining contrasting regulatory approaches to distinguishing between this token distribution model and traditional securities offerings. Notably, 11 percent of Singapore-registered Q3/Q4 2018 token offering dollar-volume was purely-private, versus 94 percent in the U.S. Policy considerations related to this distribution method and the open digital token offering are presented, as are contrasting outcomes: this research estimates that over 70 percent of Singapore's one-to-two-year-old open token offerings resulted in operational networks or minimum-viable-products, versus fewer than 40 percent of U.S. private sales. Also, about 40 percent of smart contract platform projects that conducted 2017-18 token sales were Singapore-registered – many more than in any other country. For reasons explored in this research, these findings support the view that open digital token offerings benefit projects aiming to concurrently raise funds, build up a user-base, and incentivise technologists to contribute to project development. Moreover, risks to retail participants posed by this distribution method are manageable. Singapore's policy approach towards open digital token offerings has benefited the Lion City, which was likely home to more digital token projects that conducted 2018 token sales than any other city in the world.

Keywords: *Arbiter Rent; Contracts; Duration; HTLCs; Blockchains; Thomas Jefferson; Economic Arrow of Time; Coasian exchange; Contractual Cryptoeconomy*

JEL Classifications: *G18, G28, F39, K20, K22, K23, O16, O38*

1. Introduction

Last year, the dollar-volume of digital token distributions eclipsed the value of initial public offerings within a developed economy with robust capital markets infrastructure. In Singapore, the value of 2018 initial public offerings was $730 million [1], yet as this research finds, Singapore-registered 2018 digital token sales raised over $1.6 billion [2].[i] Understanding Singapore's important role within the digital token economy first necessitates understanding digital tokens. For purposes of this research, "digital tokens" are defined as "transferable units generated within a distributed network that tracks ownership of the units through the application of blockchain technology" [3]. Unlike traditional financial assets, a digital token serves as "a cryptographically-secured representation of a token-holder's rights" to perform certain functions within or receive benefits from a token network [4] [5]. In the case of virtual currencies, a type of digital token, these rights include the ability to store and exchange value within a distributed peer-to-peer payments network [4].

The initial batch of a project's digital tokens can be distributed through various approaches.[ii] For the last two years, the most popular approach, by far, has been the open digital token offering. This article defines an "open digital token offering" as occurring when a software project or business provides purchasing access to some portion of the initial supply of digital tokens associated with a project to most of the global public (some barriers to access may exist[iii]). Conversely, "private initial token sales" – an alternative form of initial token distribution –restrict outside purchases of any share of a project's first batch of tokens to only a relatively small number of participants, generally high-net-worth or institutional buyers. Funds raised via these two distribution approaches are commonly used to finance the development of a digital token project's network, platform, or services.

Section 2 presents estimates of 2017-18 regional open digital token offering trends, finding that the Cayman Islands, Singapore, Switzerland, and the U.S. were the four major hubs of "successful" 2017 open digital token offerings,[iv] but by Q3/Q4 2018, only Singapore remained a leading home to this distribution model. During the second half of 2018, purely-private digital token sales accounted for nearly all digital token offering dollar-volume in the U.S., but just 11 percent in Singapore. This contrast stems from differing regulatory approaches examined in Section 2, which help explain Singapore's role as a dominant hub of the open digital token offering.

Section 3 assesses the outcomes of Singapore's open digital token offering embrace, finding that a significantly greater share of one-to-two-year-old Singapore-registered open token offerings relative to U.S. private initial token sales resulted in operational associated networks or services. Singapore-registered token offerings also accounted for a disproportionately large share of 2018 "smart contract platform" projects (defined below). For reasons explored in Section 3, these outcomes provide support to the view that open digital token offerings are well-suited for projects aiming to use a token distribution event to concurrently fundraise, build up a project's user-base, and incentivise contributions by developer communities. Of course, operational projects are not inherently successful projects, and many may fail, so the scope and management of risks facing open digital token offering retail participants is examined with a focus on Singapore. The extent to which token projects registered in Singapore are primarily physically-based in the country is also estimated.

Section 4 concludes that the consequences of Singapore's open digital token offering embrace highlight beneficial features of this distribution model, which is well-suited for the swift development and deployment of new distributed services and networks. Singapore, likely home to more digital token projects that conducted successful 2018 token sales than any other city, stands to benefit in the years to come from its open digital token offering embrace.

2. How Policy Influenced Regional Trends in 2017-18 Open Digital Token Offerings

While the first open digital token offering took place in 2013 [5], overall token sale volume did not dramatically accelerate until 2016 and 2017 [3], after Ethereum's 2015 release. Ethereum is an open-source, decentralised platform for executing and recording "smart contracts" ("set[s] of promises, specified in digital form, including protocols within which the parties perform on these promises" [6]) [7], and as a "smart contract platform," it allows programs to be transparently appended to and run on its blockchain [8]. The late 2015 development of an open-source standard for Ethereum smart contracts [9], the "ERC-20 standard," provided best practices for coding applications that generate new types of tokens recorded on the Ethereum blockchain (tokens "run on top of Ethereum") [8]. This drove a huge increase in token offering volume [10] – roughly $12 million was raised via 2015 digital token sales; in 2016 and 2017, that figure grew to over $100 million and over $7.5 billion, respectively [3]. While a token project may eventually swap tokens running on top of Ethereum for tokens recorded and transmitted within a new network it launches [5], at least 60 percent of digital tokens with active secondary markets run on top of Ethereum [11], and many of these may be used within applications designed to permanently run on the Ethereum blockchain.

By 2017, hundreds of token projects were utilising smart contract platforms so that project supporters across the world could receive some of a project's initial batch of tokens in exchange for providing funds to the project to support its team's efforts to either build out an application or launch a new network – a process that some policymakers consider to be, under certain circumstances, an unregistered public securities offering. The disclosure, reporting, and structural requirements of a registered public securities offering, however, are quite costly [12]. Moreover, while regulators may exempt small-sized securities offerings or sales exclusively available to wealthy persons from certain public offering requirements, exemptions can lead to regulatory complications for digital token projects, as explained later. Indeed, widely-distributed digital tokens are often quite different than the equity securities historically issued via these public and private channels, which generally entitle holders to a share of distributed profits and the value of a firm, and can provide ownership rights [13].[v] One analysis of 253 digital tokens distributed from 2014 through late 2017 finds that three dominant uses are: 1) access to platform services (68 percent); 2) project governance

decisions (25 percent); and 3) payments (21 percent) [14]. Other research finds that over 75 percent of tokens distributed by projects from 2013 through early 2017 provide access to platform services and about half enable payments [5]. Given the stark differences between traditional securities and most digital tokens, applying traditional securities regulations to small projects focused on developing digital token networks can make those projects unworkable [15].

The analysis below estimates 2017-18 successful open digital token offering trends by jurisdiction using data primarily obtained through collaboration with Smith+Crown, a research and advisory consultancy. Policy factors that influenced 2017-18 trends, particularly those related to securities law, are concurrently examined, revealing external and internal forces behind Singapore's role as a hub of the open digital token offering. The Appendix sets forth the methodology used to construct this study's dataset – unlike other datasets used to analyse regional token offering trends, it distinguishes between private initial token sales and open digital token offerings as well as a token project's physical location versus the jurisdiction of legal registration for its token sale.

2.1. Switzerland, the Cayman Islands, Singapore, and the U.S.: 2017 Open Token Offering Hubs

As Figure 1[vi] shows, in 2017, Switzerland was the jurisdictional home to a larger dollar-volume share of successful open digital token offerings (24 percent)

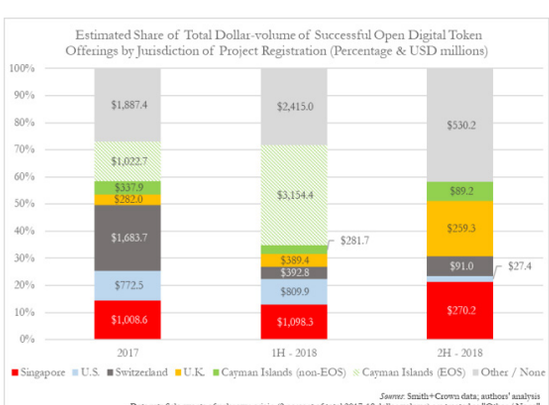


Figure 1. Unlike other jurisdictions, Singapore was a leading home of open digital token offerings during both 2017 and 2018

than any other jurisdiction in the world, followed by the Cayman Islands (19 percent, of which over 75 percent was U.S.-located EOS's token sale) [2]. Singapore and the U.S. accounted for 14 and 11 percent of total 2017 dollar-volume, respectively, and no other jurisdiction made up more than five percent [2].

In Singapore, the Securities and Futures Act's pre-existing definition of a security [16] (which in the digital token context, largely hinges on a determination of whether ownership or a security interest over the token issuer's assets exists [4] [17]) enabled many open digital token offerings to not be classified as securities offerings throughout 2017. Singapore's emergence as a hub of this distribution model was further enabled by its technologist and legal communities' proactive engagement with the Monetary Authority of Singapore ("MAS") [18] – the country's chief financial markets regulator. By August 2017, the MAS clarified that many open digital token offerings are not securities distributions [4]. In November 2017, it released guidelines providing clear examples of what token sale activities do and do not constitute a securities offering, as well as regulatory responsibilities of a digital token project [19].[vii]

In 2017, the regulatory posture towards open token offerings in the U.S., Switzerland, and the Cayman Islands was relatively less proactive. U.S. Securities and Exchange Commission ("SEC") 2017 enforcement actions provided some insights into circumstances under which the agency will, by applying an ambiguous multi-pronged legal test,[viii] view open digital token offerings to constitute securities distributions, but activity to clarify the regulatory status of particular offering approaches was minimal [3]. Switzerland's top securities market regulator announced in late 2017 that it was investigating some previous open digital token offerings for regulatory breaches [20], but that depending on the circumstances, open digital token offerings may not be considered securities distributions [21]. In the Cayman Islands, regulators made no statements regarding the applicability of securities law to open digital token offerings, although its legal definition of a security is quite narrow [22].

2.2. Singapore Remained an Open Token Offering Hub as Policies Elsewhere and Market Trends Shifted

Figure 1 illustrates how by the second-half of 2018, negative digital token market conditions contributed to a sharp dollar-volume decline in open token offerings relative to early 2018. Yet these conditions were global, and do not explain the disparate shifts in jurisdictional shares of dollar-volume illustrated above. By the second-half of 2018, Cayman, Swiss, and U.S. open digital token offerings accounted for just seven, seven, and two percent of total global dollar-volume, respectively [2]. Alternatively, 21 percent occurred in Singapore, 42 percent took place in smaller jurisdictions (each accounting for less than five percent of total 2018 volume), and 20 percent was in the U.K. [2].[ix]

Several factors help explain these outcomes. For starters, some Asian jurisdictions banned forms of open digital token offerings in Q3 2017 [23].

Singapore's location, regulatory approach towards open digital token offerings, and rules on foreign investment and visitors – some of the most open in the world, and less-restrictive than those in Switzerland, the U.K., and the U.S. [24] – drew Asia-based projects to Singapore the following year amidst these unfavourable regulatory shifts. Indeed, data indicate that half of non-Singapore-based digital token project teams that conducted successful 2018 Singapore-registered token offerings were primarily physically-located elsewhere in Asia (excluding Russia) [2]. Also in 2018, policy changes drove Swiss banks to close accounts for digital token projects in large volumes and reportedly dramatically increased the relative cost of certain compliance processes [25] [26]. As some countries' regulatory approaches towards open token offerings became stricter, relatively more accommodative policy frameworks in the U.K. and smaller countries [27] attracted a few sizable open digital token offerings [2],[x] helping explain the larger role of these jurisdictions in 2018 as compared to 2017. Conversely, after the enormous EOS sale ended, Cayman-registered projects accounted for a much smaller share of global open token offering dollar-volume. Perhaps most notably, 2018 U.S. securities regulation trends drove an embrace of the private initial token sale over the open digital token offering for digital token projects seeking sale participants from the U.S.

2.3. Singapore Continued Embracing Open Token Offerings as Private Initial Token Sales Dominated in the U.S.

In February 2018, U.S. SEC Chairman Jay Clayton notoriously remarked: "every [initial coin offering] I've seen is a security" [28]. If a token project markets to the general public securities not registered with the SEC or issued under certain SEC exemptions, then the issuer can be subject to serious penalties, as well as costly class-action lawsuits [29]. Moreover, non-U.S. persons can be subject to enforcement actions for offering unregistered securities to U.S. persons [30] [31]. Chairman Clayton's sweeping remarks were followed by about twenty enforcement actions related to digital tokens [32], and perhaps as many as 100 subpoenas of token projects.[xi] By year-end, no open digital token offering was affirmatively classified by name by the SEC as not being a securities distribution.[xii]

Accordingly, throughout 2018, token projects increasingly banned U.S. persons from participating in open token offerings and relied upon private initial token sales involving a "Regulation D" securities offering to access U.S. buyers. Regulation D allows fundraising events to avoid expensive public securities offerings requirements if sales are generally restricted only to "accredited investors" – primarily defined as individuals/households making over $200,000/$300,000 annually or with a net worth over $1,000,000 [33]. Many Regulation D safe-harbour sales used the U.S. accredited investor threshold as a sole determinant for sale participation regardless of the country where those seeking to purchase tokens were legally-domiciled.[xiii] Several U.S. token projects utilised the Regulation Crowdfunding ("CF") exemption to conduct open digital token offerings exempted from public securities offering requirements, but these capped sales likely accounted for just 1 percent of overall 2018 token sale dollar-volume [2] [34].[xiv]

As Figure 2[xv] shows, by Q3/Q4 2018, purely-private sales accounted for 94 percent of the dollar-volume of successful U.S. token offerings, versus just 11 percent in Singapore – which continued to embrace the open digital token offering [2]. Indeed, in October 2018, the MAS's Managing Director Ravi Menon stated that the MAS had "seen quite a lot of [digital token offering] activity that is not security related" [35]. In only one instance in 2018 did the MAS announce that it directed

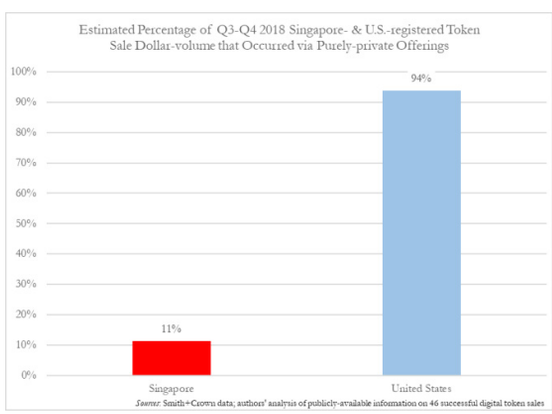


Figure 2. Purely-private token sales accounted for almost all Q3/Q4 2018 U.S. token sale volume, but were relatively minimal in Singapore

a project to cease offering tokens to Singapore-based persons because it considered the project's sale of tokens to be an unregistered public securities offering [36] – evidence of a clearly-understood regulatory distinction between open digital token offerings and traditional securities distributions.

Surely, some 2018 private initial token sales took place without involving Regulation D. The vast majority of private initial token sale events, however, involved a Regulation D offering [2]. Overall, approximately 75 percent of 2018 digital token offering dollar-volume was open, rather than purely-private [2].

3. Exploring the Implications of Singapore's Open Digital Token Offering Embrace

Clearly, a number of external and internal policy factors contributed to Singapore's emergence as a global open digital token offering hub. This section explores outcomes of Singapore's embrace of this token distribution model related to: 1) the operational status

and focus of Singapore-registered token projects; 2) open token offering retail participant risks; and 3) the extent to which Singapore-registered projects are physically-based in the country.

3.1. Open Digital Token Offerings Offer Unique Benefits Related to Widespread Token Distribution

As a recent study helps illustrate, open digital token offerings can enable digital token networks to concurrently raise funds and build up an active community of users and project contributors [37]. Indeed, research finds that higher community engagement is associated with a token project's success [38]. As one analysis explains, despite the growing relevance of institutional investors in open digital token offerings (about 37 percent of 2018 token offerings through mid-Q3 reportedly conducted private sale stages [39]), "putting a token into the hands of 50,000 people who actually went through the process of research and purchase is the best form of mass-market engagement available that will increase the likelihood of project success" [40].

Figure 3[xvi] suggests that an open token offering model may indeed accelerate the pace at which token networks and applications become operational relative to purely-private sales. It shows that by mid-June 2019, over 70 percent of Singapore-registered projects that conducted successful open digital token offerings from Q3 2017 through Q2 2018 launched "operational"

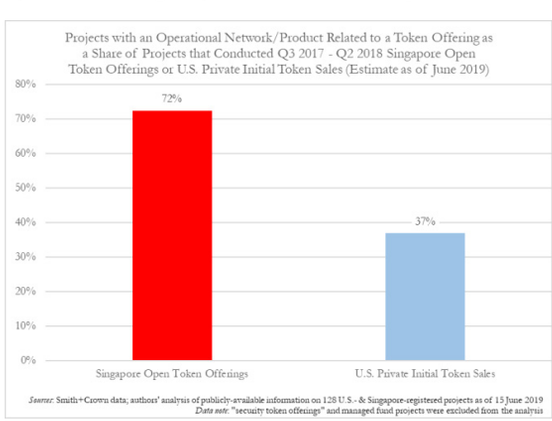


Figure 3. A greater share of one-to-two-year-old Singapore open digital token offerings resulted in operational networks and products relative to Q3 2017 - Q2 2018 U.S. private initial token sales

products or networks related to the token sale, versus 37 percent of U.S.-registered projects that successfully conducted a Regulation D safe-harbour private initial token sale during that time. "Operational" is defined as the publicly-available release of: 1) a token network's open-source and live testnet or mainnet; and/or 2) a minimum-viable-product usable by the project's targeted customer base.

One driver of the discrepancy in Figure 3 is that regulations restrict the re-sale to non-accredited investors of digital tokens distributed via a Regulation D safe-harbour offering [41] [42]. This impedes the ability of projects that conduct token offerings using the Regulation D safe-harbour to leverage primary or secondary digital token markets to facilitate widespread token ownership by a globally-dispersed community of developers. As the founder of a project that conducted one of the largest private initial token sales to date remarked after apologising that his project's token offering would be purely-private: "[the accredited investor threshold] excludes some of the groups most capable of investing in these kinds of projects, for example, cryptography and game theory PhD students" [43].

Indeed, Ethereum sale data and subsequent survey data suggests 50 to 75 percent of Ethereum's open digital token offering participants contributed less than $1,000 [44] [10], and the network's early attraction of a large community of well-informed retail token-holders played a critical role in its success [10]. Open digital token offerings facilitate participation in open-source software development and create a sense of empowerment and ownership, thus mobilising programmers to test and improve underlying software [14]. This open-source ethos is particularly important for the development of smart contract platforms such

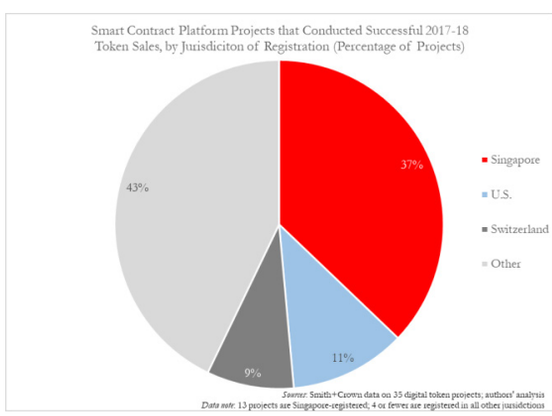


Figure 4. Nearly 40 percent of smart contract platform projects that conducted successful 2017-18 token sales are registered in Singapore

as Ethereum – it is difficult to imagine developers building applications or engaging with strangers on a platform that they do not understand and cannot test [45]. Accordingly, as Figure 4[xvii] illustrates, a disproportionate share of smart contract platform projects that conducted 2017-18 token offerings were Singapore-registered, likely due in part to Singapore's embrace of the open digital token offering. These projects largely aim to increase the range of economic and social contexts in which open blockchain solutions can be applied by building platforms that overcome some of Ethereum's scalability challenges.

3.2. Risks to Open Digital Token Offering Retail Participants are Manageable

Open digital token offerings can result in inexperienced persons purchasing tokens from digital token projects that are not long-term viable – many projects have failed or probably will fail [46] [47]. Yet inexperienced retail exposure to these tokens is much more likely to be facilitated by online accounts easily-opened with secondary market trading venues rather than directly via open digital token offerings. Moreover, few Singapore-registered digital token offerings involve substantial direct Singapore-based retail purchases, although this is reportedly in part because some projects restrict Singapore persons' participation in token offerings [48]. Research also suggests, however, that most digital token offering participants contribute modest-size dollar-amounts, and that these contributors largely have a technology background or meaningful investment experience [10]. Indeed, participation in open digital token offerings usually necessitates a moderate level of technological acumen and market awareness – a purchaser often must understand how to operate an ERC-20 "wallet," and sale participation may require first signing up via a whitelist.

Surely, despite these barriers, the low cost of structuring an open digital token offering can allow fraudsters to solicit funds with relative ease. As much as ten percent of pre-mid-2018 digital token sale dollar-volume were scams [49], although some research suggests that the degree of fraud is much lower [50] and that "investors are shrewd enough to spot [scams]" [46]. Moreover, in Singapore, fraud can result in lengthy jail sentences [51], and while some uncertainty surrounds the applicability of criminal law to matters involving digital tokens [17], two foreigners recently charged for promoting a fraudulent digital token project may face up to five years in jail [52]. Furthermore, the Singapore-registered entity responsible for a token sale must have at least one Singapore citizen or permanent resident on the board, as well as a local secretary [53]. These gatekeepers, as well as Singapore's legal community (which drafts token offering documents) and the Accounting and Corporate Regulatory Authority, further minimise the likelihood of fraudulent open digital token offerings.

While Singapore's open token offering embrace has not made it a safe-haven for fraudulent projects, markets for some tokens generated via Singapore-registered offerings have been nefariously manipulated. Bad actors can create false optimism and spikes in a token's value, and then sell the token at a market high, driving a large price decline that harms retail token-holders [54]. In fact, Singapore's first open digital token offering resulted in a token later manipulated by such a pump-and-dump scheme [55]. Singapore's government has warned of this predatory market behaviour [56], but retail investors can still fall victim. Yet market manipulation is a serious issue for many digital tokens – not a problem exclusive to those generated via open token offerings.

3.3. Nearly Half of Singapore-registered Token Projects are Primarily Physically-based in the Country

Despite the large number of Singapore-registered projects primarily physically-based outside the city, Figure 5[xviii] shows that a greater share of Singapore-registered projects that successfully conducted token sales in 2018 are domestically-based relative to the respective share of Switzerland- and Cayman-registered projects primarily physically-based in those jurisdictions [2]. Surely, at 46 percent, the share of projects physically-based in Singapore has room to grow. Yet a recent industry survey finding that Singapore is the world's leading "crypto hub" city

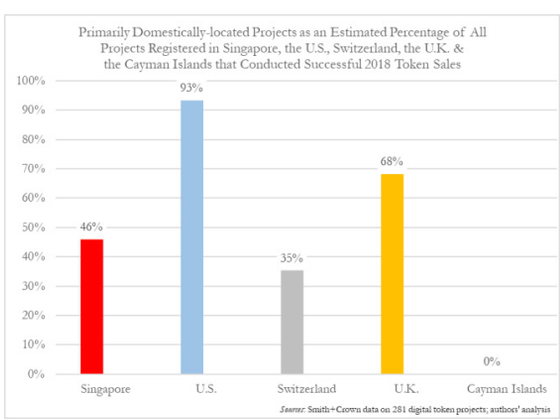


Figure 5: Almost half of projects that conducted successful 2018 Singapore-registered token offerings were primarily physically-located in the city

notes that its strengths relative to other cities include not only the robust "activity" of its digital token project community, but also Singapore's "international ecosystem" [57]. Indeed, Singapore's relative openness to foreign visitors [24] enables internationally-diverse project teams not primarily physically-located in the country – many of which are based elsewhere in Asia, as mentioned in Section 2 – to regularly visit and maintain a secondary presence there.

Moving forward, Singapore will benefit from its physical concentration of token projects, as research indicates that geographically-concentrated innovation within a particular field begets relatively deeper and swifter innovative activities [58]. Data indicate that Singapore was likely home to more projects that successfully conducted digital token sales in 2018 than any other city, with the second- and third-highest being San Francisco (including Palo Alto) and London [2].

4. Conclusion

The open digital token offering can enable projects to simultaneously: 1) raise funds for the development of a project's network, platform, or service; 2) build up a user-base; and 3) incentivise globally-dispersed communities of developers to contribute to a project. While in certain jurisdictions, this token distribution model may be deemed to be a securities offering, in practice, the open digital token offering and digital tokens it produces are often fundamentally different than traditional securities distributions and securities, respectively. Singapore's emergence as a global hub of the open digital token offering was enabled not only through existing legal frameworks and constructive steps to produce regulatory clarity regarding securities law, but also by its geographic location and openness to foreign visitors and capital.

The inclusiveness of open digital token offerings, as well as Singapore's regulatory clarity regarding this distribution model, help explain why a greater share of one-to-two-year-old Singapore-registered open digital token offerings, relative to U.S. private initial token sales, have resulted in operational networks or minimum-viable-products, and why so many token offerings for 2018 smart contract platform projects were Singapore-registered. Indeed, open digital token offerings are well-suited for incentivising the development of open-source projects. While this distribution model can ease the ability of bad actors to conduct fraud, fraudulent projects are likely not a major concern in Singapore, in part due to local gatekeepers and strict laws. There are also practical barriers-to-entry associated with open token offerings that preclude large-scale participation of an uninformed public.

While open digital token offerings have flaws and can support likely-to-fail projects, trends highlighted in this research support claims that this distribution model is advantageous relative to securities offerings and private initial token sales for certain types of projects, particularly those focused on launching distributed open-source networks and services. Because of its embrace of the open digital token offering, as well as other policy factors, Singapore is well-positioned to remain a hub of open blockchain innovations.

5. Appendix

Token projects included in the dataset used in this research's estimates of token sale activity (the "Primary Dataset" [2]) were initially sourced by Smith+Crown through: 1) a detailed Smith+Crown intake survey submitted by token projects; 2) Smith+Crown's bi-monthly reviews of online data aggregators and the SEC EDGAR database; and 3) Smith+Crown's reviews of ongoing industry events. Before including projects identified through these channels in the Primary Dataset, Smith+Crown confirmed that project team member identities were transparent, there was a reasonable amount of public documentation and information available on the project, the project raised over $25,000, and funds raised were not returned to initial backers – for purposes of this article, these criteria are used to classify a "successful" digital token offering. This sourcing methodology makes the scope of Smith+Crown's data smaller relative to those of some popular online aggregators, which may exclusively rely on information sourced through token project self-reporting.

To obtain dollar-raised figures, Smith+Crown sourced token projects' self-reported dollar-raised amounts from data aggregators, and then verified those amounts using on-chain analysis,[xix] SEC EDGAR, other government filings, reports from reliable news sources, or official project statements. If a raise amount was unverifiable, then Smith+Crown entered the amount raised by the project as zero. Generally, token sale dates were determined using the reported date of a sale period ending, and multiple sale stages of a single token offering were treated as a single offering event as long as: 1) sale terms were largely similar; and 2) sale periods were not separated by more than thirty days (otherwise, sales were treated separately).[xx]

Unlike datasets used in other analyses of global token sale trends (for example, [27] [59]), the Primary Dataset clearly distinguishes between a project's legal jurisdiction and physical location. The legal jurisdiction of the entity responsible for a token offering was determined for almost all 2017-18 token sale dollar-volume, and was identified using information provided on the sourcing survey, which Smith+Crown verified and, as necessary, corrected through a review of a project's website and sale terms in collaboration with the authors.[xxi] To determine the primary physical location of digital token projects, publicly-available information on the project's website was used. When data was not available, LinkedIn.com information was reviewed, and the reported city of the project's or CEO's LinkedIn page was treated as the project team's location. If that data was not available, then the self-reported location of the CTO or the predominant location of other project team members was used. For six percent of the projects reviewed to produce Figure 5, the primary location of the project team was listed as unknown, and overall, for approximately 25 percent of 2018 token sale events contained in the Primary Dataset, project team location information was unknown or not recorded.

To determine whether a token offering was an open digital token offering or a private initial token sale, Smith+Crown and the authors reviewed government filings, project announcements, reputable news sources, and token sale terms.[xxii] Multi-tiered sales consisting of both public and private sale stages (including Regulation D offerings followed by public sales) were

generally treated as one open digital token offering, in line with this article's definition of that distribution method; conversely, private sales conducted in advance of cancelled or planned (but yet to occur) open sale rounds were treated as private initial token sales (for example, Telegram's token sale). Digital token projects that conducted Regulation D offerings concurrently or shortly before an open digital token offering that restricted U.S. non-accredited-investors from participating were treated as part of a single open digital token offering. Security token offerings and token sales by projects structured as investment funds were not treated as open digital token offerings, but were included in this article's holistic analyses of digital token offerings (including Figures 2 and 5).[xxiii]

Figure 3 was produced using a definition of "operational" set forth in Section 3 and developed in collaboration with Smith+Crown, LongHash, and other industry participants. Q3 2017 to Q2 2018 Singapore open digital token offerings and U.S. private initial token sales were classified as "operational" or not as of mid-June 2019 based on a review of publicly-available information. Proof-of-works and proof-of-concepts were not treated as "operational" projects. Project classifications used to produce Figure 4 were developed from Smith+Crown's review of project white papers and public information. Based on that review, Smith+Crown tagged certain projects as "smart contract platform" projects, meaning that the project's primary focus is developing a smart contract platform.

References:

[1] "Singapore IPO proceeds plunge to $730m in 2018," Singapore Business Review, 2018 Dec 21. [Online]. Available: https://sbr.com.sg/markets-investing/in-focus/singapore-ipo-proceeds-plunge-730m-in-2018. [Accessed 15 Jun 2019].

[2] Smith+Crown, Dataset on file with authors [see Appendix for methodology used by Smith+Crown and the authors to construct dataset], 2019.

[3] Token Alliance, "Understanding digital tokens: market overviews and proposed guidelines for policymakers and practitioners," Chamber of Digital Commerce, 2018.

[4] MAS, "MAS clarifies regulatory position on the offer of digital tokens in Singapore," 1 Aug 2017. [Online]. Available: http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx. [Accessed 15 Jun 2019].

[5] D. Chuen, L. Low and Y. Wang, "Introduction to initial crypto-token offering," in Inclusive FinTech: Blockchain, Cryptocurrency and ICO, Singapore, World Scientific Publishing Company, 2018, pp. 83-114.

[6] N. Szabo, "Smart contracts: building blocks for digital markets," 1996. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. [Accessed 15 Jun 2019].

[7] Ethereum Foundation, "Developer resources: guides, resources, and tools for developers building on Ethereum," [Online]. Available: https://www.ethereum.org/developers/. [Accessed 15 Jun 2019].

[8] P. V. Valkenburgh, "What does it mean to issue a token 'on top of' Ethereum?," Coin Center, 10 May 2017. [Online]. Available: https://coincenter.org/entry/what-does-it-mean-to-issue-a-token-on-top-of-ethereum. [Accessed 15 Jun 2019].

[9] F. Vogelsteller, "ERC: token standard," GitHub, Nov 2015. [Online]. Available: https://github.com/ethereum/EIPs/issues/20. [Accessed 15 Jun 2019].

[10] D. Chuen, L. Low, M. Chwierut, W. Anderson, B. Lio and B. Downes, "The characteristics of token investors," in Inclusive FinTech: Blockchain, Cryptocurrency and ICO, Singapore, World Scientific Publishing Company, 2018, pp. 125-171.

[11] CoinMarketCap, Dataset on file with authors, 2019.

[12] PricewaterhouseCoopers, "Considering an IPO to fuel your company's future? Insight into the costs of going public and being public," Nov 2017. [Online]. Available: https://www.pwc.com/us/en/deals/publications/assets/cost-of-an-ipo.pdf. [Accessed 15 Jun 2019].

[13] International Monetary Fund, "Handbook on securities statistics," 2015. [Online]. Available: https://www.imf.org/external/np/sta/wgsd/pdf/hss.pdf.. [Accessed 15 Jun 2019].

[14] S. Adhami, G. Giudici and M. Stefano, "Why do businesses go crypto? An empirical analysis of initial coin offerings," Journal of Economics and Business, vol. 100, pp. 64-75, May 2018.

[15] H. Peirce, "Regulation: a view from inside the machine," 8 Feb 2019. [Online]. Available: https://www.sec.gov/news/speech/peirce-regulation-view-inside-machine. [Accessed 15 Jun 2019].

[16] Securities and Futures Act (Cap. 289), Section 2(1).

[17] J. W. Lim, "A facilitative model for cryptocurrency regulation in Singapore," in Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, London, U.K., Elsevier Inc., 2015, pp. 361-380.

[18] S. Yep, "How Singapore became Asia's ICO hub," LongHash, 30 Apr 2018. [Online]. Available: https://www.longhash.com/news/14. [Accessed 15 Jun 2019].

[19] MAS, "A guide to digital token offerings," 14 Nov 2017. [Online]. Available: http://www.mas.gov.sg/News-and-Publications/Monographs-and-Information-Papers/2017/Guidance-on-Digital-Token-Offerings.aspx. [Accessed 15 Jun 2019].

[20] FINMA, "FINMA is investigating ICO procedures," FINMA, 29 Sep 2017. [Online]. Available: https://www.finma.ch/en/news/2017/09/20170929-mm-ico/. [Accessed 15 Jun 2019].

[21] FINMA, "FINMA guidance 04/2017," 29 Sep 2017. [Online]. Available: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20170929-finma-aufsichtsmitteilung-04-2017.pdf. [Accessed 15 Jun 2019].

[22] N. Rogers and C. Macculloch, "Building blocks for ICOs in the Cayman Islands," Cayman Financial Review, 22 Jan 2018. [Online]. Available: https://www.caymanfinancialreview.com/2018/01/22/building-blocks-for-icos-in-the-cayman-islands/. [Accessed 15 Jun 2019].

[23] J. Russell, "First China, now South Korea has banned ICOs," TechCrunch, 29 Sep 2017. [Online]. Available: https://techcrunch.com/2017/09/28/south-korea-has-banned-icos/. [Accessed 15 Jun 2019].

[24] I. Vásquez and T. Porcnik, "The human freedom index, XLSX (2016 "foreign ownership/investment restrictions," "capital controls," and "freedom of foreigners to visit" variables)," Cato Institute, 2018. [Online]. Available: https://object.cato.org/sites/cato.org/files/human-freedom-index-files/hfi2018web-revised3.xlsx. [Accessed 15 Jun 2019].

[25] A. Irrera and B. H. Neghaiwi, "Switzerland seeks to regain cryptocurrency crown," Reuters, 19 Jul 2018. [Online]. Available: https://www.reuters.com/article/us-cryptocurrencies-banking-switzerland/switzerland-seeks-to-regain-cryptocurrency-crown-idUSKBN1K91AY. [Accessed 15 Jun 2019].

[26] K. Sedgwick, "Swiss regulations are driving ICOs away," Bitcoin.com, 9 Apr 2018. [Online]. Available: https://news.bitcoin.com/swiss-regulations-are-driving-icos-away/. [Accessed Jun 15 2019].

[27] W. Kaal, "Initial coin offerings: the top 25 jurisdictions and their comparative regulatory responses (as of May 2018)," Stanford Journal of Blockchain Law & Policy, vol. 2, 2019.

[28] M. Orcutt, "Cryptocurrencies crashed in 2018. Now they're right where they should be," MIT Technology Review, 26 Dec 2018. [Online]. Available: https://www.technologyreview.com/s/612659/cryptocurrencies-crashed-in-2018-now-theyre-right-where-they-should-be/. [Accessed 15 Jun 2019].

[29] G. P. Fondo, M. Chang, M. Spillane, S. Fox and T. Kistner, "ICO participant liability — could you be liable for assisting in the sale of unregistered securities?," Bloomberg Law, 15 Dec 2017. [Online]. Available: https://news.bloomberglaw.com/securities-law/ico-participant-liability-could-you-be-liable-for-assisting-in-the-sale-of-unregistered-securities. [Accessed 15 Jun 2019].

[30] T. Hanusik and T. Rodriguez, "I don't live in the United States, so how can the SEC sue me? SEC actions against a foreign national living outside the United States," Bloomberg Finance L.P., 2008. [Online]. Available: https://www.crowell.com/documents/SEC-Actions-against-a-Foreign-National-Living-Outside-the-United-States.pdf. [Accessed 15 Jun 2019].

[31] J. Debler, "Foreign initial coin offering issuers beware: the Securities and Exchange Commission is watching," Cornell International Law Journal, vol. 51, pp. 245-272, 2018.

[32] SEC, "Cyber enforcement actions," [Online]. Available: https://www.sec.gov/spotlight/cybersecurity-enforcement-actions. [Accessed Jun 15 2019].

[33] U.S. Code of Federal Regulations Title 17 Parts 230.501-230.508.

[34] P. H. Lee, "Crowdfunding capital in the age of blockchain-based tokens," St. John's Law Review, vol. 92, pp. 833-913, 2018.

[35] C. Chanjaroen and H. Amin , "Singapore will help crypto firms set up local bank accounts," Bloomberg, 10 Oct 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-10-10/singapore-aids-crypto-firms-seeking-banks-while-staying-vigilant. [Accessed Jun 15 2019].

[36] MAS, "MAS warns digital token exchanges and ICO issuer," 24 May 2018. [Online]. Available: http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-warns-Digital-Token-Exchanges-and-ICO-Issuer.aspx. [Accessed 15 Jun 2019].

[37] J. Li and W. Mann, "Initial coin offering and platform building," Working paper, Jun 17 2018. [Online]. Available: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-af-conference/paper-li.pdf. [Accessed 15 Jun 2019].

[38] H. T. Sabrina, M. Niessner and D. Yermack, "Initial coin offerings: financing growth with cryptocurrency token sales," ECGI working paper series in finance, working paper no. 564/2018, Jul 2018. [Online]. Available: https://ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf. [Accessed 15 Jun 2019].

[39] J. Lee, "ICOs are turning exclusive as wealthy investors snatch up deals," Bloomberg, 8 Aug 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-08-08/token-sales-turn-exclusive-as-private-investors-snatch-up-deals. [Accessed 15 Jun 2019].

[40] M. Dibb, "Are public token sales a thing of the past?," Medium: Astronaut Capital, 29 May 2018. [Online].

Available: https://medium.com/astronaut-capital/are-public-token-sales-a-thing-of-the-past-15c89efefa1a. [Accessed 15 Jun 2019].

[41] U.S. Code of Federal Regulations Title 17 Part 230.144.
[42] U.S. Code of Federal Regulations Title 17 Part 230.144A.

[43] I. Allison, "Filecoin laments shutting out crypto supporters to meet SEC regulations," International Business Times, 8 Aug 2017. [Online]. Available: https://www.ibtimes.co.uk/filecoin-laments-shutting-out-crypto-supporters-meet-sec-regulations-1633620. [Accessed 15 Jun 2019].

[44] V. Buterin, "Ether sale: a statistical overview," Ethereum Foundation, 8 Aug 2014. [Online]. Available: https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/. [Accessed 15 Jun 2019].

[45] P. V. Valkenburgh, "What is "open source" and why is it important for cryptocurrency and open blockchain projects?," Coin Center, 17 Oct 2017. [Online]. Available: https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects. [Accessed 15 Jun 2019].

[46] H. Benedetti and L. Kostovetsky, "Digital tulips? returns to investors in initial coin offerings," Working paper, May 20 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182169. [Accessed 15 Jun 2019].

[47] J. Daniell, "Ethereum's Vitalik Buterin on 'tokens 1.0'," ETHNews, 24 Oct 2017. [Online]. Available: https://www.ethnews.com/ethereums-vitalik-buterin-on-tokens-10. [Accessed 15 Jun 2019].

[48] R. Jayaseelan, "Singapore's ICO gamble," The Star Online, 24 Dec 2018. [Online]. Available: https://www.thestar.com.my/business/business-news/2018/12/24/singapores-ico-gamble/. [Accessed 15 Jun 2019].

[49] Statis Group, "Cryptoasset market coverage initiation: network creation," Bloomberg, Jul 2018. [Online]. Available: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ. [Accessed 15 Jun 2019].

[50] D. Liebau and P. Schueffel, "Cryptocurrencies and initial coin offerings: are they scams? - an empirical study," The Journal of The British Blockchain Association, vol. 2, no. 1, pp. 47-55, 2019.

[51] S. Sharpe, "Financial crime in Singapore: overview," Thomson Reuters Practical Law, 2017. [Online]. Available: https://uk.practicallaw.thomsonreuters.com/3-618-7957?__lrTS=20190325161937875&transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_Ib17914890ef411e798dc8b09b4f043e0. [Accessed 15 Jun 2019].

[52] R. Mui, "Two men charged in Singapore with promoting 'fraudulent cryptocurrency' OneCoin," The Business Times, 10 Apr 2019. [Online]. Available: https://www.businesstimes.com.sg/government-economy/two-men-charged-in-singapore-with-promoting-fraudulent-cryptocurrency-onecoin. [Accessed 15 Jun 2019].

[53] Flag Theory, "Where to set up a foundation for an ICO (a comparative analysis)," 6 Oct 2017. [Online]. Available: https://flagtheory.com/foundation-initial-coin-offering-ico/. [Accessed 15 Jun 2019].

[54] J. Xu and B. Livshits, "The anatomy of a cryptocurrency pump-and-dump scheme," in 28th Usenix Security Symposium, Santa Clara, CA, USA, 2019.

[55] S. Shifflett and P. Vigna, "Traders are talking up cryptocurrencies, then dumping them, costing others millions," 5 Aug 2018. [Online]. Available: https://www.wsj.com/graphics/cryptocurrency-schemes-generate-big-coin/. [Accessed 15 Jun 2019].

[56] Singapore Government, "Are digital tokens such as cryptocurrencies a simple, safe, and sure-fire way of making money?," Factually, 25 May 2018. [Online]. Available: https://www.gov.sg/factually/content/digital-tokens. [Accessed Jun 15 2019].

[57] R. Kurani, "Which are the best locations for blockchain companies?—we asked our well-travelled crypto friends," Medium, 22 Feb 2019. [Online]. Available: https://medium.com/birds-view/which-are-the-best-locations-for-blockchain-companies-bd816c940456. [Accessed 15 Jun 2019].

[58] M. Muro and B. Katz, "The new 'cluster moment': how regional innovation clusters can foster the next economy," Metropolitan Policy Program, Brookings Institution, Sep 2010. [Online]. Available: https://www.brookings.edu/wp-content/uploads/2016/06/0921_clusters_muro_katz.pdf. [Accessed 15 Jun 2019].

[59] Ernst and Young, "EY research: initial coin offerings (ICOs)," EY, Dec 2017. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf. [Accessed 15 Jun 2019].

[i] Dollar-volume figures throughout this article are in U.S. dollars. This figure includes open digital token offerings, security token offerings, and private initial token sales. See the Appendix for methodology used to calculate dollar-volume figures of 2017-18 digital token sales presented throughout this research.

[ii] Trends related to initial mining events and airdrops are not analysed in this research.

[iii] Obstacles related to retail investor technological acumen are discussed in Section 3. Additionally, compliance with anti-money laundering laws, sanctions. and/or securities law interpretations may

cause projects to decide to prohibit certain nationalities from participating in open digital token offerings.

[iv] For an explanation of how this research defines a "successful" digital token sale, see the Appendix.

[v] The U.S. legal definition of a security extends beyond equity and debt securities and includes "investment contracts," defined according to a multi-prong common law test [3] (see footnote viii and accompanying text).

[vi] Figure 1 was produced by the authors using a Smith+Crown dataset of 2017-18 digital token offerings [2]. Sale-level data related to country of registration and distribution type were independently reviewed by the authors for approximately 90 percent of the dollar-volume of token sale events included in the dataset (see Appendix for more on methodology).

[vii] These guidelines also clarified that open digital token offerings not subject to direct MAS regulation are nonetheless likely subject to certain Singapore laws aimed at combatting money laundering and terrorism financing [19].

[viii] According to the Supreme Court's 1946 "Howey Test," an "investment contract" – a type of security – exists if 1) an investment is made in 2) a common enterprise by 3) investors reasonably expecting to earn profits 4) as a result of others' managerial or entrepreneurial efforts (see [3] [15]).

[ix] Small jurisdictions with a sizable share of 2018 open digital token offering dollar-volume include Gibraltar (4 percent) and Estonia (4 percent) [2]. Singapore and the U.K. accounted for 14 and 7 percent of 2018 dollar-volume, respectively [2].

[x] For example, approximately half of the dollar-volume of the U.K.'s nine successful Q3/Q4 2018 open digital token offerings is attributable to two projects [2]. In Singapore, on the other hand, there were over 20 successful open digital token offerings during this time, the largest of which accounted for just 11 percent of total offering dollar-volume [2].

[xi] Figure estimated through conversations with U.S.-based legal and regulatory experts.

[xii] Bitcoin's initial distribution was not an open digital token offering (as defined in this research), but rather, was an initial mining event.

[xiii] For example, Filecoin's private initial token sale.

[xiv] Regulation CF offerings are each capped at $1.07 million and represented approximately $22 million of token sale dollar-volume in 2017 through mid-2018 [34]. While in 2018 some projects reportedly applied to sell tokens to the public using the SEC's Regulation A+ exemption, the SEC did not approve any Regulation A+ token sales.

[xv] Figure 2 was produced by the authors using a Smith+Crown dataset of 2017-18 digital token offerings and through the authors' classification of token sale type as determined by a review of publicly-available information related to 46 Q3/Q4 2018 U.S.- and Singapore-registered digital token sales (see Appendix for more on methodology) [2].

[xvi] Figure 3 was produced by the authors using a Smith+Crown dataset of 2017-18 digital token offerings and through the authors' classification of token sale type and the operational status of networks or products associated with a token sale as determined by a review of publicly-available information related to 128 U.S.- and Singapore-registered digital token projects that conducted open digital token offerings or private initial token sales from Q3 2017 through Q2 2018 (see Appendix for more on methodology) [2].

[xvii] Figure 4 was produced by the authors using a Smith+Crown dataset of 2017-18 digital token offerings (see Appendix for more on methodology) [2].

[xviii] Figure 5 was produced by the authors using a Smith+Crown dataset of 2017-18 digital token offerings (see Appendix for more on methodology) [2].

[xix] When possible, Smith+Crown used Etherscan to examine the actual amounts raised by a token project. As off-chain sales of digital tokens proliferated, this method became less workable.

[xx] One exception to this general rule was EOS's large, prolonged fundraising event, which was "grouped into monthly amounts, with each month being treated as a separate [sale event]" [3]. In a few instances, data constraints forced the estimation of sale dates and/or the consolidation of sale periods with unclear start or end dates.

[xxi] For approximately two percent of 2017-18 open digital token offering dollar-volume, legal jurisdiction was classified as unknown [2].

[xxii] The authors independently reviewed publicly-available information on distribution type and country of legal jurisdiction for approximately 90 percent of 2017-18 token sales by dollar-volume.

[xxiii] These types of projects accounted for approximately two percent of successful 2017-18 digital token distribution dollar-volume [2].

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
RWG[1] and DLKC[1,2] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
RWG[1] wants to thank the Foundation of the Chamber of Digital Commerce for a modest travel and conference expenditures grant that funded research-related visits to Hong Kong, Singapore, and Tokyo.

Acknowledgements:
RWG and DLKC deeply thank Smith+Crown (Matt Chwierut, Brian Lio, Alistair Simmonds, and Stuart Young) for providing data that made this research possible. The authors are also appreciative of helpful insights shared by LongHash (Emma Cui and Shi Khai Wei) and CoinMarketCap (Carylyne Chan and Aaron Khoo), as well as by Paul S. Atkins, Perianne Boring, Jehan Chu, Matthew Comstock, Nizam Ismail, Amy Davine Kim, TM Lee, Daniel Liebau, Bobby Ong, Remington Ong, Teong Jing Sim and Diego Zuluaga.

Photo by Austin Distel on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(2)2019

Cryptocurrency Investing Examined

Jim Kyung-Soo Liew[1], Richard Ziyuan Li[2] , Tamás Budavári[2], Avinash Sharma[3]
Johns Hopkins University, USA
[1]Carey Business School
[2]Department of Applied Mathematics and Statistics
[3]Bioengineering and Biomedical Engineering
Correspondence: kliew1@jhu.edu
Received: 17 January 2019 **Accepted:** 28 March 2019 **Published:** 28 May 2019

Abstract
In this work we examine the largest 100 cryptocurrency returns ranging from 2015 to early 2018. We concentrate our analysis on daily returns and find several interesting stylized facts. First, principal components analysis reveals a complex daily return generating process. As we examine data in the most recent year, we find that surprisingly more than one principal component appears to explain the cross-sectional variation. Second, similar to hedge fund returns, cryptocurrency returns suffer from the "beta-in-the-tails" hidden risk. Third, we find that predicting cryptocurrency movements with machine learning and artificial intelligence algorithms is marginally attractive with variation in predictability power per crypto-currency. Fourth, lower volatile cryptocurrencies are slightly more predictable than more volatile ones. Fifth, evidence exists that efficacy of distinct information sets varies across machine learning algorithms, showing that predictability may be much more complex given a set of machine learning algorithms. Finally, short-term predictability is very tenuous, which suggests that near-term cryptocurrency markets are semi-strong form efficient and therefore, day trading cryptocurrencies may be very challenging.
Keywords: *AI, Bitcoin, Cryptocurrencies, Machine Learning, PCA, Beta-in-the-Tails*
JEL Classifications: *G12, G14, G17, G40, G*

1. Introduction

Cryptocurrency is a digital asset designed to work as a store of value and a medium of exchange[1]. As of February 28th, 2018, the total market capitalization of the cryptocurrency market stood at $448 billion and consists of 1,524 types of currencies. Amongst the many controversies surrounding cryptocurrencies, a popular topic of debate is whether it should be classified as a commodity, investment, property, currency or digital currency. Bitcoin puts cryptocurrencies center stage in the popular press and with the recent painful pull back in early 2018, the interest in Bitcoins in particular continues to hold. Bitcoins started 2017 at $998.33 and grew 14x to finish the year at $14,156.40, as is shown in Fig. 1. As of February 28th, the price was $10,559.20.
Bitcoin, the first successful cryptocurrency, was created in January 2009, in the aftermath of the financial crisis of 2008, by an unknown person or a group of people under the Japanese name of Satoshi Nakamoto. Bitcoin utilizes a technology called blockchain, which is a combination of cryptography, consensus algorithms,

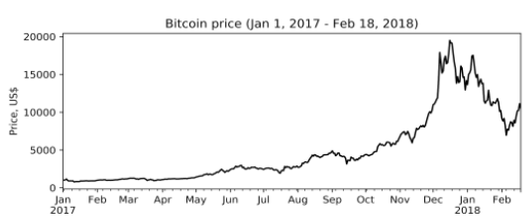


Figure 1: Bitcoin price from Jan 1, 2017 to Feb 18, 2018

economic incentives and distributed ledger to secure its transactions. While the technical discussion of blockchain is beyond the scope of this work, this technology has endowed Bitcoin with many important characteristics, such as;

- Decentralization,
- Trusted network built upon potentially untrustworthy nodes,
- Transparency, and
- Immutability history, etc.

Many cryptocurrencies were invented after Bitcoin, but

Bitcoin continues to be the most popular, as evidenced by it having the largest market capitalization and trading volume, shown in Table 1 below. Subsequently, our investigation primarily focuses on Bitcoin prices in this research.

Index	Name	Price	Market Cap ($Billion)	Volume (24 hrs $Billion)
1	Bitcoin	$10,559.20	$178.4	$6.9
2	Ethereum	$869.63	$85.1	$2.0
3	Ripple	$0.921	$36.0	$0.33
4	Bitcoin Cash	$1,223.85	$20.8	$0.38
5	Litecoin	$208.43	$11.6	$0.78
6	NEO	$135.27	$8.8	$0.33
7	Cardanol	$0.317	$8.7	$0.12
8	Stellar	$0.346	$8.2	$0.037
9	EOS	$8.64	$6.0	$0.38
10	IOTA	$1.89	$5.3	$0.044

Table 1: Top Ten Cryptocurrencies

(Source: CoinMarketCap.com, data as of February 28th, 2018.)

While participants of the Bitcoin blockchain can transfer Bitcoins with each other directly, most investors have to go to cryptocurrency exchanges if they want to purchase Bitcoins with U.S. dollars or other traditional currencies. While the quoted prices from different exchanges can vary largely, arbitrage was very difficult due to the lack of easy access to short Bitcoins, until CBOE and CME introduced Bitcoin futures in December 2017.

1.2 Artificial Intelligence (AI)

Similar to cryptocurrency, AI is another increasingly intriguing technological development. AI represents a broad range of techniques including machine learning, deep learning, natural language processing, etc. Its application is rapidly penetrating every aspect of human society - e-commerce, autonomous vehicles, image recognition, to name a few. A detailed discussion of AI techniques and their application, unfortunately, is beyond the scope of this paper.

Financial institutions are increasingly testing and deploying AI techniques to obtain an edge in their business, such as in trading. Money managers have been employing thousands of quantitative experts to develop sophisticated AI models for predicting prices, identifying signals, monitoring sentiment, etc. While the efficacy of these efforts is still debatable, AI models and strategies are prevailing in every market (equity, commodity, FX, etc.). It is, therefore, only a matter of time before practitioners and academic researchers begin using AI techniques to analyze cryptocurrency markets. We hope our findings herein will serve as an important contribution to this growing field.

1.3 Our Research Results

In this paper, we first analyze the top 100 cryptocurrencies using correlation analysis and principal component analysis (PCA). Daily returns reveal that in some period there exists a single dominant component however, in the most recent prior year there appears to be two components that help explain the variation of the cryptocurrency returns. Next, we compare cryptocurrencies with traditional assets. We also perform Liew [2013]'s beta-in-the tail analysis to examine potential hidden risks. We find some evidence that similar to hedge funds, cryptocurrencies may suffer from this hidden risk.

Finally, we conduct rolling prediction analysis on 57 cryptocurrencies with 11 AI algorithms. Our results show that predictability may be difficult and there are many heterogeneous effects here. Some information sets perform better with some family of algorithms, and larger cryptocurrencies with lower volatility maybe more predictable than smaller cryptocurrency with higher volatility.

The remainder of this paper is organized as follows: Section 2 reviews prior literature, Section 3 presents our data and preliminary analysis, Section 4 describes the methodology, Section 5 provides the results and Section 6 summarizes and concludes.

2. Literature Review

While there are many cases and projects about Bitcoin price predictions online, scarce academic research presently exists regarding Bitcoin price predictability. We review the most important prior research in this subject by aggregating them into three different groups.

The first group attempts to predict Bitcoin prices with information about the Bitcoin blockchain network. For example, Madan et al. [1] from Stanford use three machine learning algorithms to predict the sign of daily price change of Bitcoin based on data about the Bitcoin blockchain network, including average confirmation time, block size, hash rate, etc. They report a highest accuracy of 98.7%. Another group of Stanford researcher, Greaves et al. [2] perform similar analysis, getting a classification (sign of hourly price change) accuracy of 55%. In addition to information about the blockchain network, McNally [3] adds daily open, high, low, and close prices as explanatory variables, reporting a classification (signs of daily price changes) accuracy of 52%. El-Abdelouarti Alouaret [4] moves further by including the S&P 500 index and EUR/USD rate,

as well as a variable named bitcoins days destroyed. Similar to sentiment analysis, it also includes a variable representing daily page view on the Wikipedia item "Bitcoin". It also uses vector autoregression and recurrent neural network to conduct price prediction instead of classification.

The second group of studies focus on the relationship between social media data and Bitcoin performance. For instance, Mai et al. [5] analyze Bitcoin-related user posts from a forum and Twitter and demonstrate that more bullish posts are associated with higher future Bitcoin returns. They also conclude that the social media effects on Bitcoin performance are driven by the "silent majority", and the impact of forum posts is larger than that of tweets. Stenqvist et al. [6] try to predict Bitcoin price (up/down) using sentiment analysis on Twitter, and report that the sentiment change over a 30-minute period is useful for predicting price movement of 2 hours later, resulting in an accuracy of 79%. Instead of performing sentiment analysis on all social media content posted, Kim et al. [7] extract the hottest topics on a Bitcoin-related forum and define a time series score to represent the "strength" of each topic. While these scores are not significant in Granger causality tests, a deep learning model with these scores as inputs leads to prediction (for price and transaction volume) accuracies ranging from 50%+ to 80%+. Interestingly, Kaminskt [8], by analyzing Twitter posts, claims that social media sentiments mirror the Bitcoin market activity, rather than being predictive.

Instead of Bitcoin blockchain network data and social media data, some papers examine the performance of Bitcoin in other ways. Chu et al. [9] fits log returns in fifteen popular parametric distributions in finance and find that the generalized hyperbolic distribution is the most appropriate. Balcilar et al. [10] perform causality-in-quantiles tests and point out that Bitcoin trading volume can predict price returns but fail to predict volatility. Indera et al. [11] use Multi-layer Perceptron (MLP) to predict Bitcoin price based on historical open, high, low, and close, as well as the moving average technical indicators, reporting significant results (in mean mean-squared error).

The third group of research comprises of researchers attempting to use every factor to predict Bitcoin price. Georgoula et al. [12] and Garcia et al. [13] contribute their work in this way. As they provide many conclusions, we are not summarizing here.

3. Data and Preliminary Analysis

3.1 Cryptocurrency

As we mentioned above, there are 1,524 different cryptocurrencies as of February 28, 2018, and they are traded at many different exchanges (markets). Fortunately, CoinMarketCap.com collects transaction data of these cryptocurrencies from various exchanges and publishes both up-to-date and historical data for free, which can be obtained through their API. Taking advantage of this resource, we scrap the historical data of the top 100 cryptocurrencies, in terms of market capitalizations as of February 18, 2018. Before selecting the top 100, we remove those with relatively short history1. Therefore, all selected cryptocurrencies date back to at least January 1, 2017, and Fig. 2 shows the number of cryptocurrencies under analysis over time. The data includes close price, trading volume, and market capitalization during the period of January 1, 2015 to December 31, 2017.

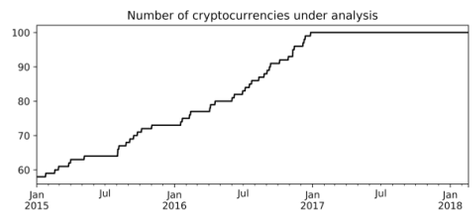


Figure 2: Number of cryptocurrencies under analysis (Jan 2015 - Feb 2018)

3.1.1 Price returns

We calculate daily, weekly, and monthly returns for each cryptocurrency as (holding period returns):

$$R_t = \frac{P_t}{P_{t-1}} - 1$$

We conduct normality tests on all returns series and find that during Jan 1, 2015 to Feb 18, 2018, none of the daily price returns of any cryptocurrency is normal at the significance level of 95%. For weekly returns, two cryptocurrencies yield normal returns. And ten of them have normal monthly returns. Therefore, we think it is more appropriate to use holding period returns rather than log returns.

Table 2, Table 3, and Table 4 provide statistical summary of price returns of Bitcoin (BTC), Ethereum (ETH), and Ripple (XRP), respectively, which are the top 3 cryptocurrencies in terms of market capitalization, as of February 18, 2018. All the three have an average daily return of less than 1% as well as single-digit weekly returns.

Table 2: Statistics summary for price returns of Bitcoin (Jan 2015 - Feb 2018)

	Count	Mean	Standard deviation	Minimum	Median	Maximum
Daily	1144	0.0039	0.0403	-0.2115	0.0026	0.2525
Weekly	163	0.0268	0.1053	-0.2834	0.0187	0.5097

Notes: the "Count" means the number of daily returns and etc. This note applies to the next three tables.

Table 3: Statistics summary for price returns of Ether (Aug 2015 - Feb 2018)[i]

	Count	Mean	Standard deviation	Minimum	Median	Maximum
Daily	926	0.0097	0.0798	-0.7280	-0.0002	0.5103
Weekly	132	0.0682	0.2514	-0.3394	0.0098	1.4227

Table 4: Statistics summary for price returns of Ripple (Jan 2015 - Feb 2018)

	Count	Mean	Standard deviation	Minimum	Median	Maximum
Daily	1144	0.0065	0.0914	-0.4600	-0.0035	1.7937
Weekly	163	0.0494	0.2808	-0.3311	-0.0169	1.9992

Table 5 presents the average statistics summary for the top 100 cryptocurrencies. On average, these cryptocurrencies have an average history of 30 months[ii]. Due to some volatile cryptocurrencies, the average returns and average standard deviations are larger than those for the top 3 shown above.

Table 5: Average statistics summary for price returns of the Top 100 cryptocurrencies (Jan 2015 - Feb 2018)

	Count	Mean	Standard deviation	Minimum	Median	Maximum
Daily	962	0.0452	0.4701	-0.5580	-0.0009	9.0874
Weekly	137	0.1636	0.9940	-0.5356	0.0064	9.2084

Notes:

1. First, we calculate the statistics summary for eac cryptocurrency, including count, mean, standard deviatio minimum, median, and maximum. Then, we calculate th averages of these statistics of all cryptocurrencies.
2. Not all cryptocurrencies have history back to January 2015. Th missing values are dropped before calculating the statistics.

3.1.2 Correlations

To reveal the relationship between various cryptocurrencies, we calculate the correlations of price returns between the top 100 of them. Fig. 3 present the heatmaps of the correlations of daily returns. And Table 6 provides statistics summary for the correlations across all top 100. Obviously, most of the cryptocurrencies are positively correlated and correlations are getting higher when the time frame becomes larger. Another interesting finding is that correlations between large market-cap cryptocurrencies are higher than correlations between smaller market-caps.[iii] Therefore, we can conclude that most cryptocurrencies are moving in herds with lower double-digit correlations, and this phenomenon is stronger between large market-caps.

Finally, to find out how correlations among cryptocurrencies develop over time, we perform a rolling analysis as is shown in Fig. 4. On each day, we calculate the correlations based on daily returns of the preceding 60 (180) days, and then we use the arithmetic mean as the average correlation for that day. That said, the statistic represents the level of correlation of the overall cryptocurrency market during the past 60 (180) days. Obviously, an interesting finding is the spike of market correlation in the second half of 2017, which was exactly accompanied with the rising hotness of cryptocurrencies.

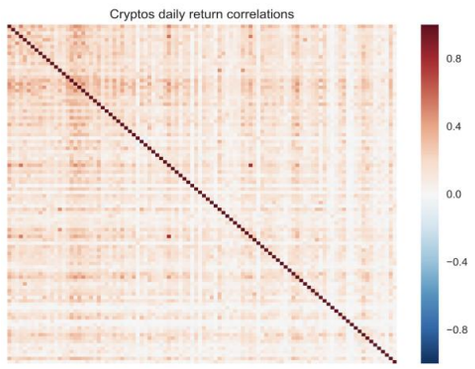


Figure 3: Correlations of daily price returns between top 100 cryptocurrencies (Jan 2015 - Feb 2018)

Table 6: Statistical summary for correlations of returns between top 100 cryptocurrencies (Jan 2015 - Feb 2018)

	Mean	Standard deviation	Minimum	Median	Maximum
Daily	0.1210	0.0522	0.0052	0.1290	0.2289
Weekly	0.1569	0.0659	0.0036	0.1729	0.2855

Notes:
First, for each cryptocurrency, we calculate the mean of its correlations with other cryptocurrencies. Then, we calculate these statistics of the means of correlations.

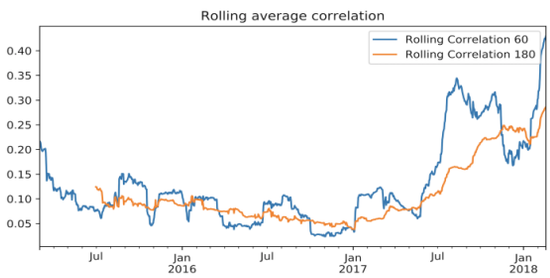


Figure 4: Rolling average correlation (60-days and 180-days, Jan 2015 - Feb 2018)

To have a closer look at Bitcoin, we summarize the statistics of its correlations of price returns with other cryptocurrencies in Table 7. On average, Bitcoin has a correlation of price returns (daily, weekly) of about 0.20 with other cryptocurrencies. In addition, Table 8 lists the most and least correlated cryptocurrencies with Bitcoins. One interesting cryptocurrency stood out upon a quick inspection - Litecoin (LTC) is highly positively correlated with Bitcoin in both time frames. We also examine the autocorrelation of Bitcoin, as is shown in Fig. 5. The autocorrelations for daily returns fall between -0.05 and 0.05, implying a low autocorrelation nature.

Table 7: Statistics summary for correlations of between Bitcoins and other cryptocurrencies (Jan 2015 - Feb 2018)

	Mean	Standard deviation	Minimum	Median	Maximum
Daily	0.2211	0.1158	-0.0140	0.2225	0.5035
Weekly	0.1897	0.1382	-0.1135	0.1962	0.4976

Notes: These statistics are calculated based on the correlations of price returns between Bitcoins and the other 99 cryptocurrencies.

Table 8: Most and least correlated cryptocurrencies with Bitcoins (Jan 2015 - Feb 2018)

	Daily returns		Weekly returns	
	Symbol	Correlation	Symbol	Correlation
Most correlated	PPC	0.5035	SBD	0.4976
	LTC	0.5006	LTC	0.4706
	DOGE	0.4740	GOLOS	0.4463
	NMC	0.4678	EMC2	0.4315
	WAVES	0.4401	NMC	0.4281
Least correlated	PASC	-0.0140	ZOI	-0.1135
	PURA	0.0029	GAME	-0.0991
	NYC	0.0244	PIVX	-0.0915
	MOON	0.0248	EMC	-0.0829
	EXP	0.0306	CRW	-0.0681

Notes: the ranks are based on magnitudes of correlations.

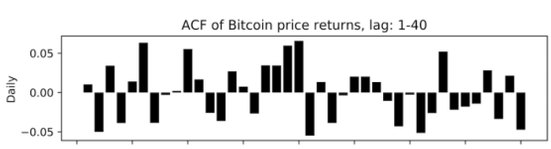


Figure 5: Autocorrelation function of Bitcoin daily price returns (Jan 2015 - Feb 2018)

Notes: the lags range from 1 to 40.

3.1.3 Principal Component Analysis (PCA)

To uncover the common drivers of price returns, we employ a popular dimensionality reduction technique - PCA. The starting time of each cryptocurrency varies, thus, to avoid artificially creating biasedness by filling backward on the missing leading values, we select three subsets of time for our PCA analysis and only employ overlapping series. First, we select the 59 cryptocurrencies which have full history back to January 1, 2015. Second, we select the 74 cryptocurrencies with full history back to January 1, 2016. Finally, we select the 100 cryptocurrencies which have returns back to January 1, 2017. We perform PCA for our three periods employing daily price returns.

Figure 6, Figure 7, and Figure 8 present the results for 2015 to Jan 2018, 2016 to Jan 2018, and 2017 to Jan 2018, respectively. In the first and second case, the first principal component captures the majority of the variance, with less variation explained by the other four principal components. In the third case, the period from 2017 to February 2018 the daily returns appear to differ in their structure. Figure 8 displays that the variation explained by the second principal component gains significantly as the first principal component fall to less than 60%.

Clearly, 2017 was a banner year for cryptocurrency and the addition of more retail investors could be one of the explanations of why this period may have a different underlying structure in the return generating process compared to the two other periods. Retail investors became more heavily involved purchasing cryptocurrencies as evidenced by CoinBase having more accounts than Charles Schwab in November 27, 2017[iv]. This changing investor base could possibly bring in more of a herding and momentum behavior if these retail investors are susceptible to known biases similar to those affecting stock retail investors.

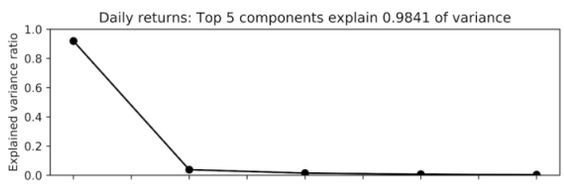


Figure 6: Explained variance ratios for PCA components (58 cryptocurrencies, Jan 2015 - Feb 2018)

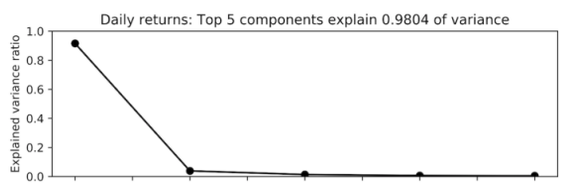


Figure 7: Explained variance ratios for PCA components (73 cryptocurrencies, Jan 2016 - Feb 2018)

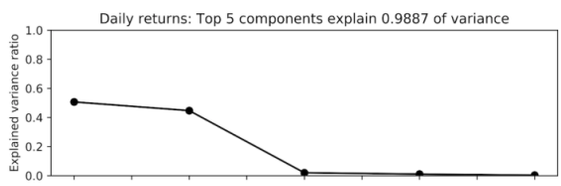


Figure 8: Explained variance ratios for PCA components (100 cryptocurrencies, Jan 2017 - Feb 2018)

3.2 Traditional assets

Recent literature [14] shows that Bitcoin provides diversification to portfolio comprised of traditional assets. We dig in and investigate the cross-market relationship between the top 100 cryptocurrencies and traditional assets. Daily prices of following assets are downloaded from Bloomberg Terminal:

- S&P 500 index (SPX Index): It is a capitalization-weighted index of 500 stocks trading in the U.S. stock market.
- MSCI World Index (MXWO Index): It is a free-float weighted equity index covering stocks trading in developed markets.
- MSCI Emerging Markets Index (MXEF

Index): It is a free-float weighted equity index covering large and mid-cap stocks trading in emerging markets.
- US Dollar Index: a measure of the value of the U.S. dollar relative to the value of a basket of currencies of the majority of the U.S.'s most significant trading partners.
- Gold spot price (in US$)
- Bloomberg Commodity Index (BCOM Index): It is an index reflecting commodity futures price movement.
- VIX Index: The measure of volatility implied by S&P 500 index options, calculated and published by CBOE.

Table 9 presents the correlations between Bitcoin, other cryptocurrencies, and traditional assets, calculated in terms of daily returns. Obviously, Bitcoin is barely correlated to any traditional assets at the daily level (absolute correlations < 0.1). It exhibits a slightly positive correlation to S&P 500, MSCI, USD, Gold, and Commo, while demonstrating a negative correlation to Emg and VIX. Not surprisingly Bitcoin is positively associated with the first PCA component and very highly correlated to the market capitalization weighted cryptocurrency returns.

Table 9: Correlations between daily returns of cryptocurrencies and traditional assets (Jan 2015 - Feb 2018)

	BTC	VW	SP500	MSCI	Emg	USD	Gold	Commo	VIX
BTC	1.0000	0.9416	0.0441	0.0232	-0.0212	0.0134	0.0419	0.0351	-0.0921
VW	0.9416	1.0000	0.0538	0.0316	-0.0204	-0.0049	0.0526	0.0359	-0.0975
SP500	0.0441	0.0538	1.0000	0.9093	0.4480	0.0831	-0.1674	0.2967	-0.7880
MSCI	0.0232	0.0316	0.9093	1.0000	0.6587	-0.0413	-0.1262	0.3836	-0.7283
Emg	-0.0212	-0.0204	0.4480	0.6587	1.0000	-0.0426	-0.0053	0.3641	-0.3848
USD	0.0134	-0.0049	0.0831	-0.0413	-0.0426	1.0000	-0.4070	-0.2427	-0.0828
Gold	0.0419	0.0526	-0.1674	-0.1262	-0.0053	-0.4070	1.0000	0.2441	0.1365
Commo	0.0351	0.0359	0.2967	0.3836	0.3641	-0.2427	0.2441	1.0000	-0.2224
VIX	-0.0921	-0.0975	-0.7880	-0.7283	-0.3848	-0.0828	0.1365	-0.2224	1.0000

Notes: "VW" is the market cap weighted price returns. "MSCI" is the MSCI developed market index. "Emg" is the MSCI emerging market index. "Commo" is the Bloomberg Commodity Index.

3.3 Beta-in-the-Tails Analysis (BTA)

In this section we estimate the potential hidden risks in the cryptocurrency markets. In particular, we examine the stability of their betas for Bitcoin and the VW index with respect to the market, which we employ the S&P 500 as a proxy. Edwards and Caglayan [15] document changes in hedge fund correlation in bull and bear markets. Liew [16] introduces the beta-in-the-tail analysis for hedge funds and documents the vanishing diversification benefits as a hidden risk for hedge fund investors. In down periods the beta associated to hedge fund increases and thus decreasing the perceived diversification benefits. Similarly, we find such an occurrence for cryptocurrencies and warn potential investors to be vigilant with regards to the beta-in-the-tail risk.

Upon visual inspection we document the increasing betas in down S&P 500 daily return periods. We argue that beta-in-the-tail is a significant hidden risk for cryptocurrency investors when employing daily returns.

The methodology for daily beta-in-the-tail analysis follows: First, order all the daily returns on the S&P 500 from least to greatest. Associated to each S&P 500-day period we link both the Bitcoin return and MarketCap Weighted Index return for that day. Next, we anchor the worst daily returns for the S&P 500 and use thirty days of returns to run our regressions. That is, we estimate the beta associated with the worst thirty days in our sample period. At this point, it is important to note that the time dimension has been compromised with this sorting of the daily returns.

The regression is the crypto-returns regressed on the S&P 500 returns. Assuming that the risk-free daily returns are zero yields the CAPM's beta of Sharpe [17] and Litner [18] for the given cryptocurrency index. By anchoring the worst return day for the S&P 500 and expanding the window of daily returns we plot the slope coefficients with inclusion of another daily return. When the window has been expanded to include all the daily returns then the final regression corresponds to the beta for the whole period.

The Betas are reported in the left y-axis and the average daily returns for the window period is reported in the right y-axis on the black dashed line. Standard deviation bands surround the beta estimates. Notice that as more observations are included the standard deviation of the beta estimates reduces. The beta-in-the-tails based on daily returns reach above 1.0 compared this to the whole period beta of close to zero for Bitcoin and VW Index, respectively, as seen on the furthest left bottom corner of Fig. 9.

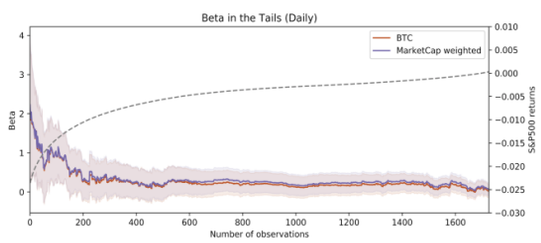


Figure 9: Beta in the Tails (daily)

Notes: Calculated based on daily returns from April 2013 to Feb 2018.

Given that cryptocurrencies trade seven days a week and twenty-four hours a day in contrast to stocks which typically trade only five days a week and six and a half hours a day, we repeat the analysis excluding the weekend in Fig. 10, Beta in the Tail Excluding the Weekends. We arrive at a similar pattern with an increase in the beta in down S&P 500 days. Beta-in-the-

tails appears robust to non-trading weekdays.

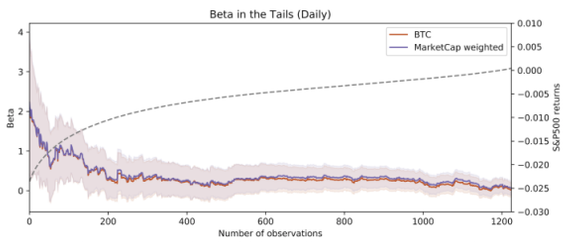


Figure 10: Beta in the Tails (daily, excluding weekends)

Notes: Calculated based on daily returns from April 2013 to Feb 2018.

4. Methodology - Rolling Prediction Analysis

In this section, we firstly give a brief introduction to the 11 machine learning algorithms we tested. Next, we describe the way we roll the prediction analysis. Finally, we present our data.

4.1 Algorithms

In this subsection, we introduced the 11 machine learning algorithms. Our problem can be easily described with linear models – we have a set of variables (x, a matrix with each column being a variable and each row being value for the corresponding day) such as historical returns, volatility and etc., and a target variable (y, a column vector); and we want to train a model that predicts y with out of sample input x.

There are three strands of algorithms in our analysis: 1) linear models, including LASSO, ElasticNet, Stochastic Gradient Descent, and Bayesian Regression; 2) tree-based models, including Decision Tree, Extra Tree Random Forest, AdaBoost, and Gradient Tree Boosting; 3) other models, including KNN, Support Vector Machine, and Multi-layer perceptron. We briefly introduced each of the algorithms as below.

A typical objective function of linear models is as below:

$$\min_{\omega} \frac{1}{n}\sum_{i=1}^{n} L\left(y_i - f(x_i)\right) + \alpha * R(\omega) \quad (1)$$

where L is loss function, R is regularization term, f is the fitted function.

Least Absolute Shrinkage and Selection Operator (LASSO):

LASSO [19] is a linear model that performs both variable selection and regularization. In contrast to simple linear regression, its objective function is as below. We use the scikit-learn default parameters: squared loss function and L2 regularization with $\alpha = 1.0$.

$$\min_{\omega} \frac{1}{2*n}\|X_\omega - y\|_2^2 + \alpha * \|\omega\|_1 \quad (2)$$

ElasticNet (EN):

EN [19] is a linear model that performs regression with both L1 and L2 regularization. This gives it the property of both LASSO and ridge regression, and the objective function is as below. We use the scikit-learn default selection of $\alpha = 1.0$.

$$\min_{\omega} \frac{1}{2*n}\|X_\omega - y\|_2^2 + \alpha * \rho * \|\omega\|_1 + \frac{\alpha * (1-\rho)}{2}\|\omega\|_2 \quad (3)$$

Stochastic Gradient Descent (SGD):

SGD [19] is an efficiency method to fit linear models. It searches for minima or maxima through iterations. We use the scikit-learn default parameters: squared loss function and L2 regularization with $\alpha = 0.0001$.

$$\min_{\omega} \frac{1}{n}\|X_\omega - y\|_2^2 + \alpha * \|\omega\|_2 \quad (4)$$

Bayesian Regression (BR):

BR [19] provides another way of performing linear regression, where linear model can be written as below:

$$y_i = \alpha + \beta * x_i \; with \; y_i \sim N(\mu_i, \sigma) \quad (5)$$

That is, y follows a normal distribution with mean μ and σ, while μ is a linear function with parameters α and β. In this way, the model can be estimated using maximum likelihood function instead of minimizing squared errors:

$$\max_{\alpha,\beta,\sigma} \prod_{i=1}^{n} N(y_i; \alpha + \beta * x_i, \sigma) \quad (6)$$

Decision Tree (DT):

DT [19] is a non-parametric method that can be used for both classification and regression. The tree is built for classifying or predicting test points based on several rules. For classification problems, the leafs of the tree are the classification labels, and for regression problems, the leafs are continuous values. We use the default parameters provided by scikit-learn: using mean square error as splitting criterion, and without max depth of trees.

Extra Tree Random Forest (ETRF):

Random forest [19] is an ensemble method built on many trees, and each tree is built through training on a sample of the entire train set with replacement. In addition, when splitting a node during the construction of trees, the best split is measured among a random subset of features rather than all features. This randomness leads to lower variance and larger bias. On the other hand, ETRF moves even further regarding

randomness in splitting the nodes – splitting thresholds are randomly assigned instead of searching for the most discriminative thresholds. We use the default parameters provided by scikit-learn: 10 trees without max depth of trees and using mean square error as splitting criterion.

Adaptive Boosting (AdaBoost):

AdaBoost [19] is an ensemble algorithm that fits a sequence of relatively weak models with repeatedly modified data. More specifically, it firstly trains on the original train set and assesses the errors. Then it modifies the train set by assigning more weights to poorly modeled points. The processes are repeated for multiple times. Decision Tree is usually used as the base model in AdaBoost. We use the default parameters provided by scikit-learn: 50 Decision Tree models as base estimators.

Gradient Tree Boosting (GTB):

Gradient Boosting [19] is another ensemble algorithm that also fits a sequence of relatively weak models with repeatedly modified data. More specifically, it firstly trains on the train set and the original predicted targets. Then it modifies the predicted targets to be certain type of residuals between the true values and the predicted (trained) values. The processes are repeated for multiple times. GTB is the combination of Decision Tree and Gradient Boosting. We use the default parameters provided by scikit-learn: 100 Decision Tree models as base estimators and without max depth.

K-nearest Neighbor (KNN):

Typically, KNN [19] method is designed for classification, where discrete labels are determined by the majority of certain amount of nearest data points. However, KNN can also be used for regression where the labels are continuous. The label assigned to a test point is determined based on the mean of the labels of its nearest data points. Scikit-learn provides three methods of searching for nearest neighbors: 1) brute force – compare distances of all pairs of data points; 2) K-D tree – use tree-based structures to reduce the calculations of distances; and 3) ball tree – partition data in a series of nesting hyper-spheres when constructing trees. As scikit-learn supports auto method selection based on input data, we use this option. Also, we use the default parameters provided by scikit-learn: 5 nearest neighbors and uniform weights.

Support Vector Machine (SVM):

For regression, SVM [19] finds the classifiers represented by hyperplanes that separate the different groups as wide a margin as possible. The hyperplanes are represented by the normal vector v and the bias b, which can be found by solving a constrained optimization problem:

$$\min_{\omega} \|\omega\| \; A = \pi r^2 \tag{7}$$

$$s.t.\, y_i * (\omega' X_i - \beta) \geq 1, i = 1, \ldots, n$$

SVM can also be used for regression, where similar kernel method is applied.

Multi-layer Perceptron (MLP):

Given a set of features and a target y, MLP [19] can learn a non-linear function estimator for either classification or regression. It trains using backpropagation with no activation function in the output layer, which can also be seen as using the identity function as activation function. Therefore, it uses the square error as the loss function, and the output is a set of continuous values. We use the default parameters of scikit-learn: one hidden layer with 100 hidden units and "relu" as activation function.

4.2 Rolling Methodology

We perform rolling prediction analysis. That is, we train our models based on prior historical data and predict future returns. The procedure then rolls forward by expanding the train set by one day and then repeating the training and prediction procedure. A detailed description is as below.

Suppose we stand on day D_t, and we want to predict the n-day (n>=1) price returns ahead. To allow the prediction to take place at any time of day Dt, we only refer to information up to the previous day D_{t-1}. There are two important considerations:

Our predicted variable (y) is calculated as: $R_t = \frac{P_t}{P_{t-1}} - 1$

and our explanatory variables (X), we can only use variables up to day D_{t-1}. For example, the m-day historical return on D_t: $\mathrm{HR}_{t-m,t-1} = \frac{P_{t-1}}{P_{t-m}} - 1$.

Table 10 provides an example of our data structure.

Table 10: An example of data structure of rolling prediction

Date	Predicted variable (y)	Explanatory variables (X)	
	n-day returns	Historical m-day returns	Historical k-day moving averages
D_t	P_{t+n} / P_t -1	P_{t-1} / P_{t-1-m} -1	SUM(P_{t-k}, …, P_{t-1})/k
D_{t+1}	P_{t+1+n} / $P+1_{t+1}$ -1	P_t / P_{t-m} -1	SUM(P_{t-k+1}, …, P_t)/k

Another problem concerning time series rolling analysis is time series leakage. More specifically, standing on day

Dt, though we have access to historical information (X) up to the previous day (D_{t-1}), but we do not have the predicted variable (y), whose calculation involves the close price on day (t+n). That said, standing on day D_t, if we want to train a model and predict the n-day returns ahead, the train set can only be constructed based on data from day D_0 to D_{t-n} (the predicted variable for D_{t-n} is $R_{t-n} = \frac{P_{t-1}}{P_{t-1-n}} - 1$)

Finally, we repeat our rolling method with a specific example. Suppose we have constructed a time series data set of 1,000 days: the y is a series of 30-day returns and X is a matrix of size 1,000 by 20 (20 explanatory variables). We want to experiment a rolling prediction of 30-day returns. We set the minimum train set size as 100. First, we train a model based on the data from D_0 to D_{99} (the predicted variable for D_{99} is $R_{99} = \frac{P_{128}}{P_{98}} - 1$; then we use the trained model to predict the $R_{130} = \frac{P_{159}}{P_{129}} - 1$ based on X_{130} (a 1 by 20 row vector) which contains information up to day D_{129}. Next, we expand the train set to include data from D_0 to D_{100} and repeat the training and prediction. The analysis is rolled until we get R_{1000}.

4.3 Explanatory variables

Table 11 shows the explanatory variables in our rolling prediction analysis (predicting 30-day returns for Bitcoin). Based on the preliminary analysis above, we decide to exclude USD index, gold, and VIX, due to their relatively low correlations with Bitcoin. The variables are constructed in the abovementioned rolling way and standardized using StandardScaler in scikit-learn, which centers the data with sample mean and the scales them into unit variance.

In addition, we categorize these variables into eleven "information sets". In the later sections, we will examine the relative importance of each information set for Bitcoin, in terms of their contribution to the performance of our machine learning algorithms.

5. Model Results

5.1 Rolling prediction analysis (30-days) for Bitcoin

We recalculate predicted prices based on predicted 30-day returns, as is shown in Figure 11. As the ill-performance of Multi-layer perceptron during the second half of 2017 leads to poor readability, we present results of the top 3 algorithms (in terms of accuracy) from Jan 2017 to Jan 2018 in Figure 12. Obviously, none of them successfully forecasted the big price crash in Jan 2018. On the other hand, Figure 13 and Figure 14 show the accuracy and RMSE, respectively, both of which are calculated in a cumulative way (expanding the data by one prediction for each time). As the number of predictions increases, accuracy of all algorithms stabilizes in the range of 50 to 65 percent.

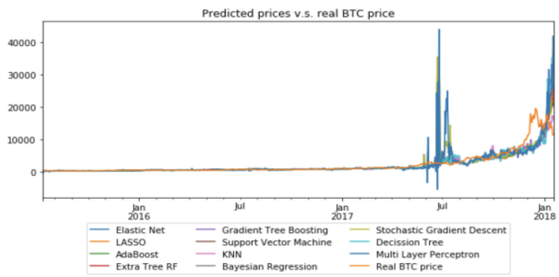


Figure 11: Predicted price vs. Real BTC price (predicting 30-day returns)

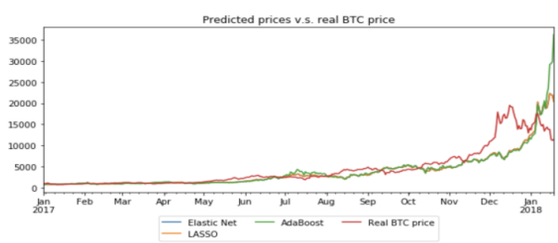


Figure 12: Predicted price vs. Real BTC price (predicting 30-day returns)
Notes: This figure shows results from Jan 2017 to Feb 2018 for the top 3 algorithms (in terms of accuracy).

5.2 Important information sets for Bitcoin

As stated above, to reveal the potentially useful information sources in predicting Bitcoin prices, we categorize all variables into 10 information sets: 1) price returns, 2) price momentum, 3) rolling volatility, 4) volume, 5) S&P 500, 6) Developed equity market, 7) Emerging equity market, 8) commodity, 9) market capitalization weighted returns of cryptocurrencies (crypto VW), and 10) the 30-day rolling correlation of the overall cryptocurrency market (rolling volatility).

We first run the rolling prediction analysis with all information sets as input, and next, we repeat the analysis for 10 times by removing one information set each time. The "relative importance" of each information set is measured as the difference between the accuracies with and without the corresponding information set as input. That is, a positive difference indicates positive contribution of the information set and negative difference implies the opposite.

Figure 15 shows the heatmap presenting the relative importance of each information set for each algorithm. Overall speaking, none of the information sets has significant impact on any algorithms, as the relative importance fall in the range between -0.05 and 0.05. However, a closer inspection would reveal that, on average, rolling volatility (past 15 days and 30 days) and correlation among cryptocurrency market (past 30 days) are useful information for most algorithms, while the market capitalization weighted historical returns (15-day and 30-day) and emerging equity market are the least beneficial.

Table 11: Explanatory variables

	Variable name	Definition	Information set
1	Price_ret10	Historical 10-day price returns	Historical price returns
2	Price_ret30	Historical 30-day price returns	
3	Price_momentum_MA10	The ratio of price to 10-day moving average minus 1	Price momentum
4	Price_momentum_MA30	The ratio of price to 30-day moving average minus 1	
5	Volume_momentum_MA10	The ratio of trade volume to 10-day moving average minus 1	Volume Momentum
6	Volume_momentum_MA30	The ratio of trade volume to 30-day moving average minus 1	
7	Price_volatility15	The standard deviation of the daily price returns over the past 15 days	Rolling volatility
8	Price_volatility30	The standard deviation of the daily price returns over the past 30 days	
9	SP500_ret15	S&P500 historical 15-day price returns	S&P 500
10	SP500_momentum_MA15	The ratio of price to 15-day moving average of S&P500 minus 1	
11	Developed_ret15	MSCI developed equity market historical 15-day price returns	Developed equity market
12	Developed_momentum_MA15	The ratio of price to 15-day moving average of MSCI developed equity market minus 1	
13	Emerging_ret15	MSCI developing equity market historical 15-day price returns	Emerging equity market
14	Emerging_momentum_MA15	The ratio of price to 15-day moving average of MSCI developing equity market minus 1	
15	Commodity_ret15	Bloomberg Commodity Index historical 15-day price returns	Commodity
16	Commodity_momentum_MA15	The ratio of price to 15-day moving average of Bloomberg Commodity Index minus 1	
17	VW_returns10	10-day market-cap weighted returns 57 cryptocurrencies *	Market capitalization weighted returns of cryptocurrencies
18	VW_returns30	30-day market-cap weighted returns 57 cryptocurrencies *	
19	PC1 **	The first principal component of PCA on x-day returns of 57 cryptocurrencies *	Principal components of cryptocurrencies
20	PC2 **	The second principal component of PCA on x-day returns of 57 cryptocurrencies *	
21	Crypto_corr30	The average correlation between the predicted coin and other cryptocurrencies over the past 30 days	Rolling correlation of the overall cryptocurrency market

Notes:

1. * All the "57 cryptocurrencies" above means the 57 cryptocurrencies which have full data back to January 1, 2015.

** The PCA is conducted in a rolling base.

5.3 Rolling prediction analysis for other Cryptocurrencies

We also examine the analysis for the 57 cryptocurrencies with available data back to January 1, 2015. Many cryptocurrencies are slightly predictable if the algorithms with the highest accuracies are chosen. Bitcoin yields the highest best accuracy as displayed in Fig. 14 below. Another finding is that higher prediction accuracy is associated with larger market capitalization and lower volatility. But we also see that higher predictability is accompanied by larger dispersion among different algorithms.

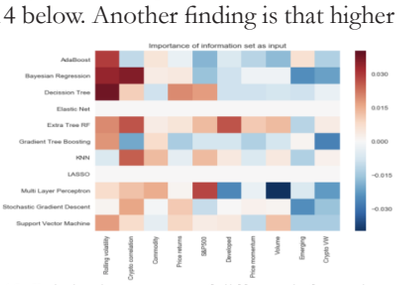


Figure 13: Relative importance of different information sets on predicting 30-day Bitcoin returns

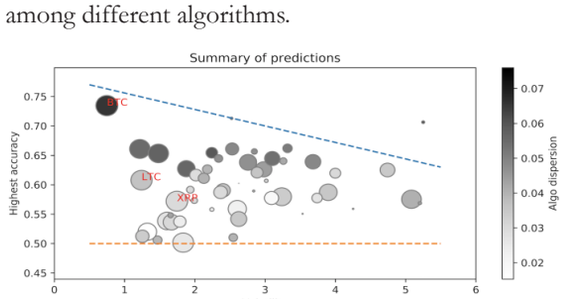


Figure 14: Summary of rolling prediction results (predicting 30-day returns)

Notes:
1. The volatility is calculated by annualizing the daily volatility over the sample period (Jan 1, 2015 - Feb 18, 2018). We limit the range of x-axis to be [0, 6] for the purpose of readability, and as result 8 cryptocurrencies are removed from the figure.
2. The highest accuracy: we run 11 algorithms for each cryptocurrency and pick the one with highest accuracy.
3. The size of dots is based on the market capitalization of each cryptocurrency, i.e., Bitcoin is the largest.
4. The color of dots is based on the standard deviations of accuracies generated by 12 algorithms (algo dispersion).

Fig. 15 presents a performance summary of the 12 algorithms. LASSO dominates in predicting the 30-day returns of cryptocurrencies. And one average, all algorithms generate accuracies in the range of 50 to 60 percent, which is above random guess but still far from accurate prediction.

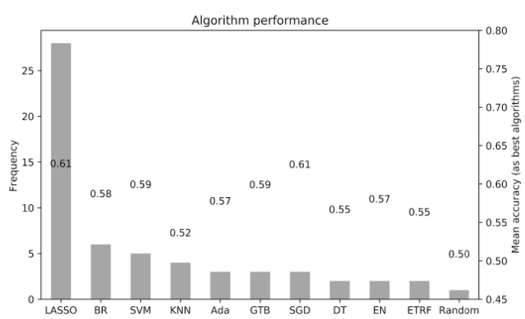


Figure 15: Summary of algorithm performance (predicting 30-day returns)

Notes:
1. The frequency is the times an algorithm performs the best among the 11 algorithms plus random guess.
2. The mean accuracy is calculated by averaging the accuracies when the corresponding algorithm performs the best.

6. Conclusion

Cryptocurrencies have captured the attention of many investors across the spectrum from retail to institutional - see Liew and Hewlett [14]. In this work we extend our understanding of the behavior of cryptocurrencies. We document several interesting findings. First off, we find that PCA reveals that the return generating process is much more complex than that for stock returns. Generally speaking, the financial community agrees that the "market" is the first dominant PCA in stock returns. However, for cryptocurrencies daily returns reveals that in some period there exists a single dominant component however, in the most recent prior year there appears to be two components that help explain the variation of the cryptocurrency returns. Next, we document a strong beta-in-the-tails hidden risk associated with Bitcoin daily returns. Similar to hedge fund cryptocurrencies may have some unstable tail behaviors.

Our analysis of machine learning algorithms applied to the data from cryptocurrencies hints that predictability may be difficult and there are many heterogeneous effects here. Some information sets perform better with some family of algorithms, and larger cryptocurrencies with lower volatility maybe more predictable than smaller cryptocurrency with higher volatility. Some care should be taken given the many moving parts across the cryptocurrency industry. The complexity will lead to possible risks of overfitting machine learning algorithms.

References:

[1] I. Madan, S. Saluja, and A. Zhao, "Automated bitcoin trading via machine learning algorithms," URL: http://cs229. stanford. edu/proj2014/Isaac% 20Madan, vol. 20, 2015.

[2] A. Greaves and B. Au, "Using the bitcoin transaction graph to predict the price of bitcoin," No Data, 2015.

[3] S. McNally, J. Roche, and S. Caton, "Predicting the price of Bitcoin using Machine Learning," in 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), 2018, pp. 339–343.

[4] Z. El-Abdelouarti Alouaret, "Comparative study of vector autoregression and recurrent neural network applied to bitcoin forecasting," PhD Thesis, ETSI_Informatica, 2017.

[5] F. Mai, Q. Bai, J. Shan, X. S. Wang, and R. H. Chiang, "The impacts of social media on Bitcoin performance," 2015.

[6] E. Stenqvist and J. Lönnö, Predicting Bitcoin price fluctuation with Twitter sentiment analysis. 2017.

[7] Y. B. Kim, J. Lee, N. Park, J. Choo, J.-H. Kim, and C. H. Kim, "When Bitcoin encounters information in an online forum: Using text mining to analyse user opinions and predict value fluctuation," PloS one, vol. 12, no. 5, p. e0177630, 2017.

[8] J. Kaminski, "Nowcasting the bitcoin market with twitter signals," arXiv preprint arXiv:1406.7577, 2014.

[9] J. Chu, S. Nadarajah, and S. Chan, "Statistical analysis of the exchange rate of bitcoin," PloS one, vol. 10, no. 7, p. e0133678, 2015.

[10] M. Balcilar, E. Bouri, R. Gupta, and D. Roubaud, "Can volume predict Bitcoin returns and volatility? A quantiles-based approach," Economic Modelling, vol. 64, pp. 74–81, 2017.

[11] N. Indera, I. Yassin, A. Zabidi, and Z. Rizman, "Non-linear autoregressive with exogeneous input (NARX) Bitcoin price prediction model using PSO-optimized parameters and moving average technical indicators," Journal of Fundamental and Applied Sciences, vol. 9, no. 3S, pp. 791–808, 2017.

[12] I. Georgoula, D. Pournarakis, C. Bilanakos, D. Sotiropoulos, and G. M. Giaglis, "Using time-series and sentiment analysis to detect the determinants of bitcoin prices," Available at SSRN 2607167, 2015.

[13] D. Garcia and F. Schweitzer, "Social signals and algorithmic trading of Bitcoin," Royal Society open science, vol. 2, no. 9, p. 150288, 2015.

[14] J. K.-S. Liew and L. Hewlett, "The case for Bitcoin for institutional investors: Bubble investing or fundamentally sound?," Available at SSRN 3082808, 2017.

[15] F. R. Edwards and M. O. Caglayan, "Hedge fund performance and manager skill," Journal of Futures Markets: Futures, Options, and Other Derivative Products, vol. 21, no. 11, pp. 1003–1028, 2001.

[16] J. Liew, "Hedge fund index investing examined," Journal of Portfolio Management, vol. 29, no. 2, p. 113, 2003.

[17] W. F. Sharpe, "Capital asset prices: A theory of market equilibrium under conditions of risk," The journal of finance, vol. 19, no. 3, pp. 425–442, 1964.

[18] J. Lintner, "The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets: A reply," The review of economics and statistics, pp. 222–224, 1969.

[19] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[i] The data of Ethereum provided by coinmarketcap.com starts on Aug 7, 2015.

[ii] The average history is calculated using the data for only 2015 to 2017, thus it is not the exact length of average history. But as most of the top 100 cryptocurrencies came into being after 2015, this calculation approximates the real length of average history.

[iii] For horizontal axis, cryptocurrencies are ranked by market capitalizations from the right (large) to the left (small). For vertical axis, they are ranked by market capitalizations from the top (large) to the bottom (small).

[iv] Accessed on Mar 14, 2018: https://www.cnbc.com/2017/11/27/bitcoin-exchange-coinbase-has-more-users-than-stock-brokerage-schwab.html

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
JL[1], RL[2], TB[2], and AS[3] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Photo by Caspar Camille Rubin on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(6)2019

Blockchain Investigations: Beyond the 'Money'

Simon F. Dyson
NHS Digital, Leeds, U.K
Correspondence: simon.dyson@protonmail.com
Received: 18 July 2019 **Accepted:** 7 August 2019 **Published:** 13 August 2019

Abstract

Cryptocurrency investigations have centered almost entirely around the transfer of value "money" or a cryptocurrency asset. The use of cryptocurrency for illicit purposes, especially Bitcoin, is well documented both in academic writing, media reporting and even film documentaries. The infamous SilkRoad marketplace in addition to the millions of dollars spent within dark markets on drugs, guns and assassinations have grabbed the headlines. This paper looks at how blockchain is creating new areas of investigation that are yet to be explored in detail. This scenario-based research examines the hosting of stolen data (P.I.I) personal identifiable information on a distributed blockchain host where the data is also accessible. The platform used is based on Ethereum infrastructure but demonstrates just one available platform that poses the paradigm. The paper examines the considerations through the lens of an incident responder /cyber investigator, forensics examiner and data controller. The scenario highlights distinct differences in considerations from a traditional response compared to dealing with the immutable and unstoppable distributed technology. The paper concludes that more is needed to be done to understand digital forensics in the blockchain era and the need to develop beyond track and trace in the cryptocurrency investigative toolbox. The discussion also brings forth how data retention and GDPR requires consideration when applying it blockchain systems.
Keywords: *Blockchain, Distributed-hosting, Distributed-storage, Ethereum, Swarm, Forensics*

1. Introduction

Research into cryptocurrency has focused generally on the transfer of value. The use of cryptocurrency in large scale criminal activities is well documented in cases such as the Silk Road drugs marketplace or in large ransomware campaigns such as Wanacry. The focus has been on the "follow the money" aspect in order to locate the perpetrators. The underlying technologies have however developed since the inception of Bitcoin in 2008. Blockchain technology is now scaling and developing new features now able to support multiple data and communication protocols across its stack. Law enforcements focus has remained around the large cryptocurrencies however the use of smart contract technology and now distributed computing and storage creates a new set of problems for investigators and those responding to incidents. This paper sets out a common leak of personally identifiable information (P.I.I) where it is hosted on blockchain technology and how the traditional responses are required to adapt. The scenario uses Ethereum and its related technology to host files. There are a number of cryptocurrency/ blockchain assets that can host the data in a similar nature. A distributed blockchain by its design contains properties that are not inherent in traditional hosting services. A blockchain is immutable in general terms so they are unstoppable and have no central authority or body.

2. Scenario and Roles

The scenario is to replicate the discovery of files taken containing (P.I.I) personally identifiable information from a server and hosted externally. The hosting, however, will take place on a distributed blockchain system. In order to establish if the PII information is legitimate, a comparison will need to take place, this will entail a visual comparison of the data. A forensic comparison of the data will need to be conducted using traditional methods to hash the file contents and examine EXIF data contained within the file. Cyber investigators searching for online hosted material will examine records of web hosting companies to see the I.P data for the hosting company and registrar details such as WHOIS information. Data controllers hold the responsibility for the holding storage and protection of the data. The data controller will need to make

decisions about steps that are possible to minimise the damage. Each role will respond using traditional methods and record the findings. A discussion section will reflect on the approaches and highlight quick wins and areas that require further work.

2.1. Cyber Investigator / Incident Response

This role will respond to initial reports and record and utilise OSINT Open Source Intelligence sources to discover evidential information to assist the investigation. The coordination of tasks to systems administration for internal log investigation and other closed source materials will be conducted.

2.2. Digital Forensics

Examination of digital material will be conducted by the digital forensics team member. This will include host forensics and also comparison of highlighted online material where required. They will take a forensic analytical approach in order to approach the problem.

2.3. Data Controller

As the responsible owner of the data, the controller will be consulted on the state of the investigation. The controller will establish additional tasks that would assist to protect the data or prevent further dissemination.

3. (GDPR) General Data Protection Regulation

In May 2018, the General Data Protection Regulations came into effect and incorporated existing legislation to protect people's data and their rights. GDPR is covered in depth in numerous resources so in this section a focus on some key themes that will be later visited will be briefly documented. GDPR covers data that belongs to people who are in the GDPR aligned nations, Europe and some additional territories. The rules outlined cover those entities that are considered a data controller or processor. A controller is the entity that holds the data for purpose, and they will process for their agreed business requirements. A processor is considered a third party that is doing something with the data on behalf of the controller, an agreement will define what that process is. GDPR defines that personal data can generally identify somebody or be used for that purpose and it offers protection to that data. There are also additional protections to sensitive personal data that protects special characteristics. The term PII (Personal Identifiable Information) is not defined by GDPR but is commonly used and will be covered as personal data under GDPR and this scenario. There are 8 individual rights that are listed under the new act. These rights are; the right to be informed, the right of access, the right of rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights of automated decision making and profiling. The right to erasure is one of the more complex and powerful rights that is created in the new act. This right caused many to question the ability of blockchain to function under such a regime. The conflict of immutability as an absolute property of blockchain in comparison to the legal requirement to deletion of GDPR is cited as pushing solutions to standard databases[1]. There are other potential ways forward such as gaining consent for perpetual processing. It is argued that address hashing is pseudonymous and that the effort to de-obfuscate a hash is disproportionate so would stand as it would not likely identify an individual. Permissioned blockchains are also suggested in order to control the data but they don't fit the public and permissionless systems of large cryptocurrency structures. There are also systems using new encryption methods such as zkSNARKS and RingCT methods that could protect data throughout the complete process [2]. Tokenised solutions are appealing although they may require off-chain processing but the use of distributed storage is possible through Ethereum – SWARM or IPFS[3]. The use of a smart contract with an upgradable contract section could allow amendable content but record the transaction metadata and deletion process[4]. Implemented correctly the ability to control and make accountable sharing structures with blockchain could strengthen systems to comply with GDPR.

4. Decentralised Blockchain Storage

Decentralised networks have been utilised for numerous cryptocurrency projects with the ability to trade tokenised value they have become used for a new wave of "Digital money". Blockchain technology itself has evolved behind the headlines of boom and bust price fluctuations and Silk Road drug dealing dark markets. The introduction of Smart Contracts utilised by Ethereum and now other blockchain technologies allows Turin complete languages and sections of code to produce complex computational outputs. Using resources on Ethereum for example is expensive if you process through the Ethereum Virtual Machine (EVM) the world computer, each byte and code execution has a price to pay using "gas". Utilising "gas" small amounts of the currency this ensures that the "halting problem" is addressed and a denial of service attack or forever loop will be too expensive to conduct. There are however a number of blockchain projects that are looking to use an additional protocol or system to provide blockchain storage using peer to peer nodes incentivised to the system. The creation of a decentralised storage system solves a number of computing problems, it creates resilience as files are striped across multiple nodes in a system. The ability to reside on multiple nodes reduces single points of failure or risk from physical events such as earthquake, tsunami or power outages. A decentralised system uses nodes in the control of world users who are incentivised to "mine"

or provide a service similar to miners and Bitcoin nodes. Services such as Dropbox operate a storage system that allows a cloud storage system however the service is a centralised under one organisation. The company is subject to US law, so privacy therefore is not guaranteed as the ability to access, subpoena, court order and secret service oversight. Nodes in a decentralised generally hold only partial fragments of the file so physical integrity is maintained as the file portion is fragmented and optionally encrypted. There are a number of decentralised file storage systems namely, IPFS (Inter Planetary File System) developed by Protocol labs this part of the system allows for distributed storage, Filecoin [5] is an additional service to incentivise storage by paying miners to store. IPFS as a protocol is used by a number of other projects and is cross blockchain agnostic [6]–[8]. In addition to the above there are other distributed storage projects in various phases of production these include Storj, Sia and Maidsafe [9]–[11]. Ethereum has its own sub project called "Swarm" this will be explored in the next section.

5. Ethereum Swarm

Swarm was designed to create a system to store dapp (Decentralised Application) code, resources on a peer2peer system. The ability to access material outside of the Ethereum chain reduces the cost of storing larger files or code in a smart contract off chain where it is cheaper to store. Dapps by their nature are applications that are not a singular stored item, therefore the use of larger code sets and files to produce more complex and visually focused items require more storage. The ability to access resource from the Swarm protocol layer allows this exchange maintaining a fully decentralised eco-system. The system will maintain the properties of a truly decentralised system transaction layer on chain and storage another chain. This makes it non-censorable, fully redundant / resilient, DDOS resistant, highly available and secured by encrypted cryptographic signatures. Ethereum integration is used with a Swarm node and a Geth node, Geth is a "GO" programming language implementation version of Ethereum. This scenario will utilise both Ethereum Geth and Swarm working on the Ropsten test net, the closest to the production service. Ropsten allows integration with the services as if it was connected to the Mainnet where the technology is already live, with the advantage of not costing real Ethereum and "gas" to test and operate. Geth version (1.8.20-stable) and Swarm version (0.3.-stable) [12], [13].

6. Blockchain Domain Naming

The (DNS) Domain Name System is used to assist with searching the internet, it translates a human readable (URL) Uniform Resource Locator into the relevant Internet Protocol Address (I.P). This directs a query such as www.a_web_address.com to the root servers to the (TLD) Top Level Domain and to the domains name server that holds the record of the I.P address example 8.8.8.8. The ability to store domain naming information on a blockchain has existed for some time with services such as Namecoin offering various services including a name resolution stored on blockchain. The criminal use of decentralised DNS services does exist but is not extensively used [14], [15], [16]. The discovery of a recent botnet that was discovered to be cleaning up bad botnets was observed in the wild using Emercoin's distributed DNS implementation [17].

The (ENS) Ethereum Naming Service provides similar functions to a DNS system and is held and operated over the Ethereum blockchain [18].

7. Method

In order to replicate an intrusion event a number of files with identifiable meta-data will be created and hosted on a virtual machine. A base forensic examination will be completed to display (Modified, Access, Created) MAC date and times, Meta data that may also include geo-data serial number or other EXIF data. The scenario host is a machine running Windows 7, the host contains a folder on the desktop entitled "Work_items" containing related documents. The documents include an image of a passport that is used for identification of the customer in this scenario and contains PII information. In addition to the image are further documents including an XLS and CSV files, this contains customer details including PII data.
Scenario – a message is received by phone that a leak of company information has occurred, and a website URL is provided.

7.1. Investigation phase

7.1.1. Cyber investigator / Incident response

The cyber investigator is initially passed information provided by a telephone call that states the web URL hosting the company's potentially stolen information. The URL is placed into a browser on a standalone environment to ensure the reported event is not a social engineering ruse and to protect the main corporate network from malicious activity. Initial activity will ensure the link is live and that the data appears to be present, accurate recording of event will take place including a screen capture of the page. A capture of the page and the source code alongside an abstraction of pertinent files will be completed for further analysis. Data will be needed to be compared to corporate data to ensure the attack is a legitimate attack and is not a hoax. OSINT Open source intelligence will reveal additional information about the web hosted material. The source code may reveal hosting details or frameworks used to create the site, these may include author and other

meta data of interest to the cyber investigator. Source code can also reveal other links hosted on other sites or resources that may allow additional investigative leads. As discussed in Open source intelligence techniques by Michael Bazzell there are numerous services that assist in the location of a website these include some of the following important areas [19]:

- Protocol
- Website name and top-level domain information
- I.P address
- Whois
- Registration data
- e-mail addressing
- The hosting company (Server hosting)
- Domain hosting (Name holder)
- DNS zone tranfers
- Registrar change history
- Ad-sense / analytical tokens – numbers
- Robots.txt
- Shodan

7.1.2. Digital Forensics

Following information from the original call the forensic response team will react to the main areas of data storage. The firewalls and server logs will be checked for intrusion or indicatiors of compromise. The data storage servers will be examined, and a RAM dump will be executed on each device. This will capture processes, network connections and master file table entries that will enable initial triage to identify any breach information. Identification of the information can take place by using methods such as hashing values and searches for names or data from the leaked source to discover if the information is owned by the company.

The order of volatility is Processor, Network, Main Memory, Semi-volatile, Resident data, Remotely logged and any data on archival media [20]

In this scenario, live data should be considered before a raw dump, if the memory dump crashes then the machines critical live data could be lost. A memory dump should be obtained and analysed the machine can be shut down and retained for a full forensic image if required.

The forensic response to an incident would record the process using contemporaneous notes and photographs.

Examine with the visual inspection of a machine and examination of live desktop activity

- Live data – command line – time & date, network connections (netstat), current user, tasklist
- Memory RAM capture – full, Dumpit.exe
- Any operational/incident specific investigation tasks.
- Power down machine when examination complete retain for full disk imaging.

7.2. Operational Phase

7.2.1. Data Controller

The General Data Protection Regulation GDPR introduced in 2018 enforces businesses and those who control data to protect the rights of the citizens whose data is held. Each European country or participating country must introduce a body to monitor and administrate enforcement of fines and breaches of the code. In the U.K the ICO (Information Commissioners Office) hold this position, they provide guidance, advice and are the primary contact if a breach occurs. GDPR requires a company that is aware of a breach of personal data to report to the supervisory authority in the U.K to the I.C.O within 72 hours of been aware that a breach has occurred. Where it is likely that a breach will affect the rights and freedoms of the individuals on who the data relates then they must also be informed "without undue delay" [21]. The principles that are to be considered around data are the security triad of Confidentiality, Integrity and Availability. The rights of the data subject are to be considered and notification made if the breach is likely an adverse effect on the data subject. An example would be where full personal data and financial data are lost these are likely to incur subsequent fraud offences using the identities of the data subject [22].

GDPR therefore requires all companies that process data in the EU or about people in the EU to have policies and procedures to detect, investigate and report on incidents with accuracy.

GDPR has a number of requirements in relation to information to be provided to the supervisory body in response to a breach. The below section details the requirements and these points will be addressed in the breach investigation plan for the data controller.

- Description of the personal data (data categories, number of individuals, number of records)
- An assessment on potential consequences following the breach
- Following the breach what measures have been or will be taken in order to mitigate risk and harm following the breach. (ICO GDPR breach guidance [23]).

It is obvious from the above requirements that a response from the cyber investigators / digital forensic team is essential in providing timely and accurate reporting to ensure the data controller can make informed decisions on the subject.

8. Initial Response

The scenario starts with a report of information reported into the Cyber security team. This was initially reported as a URL and the action will start by the teams who will perform incident response according to their response plans. The URL was reported as:
https://swarm-gateways.net/bzz:/9eaab00f3eb97cfc731ae095 8aa2c9f249a2cd0045dae7bec659e736c920112a/

9. Findings

9.1. Cyber Findings

Initial actions resulted in the preservation of the online material and the capture of HTML information of the files hosted on the site. The site contained three items of interest an image of a passport and two data files for download. The nature of the message on the site suggested an insider threat this requires further internal work to attribute.

The image was reverse searched to see if the image was hosted elsewhere on the web, this was to establish if this was disseminated elsewhere or if it was a hoax using another source. The EXIF data was examined from the passport photo, this provided metadata that included time dates, make, model, image composition and crucially geo location, see Fig 1. This established the passport image was taken in a popular café used by the sales team to on-board new customers close to company premises. This provided metadata that allowed attribution in this circumstance in the scenario set out.

Basic Image Information

Target image: https://swarm-gateways.net/bzz:/9eaab00f3eb97cfc731ae0958aa2c9f249a2cd0045dae7bec659e736c920112a/IMG_20181231_083220.jpg

Description:	dav
Camera:	Huawei SNE-LX1
Lens:	4 mm
Exposure:	Auto exposure, Program AE, 1/999,963,365 sec, f/1.8, ISO 400
Flash:	none
Date:	**December 31, 2018** 8:32:20AM (timezone not specified) (12 days, 2 hours, 57 minutes, 37 seconds ago, assuming image timezone of GMT)
Location:	Latitude/longitude: **53°** 47' 43.4" North, **1°** 32' 51.5" West (53.795395, -1.547638) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 0 meters (0 feet) below sea level Timezone guess from earthtools.org: GMT
File:	**3,840 × 5,120** JPEG (**19.7** megapixels) 2,648,563 bytes (2.5 megabytes)

Figure 1. EXIF data from the passport image

9.2. OSINT – Findings

The domain was subject to a reverse look up, WHOIS search, and it revealed a hosted service. The information was shown to a Windows Azure instance based in the Netherlands. The domain registrar shows a named contact with addressing. The I.P address was established with versioning and port numbers on a Shodan scan that revealed web ports 443 and 80 were the only active services see Fig 2.

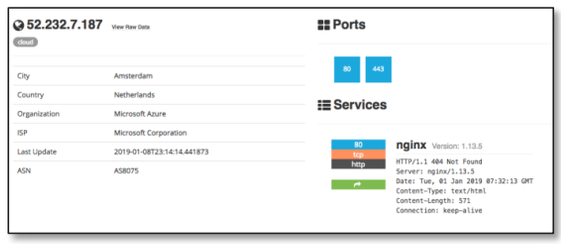


Figure 2. Shodan results from the OSINT scan

9.3. Forensic Findings

The files recovered in the discovery phase were provided for forensic analysis. The items were hashed, and the metadata examined. This information enabled identification of the company database server where the data was likely to be stored. The forensic actions as previously described were enacted capturing live, ram and forensic level data. The company server was examined, and activity was discovered around the folder of interest using Volatility. Artefacts were found in the MFTPARSER and SHELLBAGS modules that allowed activity from MAC (Modified Accessed Created) times to create a timeline of suspect activity. In addition, access to the registry keys through the Volatility modules allowed the USBSTOR to show activity in the timeframe, giving make model and GUID for the suspect USB. Table 1 shows the hashing data and the matches.

Table 1. Shows the hash detail and if the hashing matched from the blockchain storage and the host system

MD5	FileNames	Hash Match
8058eaa53e21f01cc974162ef5b900b5	\Full_customer_data.csv	Match
5370bda04d665230637191eb571100cf	\IMG_20181231_083220.jpg	Match
0be46dd2062e4b421e9b606cbe28d76e	\The_customer_data.xls	Match

10. Data controller – next steps

In this section discussed is considerations of the data controller for the blockchain element and not the general actions of the controller, the data is personal and a referral to the ICO is required in the time frames set. The current actions would now look to reduce the spread of stolen data. Legal action against the hosting company or a complaint procedure to the hosting services would be sought. A powerful tool for removal of data is the Subject Access Request procedure where a data subject has rights under GDPR for enforcement. Legal proceedings are complex and civil claims can potentially disrupt or force servers to shutdown such services as detailed between PML vs unknown [24]. This shows the complexity and interactions that a hosting company can be pursued to reduce the impact and required to remove content under national and international law.

11. Initial conclusion standard response

The conclusion established from the above investigation at this stage are mixed. The captures have been

performed to an adequate standard but there are some items that confuse the investigation. The domain and services discovered in the phase point to the "swarm gateway" a service allowing a pass through of web traffic to the Ethereum network. The Microsoft Azure server hosted in The Netherlands and the registrar name highlighted is a project lead on the Swarm service. The registrar and the WHOIS information all resolve to an unrelated subject not the true location of the data, just the portal to find it. It is important to relay that there is no information hosted on the server it is a HTTP/S proxy API that allows access to the Swarm network. There are other gateways such as https://ensgateway.com/ and IPFS specific gateways. What legal action can be taken against a portal that contains no data but provides access. Similar to that of a tor gateway or node allowing access to a darkmarket.

The forensic investigation however demonstrates that the files and data hosted on the Swarm system are not altered and retain important meta-data. The comparison shows that the integrity of the file is retained and the hashing value and EXIF data is retained when recovering from the Swarm network this confirms attribution for the company.
The investigation can conclude that the personal information has been taken from the company and this has been conducted by an individual with authority to access the service. The attack was conducted by exfiltrating data and removing it on a USB device this is a classic insider attack. The file is hosted on an unstoppable blockchain where no legal avenue exists to remove or request a cease and desist.

12. Blockchain investigations

The Swarm decentralised system operates using the URL scheme identifier as "BZZ:" the location of the file is designated by a Swarm hash or an ENS assigned domain such as "photoalbum.eth".

In the example, the ENS domain is assigned as "Unstoppable.eth" - Ropsten testnet and this resolves the content of the stolen items as examined previously to the swarm hash.

There are a number of components that work to resolve the addressing. At high-level an Ethereum registry that tracks the domains and sub-domains on the network. There are additional registrars that are involved in the hosting and reselling activities of ENS names. The Ethereum Naming Service is used to bid and retrieve a human readable address such as "Unstoppable.eth" and this is done using an Ethereum account. On successful allocation of the bid the name is under the control of the account and using Smart contract calls can be accessed and communicated with to set the requirements in the contract. The ENS record requires a resolver assigned that links the human readable name, name-hash, account or content to a resolver. There is a public resolver frequently used however custom resolvers are possible to create and likely to be adopted in some Dapps or other services. A name hash is used to represent the human readable name and is combination of cumulative hashing of domain and naming using Keccak hashing [18]. Fig 3 shows a walkthrough of the process.

In the example of the scenario the content hash was created by Swarm '9eaab00f3eb97cfc731ae0958aa2c 9f249a2cd0045dae7b ec659e736c920112a" this hash was used to search the Swarm node to retrieve the full content. The Swarm hash is created using a chunk hash function with a merkle tree, this is currently formulated

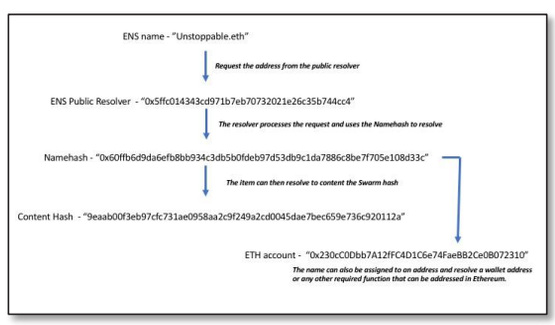


Figure 3. A breakdown of the ENS and the different elements involved in name resolution

using a 32 byte Keccak(256)SHA3. It is possible to create a hash of just a file or similarly in this case a folder with linked resources and files. In the meta-data for the html file the linked images are referenced as the hash and file Fig 4.

```
---Links---
1)  href="https://swarm-gateways.net/bzz:/9eaab00f3eb97cfc731ae0958aa2c9f249a2cd0045dae7bec659e736c920112a
/The_customer_data.xls" download=""
```

Figure 4. Web link that shows the Swarm hash in the HTML link data from the page

In Fig 5 displayed is a resolved address through the ENS service linking to the swarm hash in this case "photoalbum.eth". To discover the hash the ENS address is resolved to an account the contract held on the account can be searched for the "setContent" function as shown in Fig 6.

```
<!DOCTYPE html>
<!-- saved from url=(0047)https://swarm-gateways.net/bzz:/photoalbum.eth/ -->
<html slick-uniqueid="19"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
```

Figure 5. Web link that shows an ENS address in the HTML link from the page

```
Function: setContent(bytes32 node, bytes32 hash)

MethodID: 0xc3d014d6
```

Figure 6. Method setContent function applying the hash to the node address

ENS names can also be applied to accounts so unstoppable.eth can applied to an Ethereum account / wallet and be used instead of the long account address.

Fig 7 shows the name, resolver and account details assigned and revealed with in an ENS search within myetherwallet.com (Ropsten).

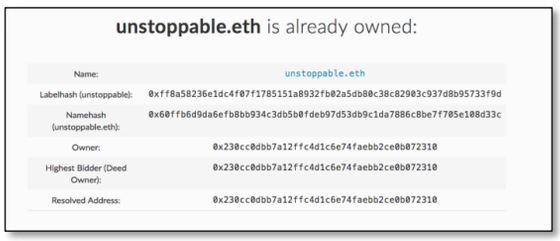


Figure 7. ENS reverse lookup that shows the Name and additional bidding and resolved address

13. Discussion

Figure 7. ENS reverse lookup that shows the Name and additional bidding and resolved address

The ability to host decentralised resources and store material that would be traditionally held on centralised services changes some of the traditional methods of search. This scenario has demonstrated how material can persist beyond the normal experience of investigators creating an unstoppable hosting problem. The practical element demonstrated the use of the Ethereum network, just one of the technologies available to perform distributed storage. The ENS Ethereum Naming Service also provides the ability to link to TLD domains such as .xyz and .luxe. It is understood that the DNSSEC and the TLD integration will not likely resolve correctly with ENS as the DNS browser protocol may override the resolving [25]. There were a number of limitations and technical issues that could not be overcome to test a .xyz domain with any objectivity or confidence. The Ropsten testnet had some service issues during my testing with ENS and syncing, this included using the third-party API Infura that demonstrated the same behaviour. Where required I have used Ropsten and confirmed behaviour across the Mainnet with alternatively hosted sites. There are interesting uses of ENS and DNS hosted on Ethereum, the EthDNS system is prototyped and documented that uses DNS records stored on Ethereum [26]. There are potentially interesting attack vectors if Swarm and ENS became mainstream the use of a bad resolvers in new "Dapps" for example. IPFS also needs to be investigated to understand how it can be used in addition to existing technology or integration with other blockchain technologies. As the example shows the ability to bring up a node write information into the distributed storage is possible both quickly and cheaply, removal of the node from the system still allows the new files to remain. Attribution using a blockchain explorer allows account identification additional resources, identifiable information and linked smart contracts. The layers of investigation cut across web technology, blockchain account records, smart contracts, blockchain naming service, blockchain storage and the host machine. These can lead directly to additional accounts that may identify cryptocurrencies entering or leaving the system. The ability to interact with a smart contract using privacy focused technologies such as zkSNARKS or private smart contracts such as Enigma allow data or image sharing autonomously with strong encryption [27]. The ability to create a photo-sharing application for payment with content hosted on decentralised storage can be achieved using privacy focused methods in addition to blockchain technologies.

What is demonstrated is a need to understand the sources of hosted material as distributed storage becomes wider spread in its adoption. Hosting malware on distributed storage or indecent images of children will require investigators and responders to locate all the sources of material. In the examples shown it is possible to make attribution to file access and use for forensic examination. File signatures, hash values, hosted distributed domains, protocol specific URLs, e.g. BZZ or IPFS can be extracted. In incident response scenarios, the ability to source and collect the sample for reverse engineering will be essential for mitigation and research. Virus scanning and network protection rules could be used to search detect and block hosted material entering or leaving a network. Fig 8 shows the host and file access to the blockchain via Blockchain node / software or via internet gateways.

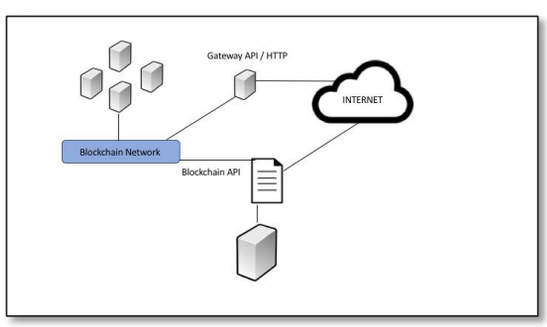


Fig 8 shows a host connecting via the blockchain protocols or via an internet gateway

14. Conclusion

This scenario has demonstrated it is possible to store content persistently on blockchain technology allowing access to those on the blockchain and to the internet through internet gateways. Decentralised storage remains uncensorable with no technical recourse to remove or even request for lawful motions against its storage. There are no regulations such as GDPR, local laws, state, or international law that have any power to control or remove it. The hosting of resources such as images or files on distributed file storage requires additional investigative methods to discover the source and linked information. The ability to attribute the access or presence of an illegal image or document can be reliable proven using hashing protocols used in Ethereum Swarm, the Swarm hash and the temporal

data from the blockchain against fragments held on the host. The requirement to recover electronic data stored or what was accessed is needed in E-discovery and for corporate legal compliance, so the need exits to be able to seek and find documents hosted as described. Malware researchers require the source file to reverse engineer or perform static analysis so the ability to access blockchain storage to recover such files along with additional threat intelligence from linked accounts and blockchain naming is essential. In this case forensic artefacts were not interfered with in terms of their integrity, this is good news for forensic investigators wanting to review rich sources of meta-data. This was only performed on the Ethereum Swarm and other storage systems may also leave metadata or artefacts, a potentially important forensic research area. Research on distributed storage is still focused on the introduction, development, scalability and the performance of the technology. There are clearly vast gaps in literature around the use and long-term performance behaviour as the technology is rapidly evolving. Blockchain forensics has focused on cryptocurrency track and trace but the evolvement of smart contracts and now storage and computational resource will be a future frontier. It is unclear on the adoption of these technologies to long-term adoption, but a new challenge and knowledge gap could appear overnight. Blockchain will undoubtable continue to pioneer computational breakthroughs but new paradigms and challenges exist in its wake. The misuse cases should be considered and researched to compliment blockchain development as a global revolution.

References:

[1] F. January, M. Ii, F. I. Directive, R. R. Review, E. Union, G. Data, P. Regulation, and T. Gdpr, "The rise of the regulator may lead to trouble for the blockchain," pp. 1–2, 2018.

[2] C. Salmensuu, "General Data Protection Regulation and the Blockchains," Liikejuridiikka, no. 1, p. 92, 2018.

[3] B. Ramsundar, R. Chen, A. Vasudev, R. Robbins, and A. Gorokh, "Tokenized Data Markets," 2018.

[4] N. Vergauwen, "Upgradeable Smart Contracts – Hacker Noon," Medium - Hackernoon, 2018. [Online]. Available: https://hackernoon.com/upgradeable-smart-contracts-a7e9aef76fdd. [Accessed: 15-Jan-2019].

[5] "Filecoin - Website," 2019. [Online]. Available: https://filecoin.io/. [Accessed: 15-Jan-2019].

[6] "IPFS is the Distributed Web," 2019. [Online]. Available: https://ipfs.io/. [Accessed: 15-Jan-2019].

[7] J. Redman, "BCH-Powered Bitcoin Files Project Adds IPFS Support - Bitcoin News," News-Bitcoin.com, 2018. [Online]. Available: https://news.bitcoin.com/bch-powered-bitcoin-files-project-adds-ipfs-support/. [Accessed: 06-Jan-2019].

[8] M. Zalecki, "Using IPFS with Ethereum for Data Storage | Tooploox," TOOPLOOX - WEB, 2018. [Online]. Available: https://www.tooploox.com/blog/using-ipfs-with-ethereum-for-data-storage. [Accessed: 06-Jan-2019].

[9] "MaidSafe," 2019. [Online]. Available: https://maidsafe.net/. [Accessed: 15-Jan-2019].

[10] "Sia," 2019. [Online]. Available: https://sia.tech/. [Accessed: 15-Jan-2019].

[11] "Storj - Decentralized Cloud Storage," Storj - Decentralized Cloud Storage. 15-Nov-2017.

[12] "Go Ethereum," Geth. [Online]. Available: https://geth.ethereum.org/. [Accessed: 15-Jan-2019].

[13] "1. Introduction — Swarm 0.3 documentation," Swarm read the docs, 2019. [Online]. Available: https://swarm-guide.readthedocs.io/en/latest/introduction.html. [Accessed: 15-Jan-2019].

[14] R. Amado, "How Cybercriminals are using Blockchain DNS | Digital Shadows," Digital Shadows_ (Web), 2018. [Online]. Available: https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-using-blockchain-dns-from-the-market-to-the-bazar/. [Accessed: 14-Jan-2019].

[15] "Namecoin," Namecoin (Web), 2019. [Online]. Available: https://namecoin.org/. [Accessed: 14-Jan-2019].

[16] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack : A Global Naming and Storage System Secured by Blockchains," USENIX Annu. Tech. Conf., pp. 181–194, 2016.

[17] I. Ilascu, "New Botnet Hides in Blockchain DNS Mist and Removes Cryptominer," Bleeping Computer - Web, 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-botnet-hides-in-blockchain-dns-mist-and-removes-cryptominer/. [Accessed: 14-Jan-2019].

[18] N. Johnson, "A developer's guide to ENS concepts – The Ethereum Name Service – Medium," Medium Blogpost Web, 2017. [Online]. Available: https://medium.com/the-ethereum-name-service/a-developers-guide-to-ens-concepts-7004eea8a073. [Accessed: 13-Jan-2019].

[19] M. Bazzell, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 5th ed. USA: CreateSpace Independent Publishing Platform, 2016.

[20] D. Murdoch, Blue Team Handbook: Incident Response Edition. 2014.

[21] "Personal data breaches," 2019.

[22] R. Jones and P. Collinson, "Identity theft warning after major data breach at Ticketmaster | Money | The Guardian," The Guardian (Online), 2018. [Online]. Available: https://www.theguardian.com/money/2018/jun/27/identity-theft-warning-after-major-data-breach-at-ticketmaster. [Accessed: 06-Jan-2019].

[23] D. P. Act, "ICO lo Guidance on data security breach management," pp. 1–8, 1998.

[24] The Crown, "PML v Person(s) Unknown [2018] EWHC 838 (QB) (17 April 2018)," 2018.

[25] N. Johnson, "ethereum/go-ethereum/name-registry - Gitter," Chatboard, 2019. [Online]. Available: https://gitter.im/ethereum/go-ethereum/name-registry. [Accessed: 15-Jan-2019].

[26] J. McDonald, "EthDNS: an Ethereum backend for the Domain Name System," Medium Blogpost Web, 2018. [Online]. Available: https://medium.com/@jgm.orinoco/ethdns-an-ethereum-backend-for-the-domain-name-system-d52dabd904b3. [Accessed: 13-Jan-2019].

[27] S. Dyson, W. J. Buchanan, and L. Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime," vol. 1, no. 2, pp. 1–6, 2018.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
SD has prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Photo by Atharva Tulsi on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(7)2019

A Blockchain Infrastructure for Transportation in Low Income Country Cities, and Beyond

Simon J Herko
TravelSpirit Foundation, UK
Correspondence: siho@travelspirit.io
Received: 26 August 2019 **Accepted:** 29 August 2019 **Published:** 5 September 2019

Abstract

For our cities of tomorrow, it is essential that transport is organised in an efficient, resilient and equitable way; enabling economic growth, social cohesion and minimising environmental impacts, including Climate Change. In cities across the world, new flexible, sharing economy services are blurring the lines between private and public transportation. However, these new transport modes are creating a "digital divide" and lack the integration and co-ordination between other services. This is needed to create seamless and sustainable travel options for people, including those belonging to vulnerable groups. This exploratory paper examines the potential for Blockchain to play a pivotal role in addressing increasing congestion and pollution in growing cities of developing countries. It draws on preliminary research into the role of Automatic Fare Collection systems and related mobility market dynamics and trends in the cities of Cape Town, South Africa and Dehli, India. By creating viable new digital infrastructure for Low Income Country Cities (LICCs), who have less incumbent legacy systems, there is potential to establish a decentralised blockchain network across these territories. There would also be scope for this network to be scaled further into wealthier countries, through a secondary wave of adoption by Mobility-as-a-Service (MaaS).

Keywords: *Blockchain, Distributed-hosting, Distributed-storage, Ethereum, Swarm, Forensics*

JEL Classifications: *A13, B41, C60, C71, D41, D43, D63, E24, E26, F02, F60, L14, L16, L17, L91, O18, O33*

1. The challenge of integrating mobility services

The proportion of the world's population living in urban areas will approach 66% by 2050[1], with much of this growth coming from Low Income Country Cities (LICCs).

However, transport in LICCs is fragmented, with no common standards for booking, payment and service delivery across different modes of transport, competing services or across regions. The majority of data is yet to be digitised and there are no mechanisms in place to support data-sharing of movements and assets. This leads to inefficient transport provision, impacting economic and social well-being and increasing congestion and pollution levels, including unsustainable carbon emissions that are accelerating Climate Change.

2. Developing the evidence base

We identified the high growth and congested cities of Cape Town, South Africa and Delhi, India, as suitable real-world case studies for examining the potential for blockchain to provide common infrastructure for LICCs.

Our research into the Cape Town and South African context was undertaken in collaboration with the Greater Tygerberg Partnership (GTP). The GTP is a not-for-profit entity funded by the City of Cape Town, under the Transport and Urban Development Authority. It serves as a facilitator to economic and social renewal and collaborative efforts between the private sector, civil society, academic institutions and government for the benefit of the Voortrekker Road Corridor (VRC). The VRC is an identified integration zone and inward investment opportunity area, comprising a population circa 350,000. It acts as the second largest economic hub and busiest transport hub in the Western Cape.

By researching the economic and social conditions in Cape Town and the wider South African region,

we have developed key insights into the challenge of bringing together transportation within and across LICCs.

In South Africa, the proportion of individuals benefiting from social grants rose from 12.7% in 2003 to 29.9% in 2016 [2]. The unemployment rate in South Africa is 26.7% [3]. Access to transport is a key enabler for accessing employment and education opportunities.

In the public and charitable sectors, transport funding subsidies are often applied to the infrastructure, not the user, creating a lack of transparency and often inefficient utilisation of scarce resources.

Although improving, a high proportion of the population (23%) are unbanked [4] and 63% are without access to smartphones [5]. Credit card penetration is at 17% and 65% of all transactions are made by cash. 54% of the population could be persuaded to switch from cash to digital wallets only if they provided a significant value-add over cash [6].

The following research insights are of particular relevance to the opportunity for a blockchain-based infrastructure intervention:

1. Competing transport businesses, including high levels of "informal" minibus taxi operations, make aggregation of services and data highly challenging and encourage disreputable operators. A commercially agnostic platform that is easy and compelling to adopt would therefore be highly desirable.
    i. In South Africa, the proportion of the population who use informal minibus taxis rose from 17.6% in 2003 to 22.4% in 2013. The proportion of mass-transit commutes that are carried by minibuses is 67.5% [7].
    ii. Customer dissatisfaction with minibuses is very high – 26.5%, compared to 3.9% for trains and 4.2% for buses.
2. In mass transit, the gap between fare revenues collected and passenger numbers serviced is too high, inhibiting further investments in infrastructure and a negative impact on the affordability of fares. Transit providers require higher surety of payment.
    i. Affordability of mass transit has an impact on poverty, inclusivity and the economy [8].
    ii. Cape Town buses have introduced a Smart Card and are enjoying growth [9].
    iii. Western Cape rail revenues are in decline due to unreliable services and poor funding [10].

For comparison with the South African research, we reviewed the transport landscape and relevant scientific papers for the National Capital Territory (NCT) of Delhi, India and its wider National Capital Region, including the significance of the Metro for rapid transit and active travel (i.e. non-motorised transport) for first and last mile access.

Despite rapid growth of the Metro network, the lack of integration of different modes has hastened the shift towards private automobiles, including two-wheelers and increasingly four-wheelers, for commuting and other short distance travel. Over the course of 2015-2016 alone, the number of private motor vehicles registered within the NCT of Dehli rose 10 percent, from 8.8 million to 9.7 million, and the trend is expected to continue without dramatic shifts in planning policy [11].

Price and first/last mile connectivity are the major influencing factors on choice of transport mode, demonstrated in shifts from Metro (faster with poorer last mile access, thus supplemented by auto hire) to bus (slower with better last mile access) amongst middle and lower income commuters following a Metro fare hike over the 2016-2017 fiscal year [12] [13].

The following insights should help inform the design and rollout of blockchain-based infrastructure for enhancing the ease of multi-modal trips, including the need to consider how funding for infrastructure to support active travel can be integrated into the conceptual framework:

1. Poor first and last mile connectivity of public transit, especially the Metro, is hampering the effectiveness of public transit at reducing congestion and enhancing mobility. Furthermore, transfers between metro and bus for first/last mile trip segments require separate fare payment methods, given the Metro fare payment card is not widely accepted by bus operators, despite pledges by operators to install card readers [14].
    i. Offering convenience expected of private motoring, especially door-to-door service, can help reverse the decline in modal share of public transit [15].
    ii. Physical facilities for active travel tend to be substandard or absent, leading to greater reliance on private cars, reduced street space for walkers and cyclists, and declining ridership of bus transit [16].
    iii. Funding for completion of discontinuous footpaths, regular maintenance, and prevention of encroachments are expected to boost the propensity of active travel [17].
2. Mobility providers including bus operators, ride-hailing and cycle-share platforms do not coordinate with each other, leaving

certain areas of the city grossly underserved relative to potential trip demand and, in the case of separate companies operating buses and metro trains, leading to lower than expected ridership on new metro lines. Local authorities are evidently aware of this shortcoming, as demonstrated by the launch of One Delhi mobile application for real time journey planning covering both bus and metro lines [18].

i. The benefits of a common mobility account have merited endorsement by the highest levels of the central government, including the Vice President in a call to combat vehicular pollution through improved ease of using public transport [19].

ii. There is a desire to address the lack of coordination by bringing ideally all mobility providers under a common organisational umbrella [20]. This desire, in practice may not be achievable, pointing towards a role of a blockchain infrastructure to support a multi-stakeholder eco-system with no centralised control.

iii. A study for a cycle sharing system that is ready for fares integration with other transport modes is ongoing in South Delhi [21].

3. Our working hypotheses on a viable blockchain

Our research is motivated by a hypothesis that, less hampered by legacy infrastructure and with strong economic drivers for innovation, LICCs can leapfrog high income countries on Intelligent Transport Systems (ITS) [22]. This would imply:

1. LICCs do not have to depend upon large programme budgets (which aside from the expense can be often open to corruption) and enter complex procurements to drive forward and realise technology-driven benefits.
2. There are ways for emerging economies to innovate faster than developed markets and play the role of pilot/pioneers in blockchain.

More specifically, there is an opportunity for a common blockchain network infrastructure, for transport booking, payments and subsidies, that, starting with Low Income Country Cities (LICCs), would enable all cities to enjoy the benefits of an integrated transport system that is interoperable across competing services and inter-regional borders.

As highlighted in our South African evidence base (while applicable across much of the African, Indian, Asian and South American continents) the informal minibus taxi sector is a complex environment, while a key ingredient to the transport mix of many LICCs. It is ripe for change, especially with regards to new payment models and methods to optimise and integrate systems.

Following an examination of the current Intelligent Transport Systems (ITS) landscape in LICCs, we identified the most compelling blockchain use-case to be for Automatic Fare Collection (AFC). A common global and universal "open-loop" infrastructure, enabled by blockchain, would replace the need for bespoke and centralised back-office systems for each city, and provide a common payment system for the informal minibus taxi sector.

Both the European Bank for Reconstruction and Development (EBRD) and World Bank have identified the key barriers to adoption of "open-loop" account-based systems outside the largest and most affluent of world cities, such as Washington D.C. Boston, London, Amsterdam, Vienna, Singapore, Hong Kong and Seoul [23] [24]. They are the cost, time and effort required to obtain the necessary banking security permissions and the complexities of public sector led procurement and implementation, which can take up to 5 years to complete.

Advanced contactless card systems in London, Hong Kong and Singapore are made possible by an effective monopoly over transport provision and a well-funded co-ordinating body (e.g. TfL's operational budget is over £6 billion per annum). They generally do not extend to new collective transport innovations such as car clubs, ride-hailing and bike-sharing; especially if operated privately. In this respect, they are less helpful operating models to replicate in emerging market economies, with their higher levels of market fragmentation, and where informal private minibus services often dominate mass transit.

Research undertaken for the World Economic Forum [25] articulates the case for improved integration and interoperability in city transportation and its potential for positive impact on global prosperity, equality and the environment. Their hypothesis is that a centralised global platform is required, risking, in our view, bringing transport under the control of a small set of data monopolies.

Our working hypothesis is that a permission-based blockchain solution could provide users equitable and open market access to transport services, with cashless, subscription-based and/or subsidised payment mechanisms. The solution would supersede "closed-loop" AFC technology (e.g. smartcards) on buses and trains and provide viable infrastructure to the informal minibus taxi market, which represents circa 70% of all mass transit trips in LICCs.

The rationale for adoption could be as follows, in terms of benefits for different stakeholders.

Benefits to End Users:

1. Cashless and trusted solution, improving safety & security.
2. Access to user-based subsidies and micro-credit worthiness.
3. Access without smartphone or contactless banking.
4. Develop personal identity and data profile.
5. Roaming capability.

Benefits to Transport Providers:

1. Surety of payment and uplift in fare revenues collected.
2. Access to customer data and new markets.
3. Fair and trustworthy subsidy compensation mechanisms.

Benefits to Cities:

1. Shift to mass-transit and reduced congestion/ pollution.
2. Platform for inward investment into public transport infrastructure.
3. Easier to allocate subsidies in line with policy objectives (e.g. active travel).
4. Affordable, easy to adopt AFC solution.

These benefits would be delivered through decentralised, self-sovereign and interoperable "mobility accounts", hosted on a permission-based blockchain [26]. This includes smart contracts to execute commercial agreements, a shared set of business rules for innovation in fares policy and blended financial subsidies, including user-based subsidy.

The primary goal of the blockchain would be to provide all LICCs with a common global ITS (Intelligent Transport Systems) infrastructure, whose adoption could be achieved organically, rather than procured. We anticipate an open, transparent and crowd-based governance structure and token economy that will ensure transaction costs remain affordable.

4. Technical characteristics of a suitable blockchain

In researching the feasibility of a blockchain solution in the South African context, we identified the following initial functional requirements to establish a viable blockchain solution and adopted network:

1. Users (including the unbanked) to access multiple transport services through a global mobility account.
2. Account system interoperability and roaming capability between transport operators, modes and across regional borders.
3. Manage rights and responsibilities of portable personal data.
4. Support trusted multi-lateral commercial arrangements between transport providers.
5. Provide low network latency, fast verification and compatibility with low power devices.
6. Resilience to fraud and denial-of-service attacks.
7. Commercially agnostic solution that can be easily adopted by competing transport providers and multiple regions and cities.
8. Close integration with existing infrastructure, and a distributed share of transaction revenues.

The decentralised delivery model of an open-source and permission-based blockchain network would also seek to address the high expense and long duration of ITS procurements for AFC implementation.

Through dialogue with Hyperledger Working Requirements Group, we have identified the Hyperledger Indy and Hyperledger Sawtooth development frameworks and modular open-source codebase as the starting point [27] [28] [29]. To meet the above functional requirements, we anticipate the following future research and development actions:

4.1. Proof of Location within the Trusted Execution Environment (TEE)

Existing Sawtooth framework accesses an efficient Proof of Elapsed Time lottery algorithm for network consensus, via a TEE developed by Intel. There is opportunity to explore a new TEE that is optimised for deployment in low power devices, including a Proof of Location to improve network security and mobility account operation.

4.2. Sharding / partitioning of the global state

Existing Sawtooth framework requires consensus of the entire global state of transactions, with a total ordering of every transaction. There is an opportunity for our blockchain network to be partitioned or 'sharded' by location, to improve scalability and reduce storage requirements. A new framework could be developed to spawn multiple permissioned overlays of Sawtooth, enabling a segmented-state management protocol.

4.3. On-Chain Smart Contracts with "Seth"

There is scope to research into the capabilities of the new Seth transaction family [30] as a means for deploying Turing complete programs for compensation, arbitration and concessionary re-imbursement processes.

4.4. Linking via "Seth", to a token-based economic model

Hyperledger frameworks are optimised for the application of permissioned blockchains within business enterprise solutions using a centralised platform business model. A design goal of commercially agnostic, distributed revenues requires a higher level of decentralisation.

There is scope for using Seth to bridge between the Sawtooth permissioned framework and Ethereum-based tokens, to enable each city and transport provider to operate their own node and gain a share in the transaction revenues.

5. Beyond LICCs: global Mobility as a Service (MaaS)

Mobility as a Service (MaaS) is a new disruptive business model paradigm [31]. With an expected market size of $1 trillion by 2030, it will empower users with hassle-free payment options and an integrated approach to accessing public transport, flights, ferries and shared economy services.

To scale globally, MaaS requires commercial collaboration between a diverse and large transport ecosystem [32], and affordable solutions for Low Income Countries. Latest public policy and industry thinking would suggest a growing consensus that such collaboration would require a greater level of "openness", both culturally and technically, within the city transport sector, than currently exists in most city states [33].

Furthermore, to satisfy the demands of inter-regional and international travel, supporting MaaS platforms need cross-border functionality, facilitating "roaming" across cities and countries. They must also integrate various public, charitable, private and consumer funding sources to enable effective investment in mass transit and active travel infrastructure.

In a small collection of cities within wealthier countries, that also enjoy advanced Open Data programmes (e.g. Finland, Germany and the Netherlands), some MaaS apps are already covering a full spectrum of collective transport services. They have, in our view, limited scope for widespread adoption due to the centralised platform approach - i.e. the "unwanted third-party aggregator". This is a problem blockchain could solve by enabling personalised aggregation to take place direct to consumer, via a trusted, commercially agnostic and decentralised infrastructure.

While there are many new blockchain solutions appearing for shipping and logistics, the application of blockchain for MaaS is in its infancy. We have identified just over half a dozen published research papers on blockchain for MaaS, from Germany, Sweden, UK (by the Transport Systems Catapult and TravelSpirit Foundation), Finland and the Netherlands [26][34][35][36][37][38][39]. This growing evidence base corroborates with our thesis that the scope of MaaS to scale effectively, even within the European market, where public policy and industry interest is the greatest, is limited without the support of a common blockchain infrastructure.

With a focus on wealthier markets, the papers we have reviewed on the application of blockchain for MaaS do not make direct references to LICC contexts. We therefore believe we have developed a novel concept for how to scale a blockchain network for ultimate adoption as a MaaS solution in wealthier countries.

6. Conclusion

The potential global impact of a blockchain-based network infrastructure on the city transportation sector is substantial. With blockchain, we can ensure a healthier democratisation of the transport economy, that, based upon liberal philosophies, will provide autonomy to local and regional economies, strengthening global collaboration and regional governance.

A case has been made for a global and universal blockchain infrastructure, for the sharing of data on movement and assets, designed with low income economies and vulnerable groups in mind. It would enable:

1. Users' access to different modes of transport in an equitable and hassle-free way.
2. Assurance to transport operators on surety of payment.
3. Cities with integrated solutions for tackling congestion and targeting subsidies.

Through the work of both the European Bank for Reconstruction & Development and the World Bank, the economic and social case for delivering Automated Fare Collection (AFC) technology in transportation systems in emerging markets is already supported by a comprehensive evidence base. Existing research on AFC solutions consistently focuses on centralised platforms and bespoke back-office infrastructure for each city. It means the opportunity for a global infrastructure, delivered through a decentralised and networked route to market, has not been researched and advocated to the same extent.

In wealthier countries Mobility-as-a-Service (MaaS) is a new business model that integrates public and private services together. Its level of adoption could be limited without a supporting blockchain infrastructure. By creating viable new digital infrastructure for

Low Income Country Cities (LICCs), who have less incumbent legacy systems, there is potential to establish a decentralised blockchain network across these territories. There would also be scope for this network to be scaled further into wealthier countries, through a secondary wave of adoption by Mobility-as-a-Service (MaaS).

To advance our understanding of this alternative vision for global AFC infrastructure (i.e. technology that is universal and enables a decentralised approach to the management and orchestration of transport) we'd recommend there to be:

1. Technology-based research and development on the Hyperledger Project open-source codebases.
2. Interventional pilots in Low Income Country Cities, and research into the institutional, commercial and funding mechanisms that would be required to establish and scale this kind of universal blockchain infrastructure.

References:

[1] "World Urbanization Prospects - Population Division," United Nations. [Online]. Available: https://population.un.org/wup/. [Accessed: 16-Aug-2018].

[2] "General Household Survey, 2016," Department Statistics South Africa. [Online]. Available: http://www.statssa.gov.za/?p=9922.

[3] "Quarterly Labour Force Survey – QLFS Q4:2017" Department Statistics South Africa. [Online]. Available: http://www.statssa.gov.za/?p=10884

[4] "Credit Card vs Cash in Africa – on the verge of convergence" Cape Business News (2019). [Online] Available: https://www.cbn.co.za/opinion/credit-card-vs-cash-in-africa-on-the-verge-of-convergence/

[5] "In South Africa, Cash Is Still Right On The Money" PYMNTS.com (2019). [Online] Available: https://www.pymnts.com/cash/2017/south-africa-cash-usage/

[6] "Mobile wallets 'key' to SA e-commerce," Fin24tech, 30-Mar-2016. [Online]. Available: https://www.fin24.com/Tech/Mobile/mobile-wallets-key-to-sa-e-commerce-20160330

[7] P. Lehohla, "Transport Series Volume I: Profile of non-motorised transport users: In-depth analysis of the National Household Travel Survey 2013 data," Department Statistics South Africa, rep. Available: http://www.statssa.gov.za/publications/Report-71-03-01/Report-71-03-012013.pdf

[8] R. Carruthers, M. Dick, and A. Saurkar, "Affordability of Public Transport in Developing Countries," The World Bank Group, rep., Jan. 2005. Available: http://siteresources.worldbank.org/INTTRANSPORT/214578-1099319223335/20460038/TP-3_affordability_final.pdf

[9] "Golden Arrow hits profit targets." Cape Business News. (2019). [Online] Available: https://www.cbn.co.za/news/golden-arrow-hits-profit-targets/

[10] C. Presence, "Metrorail losing paying customers by the millions, MPs told," IOL News, 17-Apr-2018. [Online]. Available: https://www.iol.co.za/news/south-africa/western-cape/metrorail-losing-paying-customers-by-the-millions-mps-told-14494831

[11] S. Pillai, "Poor public transport behind Delhi vehicle boom, say experts," Hindustan Times, 20 Dec. 2016. Available: https://www.hindustantimes.com/delhi/poor-public-transport-behind-delhi-vehicle-boom-say-experts/story-4lbiZTogbYPofE2A57zcCJ.html

[12] A. Roychowdhury, "Towards Clean and Low Carbon Mobility: Addressing Affordability and Scaling up of Sustainable Transport," Centre for Science and Environment, rep., Sep. 2018. Available: http://cdn.cseindia.org/attachments/0.21487000_1536054529_Anumita-Clean-low-carbon-mobility-strategy-Sept.pdf

[13] C. Kumar and A. Ganguly, "Travelling Together but Differently: Comparing Variations in Public Transit User Mode Choice Attributes Across New Delhi and New York," Theoretical and Empirical Researches in Urban Management, vol. 13, no. 3, pp. 54-73, Aug. 2018. Available: https://www.jstor.org/stable/pdf/26472536.pdf?refreqid=excelsior%3Aba21b9e6215c4ee0989116576282054a

[14] "Use metro cards on buses for discount," The Hindu, 20 Oct. 2018. Available: https://www.thehindu.com/news/cities/Delhi/use-metro-card-on-buses-for-discount/article25266914.ece

[15] O. P. Agarwal, "Compulsion to Choice: How Can Public Transport in India Be Transformed," Economic and Political Weekly, vol. 54, no. 4, 26 Jan. 2019. Available: https://www.epw.in/node/153650/pdf.

[16] "U. Nasim and V. Chattopadhyay, "Indian roads belong to motorised vehicles, not cyclists or pedestrians," Down to Earch, 6 Nov. 2018. Available: https://www.downtoearth.org.in/news/air/indian-roads-belong-to-motorised-vehicles-not-cyclists-or-pedestrians-62049

[17] M. A. Alam, "Sustainable and Equitable Transport System in Delhi: Issues and Policy Direction," Asian Institute of Transport Development, rep., 2015, Available: https://www.unescap.org/sites/default/files/Article%202_Sustainable%20and%20equitable%20transport%20system%20in%20Delhi.pdf

[18] "Delhi commuters can now locate public transport better with 'One Delhi' app," Press Trust of India, First Post, 6 Mar. 2019. Available: https://www.firstpost.com/tech/news-analysis/delhi-commuters-can-now-locate-public-transport-better-with-one-delhi-app-6205941.html

[19] "VP calls for a public transport-centric approach to combat growing vehicular pollution," Government of India Press Information Bureau, 3 May 2019. Available: https://pib.gov.in/newsite/PrintRelease.aspx?relid=189925

[20] "Reimagining public transport in India," KPMG, rep., Oct. 2017. Available: https://assets.kpmg/content/dam/kpmg/in/pdf/2017/10/Reimagining-public-transport.pdf

[21] "Draft Detail Project Report on Public Bicycle Sharing System for SDMC (South Delhi Municipal Corporation)," Centre for Green Mobility, rep., Sep. 2015. Available: https://shaktifoundation.in/wp-content/uploads/2017/06/Public-Bicycle-Sharing-DPR-South-Delhi.pdf

[22] T. Yokota, "TTS Technical Note for Developing Countries,"

World Bank Group, rep., Jul. 2004. Available: http://siteresources.worldbank.org/EXTROADSHIGHWAYS/Resources/ITSNote1.pdf

[23] "On the move: delivering automated fare collection," European Bank for Reconstruction and Development, rep., Jul. 2017. Available: https://www.ebrd.com/documents/admin/on-the-move-delivering-automated-fare-collection.pdf

[24] C. Monsalve et al, "Public Transport Automatic Fare Collection Interoperability: Assessing Options for Poland" World Bank Group and Korea Green Growth Partnership, rep., Jun. 2016. Available: http://documents.worldbank.org/curated/en/564001469009916441/pdf/107014-WP-P148489-PUBLIC-Phase-2-Public-Transport-AFC-Interoperability-Final-Report-June-10-2016.pdf

[25] J. Moavenzadeh and V. Padilla-Taylor, "Designing a Seamless Integrated Mobility System (SIMSystem)," World Economic Forum, rep., Jan. 2018. Available: http://www3.weforum.org/docs/Designing_SIMSystem_Manifesto_Transforming_Passenger_Goods_Mobility.pdf

[26] S. Ho et al, "TSio Protocol: The Internet of Mobility," Whitepaper, TravelSpirit Foundation, UK, rep., Dec. 2017. Available: https://travelspirit.foundation/wp-content/uploads/2017/12/TravelSpirit-WhitePaper-TSio-Protocol-v-6-1.pdf

[27] "Hyperledger Architecture Volume 1, Design Philosophy and Consensus" Linux Foundation, rep., Aug. 2017. Available: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[28] "Hyperledger Architecture Volume II, Smart Contracts" Linux Foundation, rep., Apr. 2018. Available: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

[29] K. Olson, M. Bowman, J. Mitchell, S. Amundson, D. Middleton, and C. Montgomery, "Hyperledger Sawtooth: An Introduction," Linux Foundation, rep., Jan. 2018. Available: https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf

[30] "Seth Transaction Family Specification" Hyperledger Project [Online, accessed Jun. 2019]. Available: https://sawtooth.hyperledger.org/docs/core/releases/0.8/transaction_family_specifications/sawtooth_burrow_evm_family.html

[31] M. Kamargianni and M. Matyas, "A Holistic Overview of the Mobility-as-a-Service Ecosystem" University College London, rep. Mar. 2017, Available: https://docs.wixstatic.com/ugd/a2135d_8ec5294674a44129b04bcc99a324d1c5.pdf

[32] P. Karjalainen, "Guidelines & Recommendations to create the foundations for a thriving MaaS EcoSystem", MaaS Alliance, rep. Sep. 2017, Available: https://maas-alliance.eu/wp-content/uploads/sites/7/2017/09/MaaS-WhitePaper_final_040917-2.pdf

[33] S. Herko, S. Witzel, P. Karjalainen et al, "An Open Future for Cities: Preparing cities for the necessary transformation and organisational changes needed for an open future." Whitepaper, TravelSpirit Foundation, UK, rep., Dec. 2017. Available: https://www.researchgate.net/publication/334524614_An_Open_Future_for_Cities_Preparing_cities_for_the_necessary_transformation_and_organisational_changes_needed_for_an_open_future

[34] D. Sümmermann, C. D. Öge, M. Smolenski, G. Fridgen, and A. Rieger, "Open Mobility System", Concept Paper, MotionWerk GmbH, Fraunhofer FIT, TÜV Rheinland, Germany, rep., Sep. 2017 Available: https://www.omos.io/wp-content/uploads/whitepaper/OMOS_concept_paper.pdf

[35] P. Andersson and J. Torstensson, "Exploring the role of blockchain technology in Mobility as a Service,", Master's Thesis, Chalmers University of Technology, Gothenberg, Sweden, rep., Nov. 2017. http://publications.lib.chalmers.se/records/fulltext/252507/252507.pdf

[36] "Blockchain Disruption in Transport: Are You Decentralised Yet?" Transport Systems Catapult, UK, rep., Jun. 2018. Avaliable: https://s3-eu-west-1.amazonaws.com/media.ts.catapult/wp-content/uploads/2018/06/06105742/Blockchain-Disruption-in-Transport-Concept-Paper.pdf

[37] A. Karinsalo and K. Halunen, "Smart Contracts for a Mobility-as-a-Service Ecosystem,", Conference Paper, VTT Technical Research Centre of Finland, rep. Jul. 2018. Available: https://ieeexplore.ieee.org/abstract/document/8431964

[38] J. Verheul, M. Mijnheer, and J. Ferwerda, "A new Blockchain Platform Designed for the Future of Human Mobility,", Whitepaper, VMC, The Netherlands, rep., Jan. 2019. Available: https://vmc.ai/wp-content/uploads/2019/01/whitepaper.pdf

[39] T. Nguyen, J. Partula, S. Pirttikangas, "Blockchain-based Mobility-as-a-Service,", University of Oulu, Finland, Conference Paper, rep., May 2019. Available: https://www.researchgate.net/profile/Tri_Nguyen43/publication/333343145_Blockchain-based_Mobility-as-a-Service/links/5ce7e298a6fdccc9ddcabb45/Blockchain-based-Mobility-as-a-Service.pdf

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
SJH would like to thank his colleagues at the TravelSpirit Foundation and Iconic Blockchain for their support and encouragement over the past 2 years, in particular to David Alexander, Giles K Bailey, Justin Coetzee, Mike Fitzgerald, Dr Pieter J Fourie, Bren Hutchinson, Dr Maria Kamargianni, Nathan King, Rob Mann, Gary Parkinson and Yangbo Du. Also, special thanks to Johan Muller and Warren Hewitt at the Greater Tygerberg Partnership and Mark Rathbone at Brabners LLP.

Photo by Hanny Naibaho on Unsplash

THE JBBA

ANALYTICAL ESSAY

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(5)2019

A Review of fast-growing Blockchain Hubs in Asia

Yu Wang, Jing Ren, Caroline Lim, Swee-Won Lo
School of Business, Singapore University of Social Sciences, Singapore
Correspondence: carolinelimsl@suss.edu.sg
Received: 28 June 2019 **Accepted:** 26 July 2019 **Published:** 9 August 2019

Abstract
The unique combination of social and economic factors has brought about a dynamic and rapidly-evolving blockchain ecosystem in Asia. This paper systematically reviewed the development of four fast-growing blockchain hubs in Asia, namely China, Japan, Singapore and South Korea using secondary data sources. These countries are fast-growing based on the development of its digital, technological and regulatory infrastructure, patent applications, cryptocurrency trading volume and Initial Crypto-token Offerings (ICOs) activities. The review included insights into the different regulatory approaches, the blockchain startup scenes, selected enterprise or government-backed projects, as well as the research and educational landscape. Our findings suggested that the regulators, industry players, and academic institutions were purposeful and deliberate in nurturing blockchain technology innovation. Future development would be dependent on the regulatory, technological, as well as talent capability support unique to each blockchain hub.
Keywords: *: blockchain, cryptocurrency, regulation, fintech, ICO*
JEL Classifications: *D02, G18, H11, O20, O32, O50*

1. Introduction

The blockchain technology, with its properties that distributes, disintermediates and decentralises, enables value to be unlocked for peer-to-peer exchange. This distributed ledger technology (DLT) can enforce "trust" such that a mutually distrusting community can collaborate and consent to a single version of the truth, which implies trade and exchange can occur between parties not known to each other.

These features of blockchain have enabled applications across different industries. Besides applications in trade, stocks and securities exchange, banking and finance, insurance, telecommunications, voting, health care, government administration, social networking and more, the blockchain technology holds promise to financial integration and inclusion [1]. The potential of blockchain is immense.

This paper is a systematic review of the development and application of blockchain in four Asian countries - China, Japan, Singapore and South Korea. These four countries have leveraged the entrepreneurial fervour and intensity of activities to shape themselves into blockchain hubs, evidenced by our analysis of their respective technological infrastructure, regulatory support, funding, and investment capital.

Literature in the inter-organisational relationship, including innovation and knowledge hubs, can be parsimoniously organised into two paradigms – network versus dyadic. Organisations in a network paradigm developed long-term and trusting relationships that were mutually reinforcing, and behaviours followed socially accepted norms. Organisations in a dyadic paradigm were opportunistic and sought to "maximise cooperation and minimise conflicts" [2].

As technology hubs serve the community in addition to organisational interests, we adopt the network paradigm in our definition of a hub. We define a hub as a locus of innovation and entrepreneurial activities that fuels the local economy as coordinating firms collaborate & develop capabilities supported by different enablers. The literature described a financial technology ("FinTech" in short) hub to be characterised by sufficiently mature and developed technology infrastructure, availability of talented and receptive workforce (including investors, technologists, financiers), established regulatory support (e.g., favourable tax rates), involvement of the academia, government and enterprises in applied research and investment (e.g., accelerators, incubators, mentorship

and seed funding), and a demand for FinTech (e.g., large volume of daily financial transactions, the need to enhance consumer experience and improve business efficiency, and the need for financial inclusion)[3].

A critical difference between FinTech and blockchain is that the latter can be applied beyond the financial industry. Blockchain allows parties with natural mistrust to collaborate and consent to a single version of the truth, thereby boosting business efficiency where cross-company and cross-industry collaborations are needed; it also holds promise to financial and social inclusion [1]. With these in mind, we propose the enablers of a blockchain hub to include the innovator group, infrastructure readiness and programme, availability of funding and capital, and the existence of demand for blockchain applications.

As one of the emerging new technology, blockchain drew investments in research and development of large technology firms and technology startups. We termed these technological firms and technology startups as innovator group. The innovator group represented technical capabilities to advance the development and application of blockchain. Funding and capital reflected the willingness and capabilities of individual and institutional investors to support technological development, especially for a relatively new and less-understood technology like blockchain. Infrastructure readiness and programme would facilitate the development of new and innovative technology. Apart from network and technology readiness, a friendly regulatory environment and availability of skilled talent pool would encourage and facilitate technological innovations. The economic and socio-ecological contexts could generate demand for blockchain applications; a politically stable economic environment could serve as a landing for blockchain projects addressing trust issues between and across partners. Similarly, the socio-ecological contexts could provide the impetus for financial and social inclusion.

This review intends to improve the understanding of blockchain development in different jurisdictions and contribute to current literature about blockchain in the Asia region. In the subsequent section, we explained the rationale of selecting the Asian countries, namely China, Japan, Singapore, and South Korea. In the third section, we analysed and compared the status of blockchain development in each country and inter-country. We concluded this paper with a discussion on the implications for future research and practice.

2. Scope of Review

In this section, we explained the selection criteria of the four countries in Asia, beginning with a description and analysis of four key enablers of a blockchain hub namely innovator group, infrastructure and programme, funding and capital, and demand.

2.1. Innovator Group

The actors in a network were central to the activities of a blockchain hub. These actors included large technology firms, blockchain startups and related technology unicorns who drew venture capital and drove spending in research and development (R&D).

As of July 2018, China, Japan and South Korea were three Asian countries with the most number of Global 500 companies in the top ten of Fortune 500. Companies in Global 500 included large technology firms with research and investments in blockchain projects. In China, 46 of the 120 companies were involved in blockchain development representing sectors like banking, energy, IT, and motor. Japan's Sony and Fujitsu were also actively involved in blockchain projects. Almost all of the South Korea IT and motor companies in the Fortune 500, like Samsung, LG, and Hyundai, were exploring their own blockchain platforms.

Following the statistics of total blockchain-related patents filed globally by IPR Daily and Cintelliq, China filed the highest number of blockchain patents (41%), followed by the United States (32%)[i]. As of August 2018, Chinese companies occupied more than half of the top 100 companies globally for patents application on the blockchain (57 out of 100). Technology firms among them included Alibaba of China, Sony and Fujitsu of Japan and Coinplug of South Korea. The European Patent Office (EPO) showed a steady increase in patents granted normalised by population between 2009 to 2018 from countries like China, Japan, and South Korea. The year-on-year change of these three Asian countries over the period exceeded the figures reported for thirty-eight member states of EPO (including 28 states of the European Union).

Investment in blockchain startups represented the market expectation for blockchain development in the long-term. As of 31 March 2019, there were 333 technology unicorns worldwide between 2010 to 2019[ii]. Among them, more than one third (124) originated from Asia, of which China accounted for 89 unicorns. Another 15 unicorns originated from India, eight from South Korea, five from Indonesia, two from China SAR[iii] Hong Kong, one each in Japan and Singapore. Nine unicorns among them were blockchain-based in the areas of FinTech and cryptocurrency. These nine unicorns included six from China (e.g., Bitmain, Tiger Brokers), two from India (One97 Communications, PolicyBazaar), one from South Korea (Viva Republica). In China, where the regulation prohibited fund-raising through initial crypto-token offering (ICO), technology firms would become one of the main funding sources for blockchain startups.

National spending on research and development (R&D) fueled the growth of the innovator group. According to data from the UNESCO Institute of Statistics published by the World Bank, high-income countries spent on average 2.36 per cent of GDP on R&D for science and technology between 2000 to 2016[iv]. Across countries in Asia, Japan's R&D spending had consistently exceeded the average figure of high-income countries. The same index in South Korea rose steadily since 2000 to more than double that of high-income countries from 2012 onwards. Singapore's R&D spending as per cent of GDP approximated close to high-income economies. China, on the other hand, did not perform close to other high-income countries on this index, but its R&D spending rose significantly from 0.89 per cent in 2000 to 2.11 in 2016. Other Asian countries performed below average relative to the rest of the world or when compared against high-income economies.

2.2. Infrastructure and Programme

The critical determinants of a blockchain hub included both digital and regulatory infrastructure of a country. We reviewed the digital infrastructure in two aspects, namely the network readiness and technology readiness. The World Economic Forum published the Global Information Technology Report[v] to assess the state of network readiness of 139 economies from the annual executive opinion survey. The index evaluated the quality of regulatory and business environment, information and communications technology (ICT) readiness in terms of affordability, skills and infrastructure, the role of the government, business sector and population as well as the environment, readiness and usage. Countries in Asia, including China, Malaysia, Mongolia, Sri Lanka, and Thailand, demonstrated steady improvements from 2012 to 2016. Across the drivers of network readiness in 2016, Singapore performed better than other advanced economies in business and innovation environment, skills, government usage, and social impacts. Taiwan performed the best in mobile network coverage and internet bandwidth infrastructure. Singapore was ranked first in 2015 and 2016; Japan was the other Asian country ranked in the top 10 of network readiness; the others in top 10 were made up mostly of European countries. Meanwhile, South Korea hovered around 10th to 13th position between 2013 to 2016 and was ranked 13th in the most recent published ranking.

We further referenced the technological readiness ranking of eighty-two countries published by The Economist Intelligence Unit (EIU) as part of their medium- and long-term forecasts of the world's largest economies. The EIU assessed performance across three categories[vi]: access to the internet, digital economy infrastructure and openness to innovation. The index ranked each country for the historical period from 2013 to 2017 and forecasted change in performance for the period 2018 to 2022. Countries in Asia ranked in the top 10 included Singapore, Japan, South Korea, and Taiwan. Meanwhile, EIU forecasted improvements in technological readiness for these four countries/region and Hong Kong. In particular, the forecast projected Singapore to be ranked similarly to Australia and Sweden in technological readiness by the period 2018-2022.

Besides technological readiness, a workforce that was ICT-enabled, trained and skilled in blockchain development would more effectively contribute to the completion of innovative blockchain projects. According to the Global Startup Ecosystem Report [12], cities such as Beijing, Shanghai, Singapore, Bangalore, and Hong Kong possessed high-quality technology talents (such as top developers on GitHub and software engineers) that were relatively inexpensive compared to the US and European countries.

Workforce policies that encouraged science, technology, engineering and mathematics (STEM) training as well as lifelong learning in related skills and knowledge enhanced the adoption and development of blockchain technology. Preliminary results by the OECD reported that workforce capabilities and training received were associated with higher digital adoption, such as in cloud computing technology [4].

According to another OECD survey of adults aged between 16 and 65 in 35 economies in 2012 and 2015 Singapore (62%) and South Korea (60%) performed above the OECD average (55%) for adult participation rates in structured training. In the same survey, Japan performed below the OECD average.

Apart from workforce policies, lower regulatory costs and simplified compliance procedures would expedite the process of starting a business, and these would be attractive factors for blockchain startups. As of 2018, the shortest time needed to start a business was in Hong Kong (1.5 days), Singapore (2.5 days), South Korea (4 days), Thailand (4.5 days), and Sri Lanka (9 days). In contrast, Cambodia took the longest time (99 days), followed by Laos (67 days), India (29.8 days), Philippines (28 days), China (22.9 days), and Vietnam (22 days).

On the other hand, the cost of business startup procedure (in per cent of gross national income per capita) including all official fees and legal costs was the lowest in Singapore (0.5%), followed by China (0.6%), Brunei, Hong Kong (1.1%), and Mongolia (1.4%) [5].

2.3. Funding and Capital

Funding and capital played an essential role in fueling the growth of blockchain startups and thus, the

development of blockchain technology. Blockchain startups commonly raised funds through loans, donations, traditional venture capital, and ICOs [6].

Among them, ICO represented a unique fundraising method as it allowed blockchain startups to raise funds from the community at a relatively early stage. The value of ICO reflected the financial support that blockchain startups might receive and the size of the blockchain community within a region. In Asia, Hong Kong and Singapore were popular destinations for many blockchain entrepreneurs considering ICOs, after the prohibition of ICOs in mainland China and South Korea. As of October 2018, 8.14 per cent of ICOs globally occurred in Singapore and 2.81 per cent in Hong Kong[vii]. Vietnam and Japan led in the traffic to ICO listing websites globally, followed by the US and the United Kingdom. Other countries among the top 10 were China and South Korea [7]. Search volume from Google Trends suggested Asian countries and regions like China, South Korea, Singapore, and Hong Kong, to be among the top 10 worldwide for 'ICO' [viii].

By the volume of venture capital and private equity activities, Hong Kong, Japan, and Singapore were among the most attractive countries/regions for venture capital and private equity globally. They were ranked 4th, 5th and 6th respectively, after the US, UK and Canada[ix]. Other Asian countries in the top 30 list included Malaysia, China, South Korea, Thailand, and India.

The trading volume of Bitcoin served as another indicator for the scale of capital in the country; an indicator of the cryptocurrency market that drew investors' attention. Asia accounted for almost a third of cryptocurrency transactions globally. According to LocalBitcoins.com, a decentralised bitcoin exchange website, the trading volume was US$6.3 billion in July 2018, of which Asia contributed 32.8 per cent of the global volume of bitcoin traded [8]. Furthermore, statistics of the most-traded national currencies for bitcoin showed a consistent trend - Japanese Yen accounted for around 40 per cent of the global total bitcoin[x] volume, second to only US Dollar, with national currencies of other Asian countries such as South Korea, Indonesia, Thailand, Singapore, and Vietnam also among the top 20.

2.4. Demand

We proposed the demand for DLT as another enabler of a blockchain hub. Demand could stem from an economic infrastructure where multinational organisations converge as well as the socio-ecological landscape. DLT solved trust in digital asset transactions between businesses or between businesses and consumers without a central administrator [9].

The economic infrastructure of a country that would stimulate demand for blockchain applications included countries with active participation in the global production networks. We considered the global value chain participation since that reflected the relative positions of different economies in the global production networks. Forward or backward participation ratios measured each country's participation in the global value chain. Forward participation ratio measured participation through the supply side, i.e., the extent that "an economy's (or economic sector's) locally generated value-added was embedded in the production of other economies" [5]. Backward participation ratio measured participation through the demand side and "denotes the foreign value-added contribution to an economy's (or economy-sector's) exports" [5].

In Asia, Singapore led in the use of foreign inputs in the production of its exports, with a backward participation ratio of close of 60 per cent, followed by Vietnam, Taiwan (China), South Korea, and Malaysia. Brunei took the pole position in forward participation ratio at slightly more than 80 per cent, followed by Laos, Indonesia, Philippines, and Malaysia [5].

The need to resolve trust issues to boost efficiency and save cost through dis-intermediation using blockchain applications would emerge from countries with foreign direct investments (FDI). In 2017, the top three recipients of FDI in Asia was China, Hong Kong, and Singapore, followed by India, Indonesia, Japan, South Korea, Vietnam, and the Philippines [5].

A significant population of the working class in Asia earned their living outside of their home countries and remitted their earnings back to their home countries[xi]. In 2017, countries in the Asia Pacific region received US$266 billion in remittances [5]. Globally the top three remittance recipient economies were in Asia, namely India, China, and the Philippines. There were two pain points to be addressed – trusted peer-to-peer funds transfer and remittance fees. Firstly, a large population in Asia were unbanked, although a majority of them owned mobile phones connected to a 3G or 4G network [10]. Secondly, the average cost of cross-border remittance fees for sending US$200 remained high at seven per cent [11].

The socio-ecological context supported by a favourable regulatory environment and well-developed technological infrastructure laid the foundation for blockchain projects that would boost production efficiency or solve financial inclusion within the economy as well as the neighbouring region.

2.5. Rationale

Using national spending and patents filed as measures

for the impact of the innovator group, countries like China, Japan, Singapore, and South Korea, performed better than other Asian countries. Moreover, China had the highest number of technology firms and technology unicorns. Technology firms provided alternative funding sources for blockchain startups.

While China's regulation prohibited cryptocurrency trading and ICOs, trading volume in bitcoin and other cryptocurrencies were high in Asian countries or regions like Hong Kong, Indonesia, Japan, Singapore, South Korea, Thailand, and Vietnam. Activities and interest in ICOs were also high. Drawing parallel from investment trends reported in Europe, investors would likely invest more in ICOs in investment destinations that appealed to VC and PE funds; destinations included China, India, Japan, Malaysia, Singapore, South Korea, and Thailand [12].

The readiness of technological infrastructure and programmes were critical to support innovation in blockchain technology. Singapore, Japan and South Korea led in technological readiness evident from our earlier analyses. Additionally, China, South Korea, Japan and Singapore were ranked in the top 10 by the 2018 Global Digital Economy Development Index that assessed the overall digital economy development in more than 150 countries and regions worldwide [13].

The enabling factors of a hub namely the availability of talent pool in the innovator group, funding and capital, infrastructure and programme as well as demands for business efficiencies or financial inclusion, allow blockchain projects to flourish. From the performance of these enablers, we identified China, Japan, Singapore and South Korea to be fast-growing blockchain hubs in Asia relative to other countries in the region.

3. Analysis by Country

We analysed the status of blockchain development in these four countries from four aspects: regulations and standards, characteristics of blockchain startups, enterprise- and government-backed blockchain projects, and research.

We extended our study of regulations to those for cryptocurrencies-related activities such as ICOs and cryptocurrency exchanges, to present a more comprehensive view of the state of blockchain in the country. Given alternative supporting resources through retail and institutional investors, enterprises, or the government, we conceded that the prohibition or absence of regulations for ICOs or cryptocurrency exchanges did not imply the lack of support for blockchain projects.

3.1. China (Mainland)

3.1.1. Regulations and standards

With the support of the Chinese government and available skilled workforce, the digital economy was a primary driver of economic growth in China contributing 30.3 per cent of China's GDP [14]. Before the state intervention on cryptocurrency trading, Chinese investors invested heavily in cryptocurrencies without knowledge of the market nor the underlying mechanism [15].

To mitigate financial risks brought about by the volatility of Bitcoin and cryptocurrencies, seven authorities in China issued a joint announcement in September 2017 to prohibit onshore and offshore platforms related to ICOs and cryptocurrency trading [16]. Nevertheless, the prohibition did not extend to the development of bitcoin's underlying technology – blockchain. Instead, the Chinese government took the lead in advocating the development of blockchain technology through a series of initiatives. In December 2016, the State Council of China included for the first time blockchain technology in the 13th Five-Year Plan to build a national strategic technological advantage. In June 2017, the central bank of China, People's Bank of China (PBoC), expressed their intent to promote research and application of advanced technologies such as blockchain and artificial intelligence (AI) in the five-year development plan for the financial industry [17]. Four months later, the Ministry of Industry and Information Technology (MIIT) released a white paper on China's Blockchain Technology and Application Development, the country's first official guidelines on the blockchain. Additionally, the State Council issued a mandate to the local government to accelerate the development of technologies, including blockchain in May 2018 [18]. Most recently in April 2019, the regulator, Cyberspace Administration of China, endorsed 197 blockchain service providers; the endorsement gave confidence to the industry for the deployment of their services.

To nurture this vibrant technology and innovation hub, the Chinese government further introduced regulatory guidelines for technology applications. A FinTech committee was set up by PBoC to strengthen the application of RegTech (regulation technology that addresses regulatory challenges in financial services using innovative technologies such as big data, AI, and blockchain) [19]. FinTech startups, namely Gingkoo and PeerSafe, have introduced regulatory frameworks and solutions on blockchain for domestic government and banks.

3.1.2. Blockchain startups

Despite the prohibition of ICOs, new blockchain companies in China outnumbered that of the US in 2016; these Chinese blockchain startups accounted for 28 per cent of new startups globally [20]. Furthermore, as at the end of 2017, China submitted the most

patent applications for blockchain with 550 patent submissions, nearly twice that of 284 applications from the US [21].

There were over 400 blockchain startups in China as of March 2018, according to data from ITJuzi and BlockData. Instead of blockchain solutions, infrastructure and social media, the majority of Chinese blockchain companies focused on technology applications for the financial industry, and on traditional economic sectors like: agriculture, manufacturing, supply chain and logistics. Seventy-eight per cent of these operated out of Beijing, Shanghai, Shenzhen, and Hangzhou, which suggested an agglomeration effect.

Wanxiang Blockchain Labs, a non-profit research institution funded by China Wanxiang Holding setup the first blockchain research centre in Shanghai in 2015 to pioneer research, development, and application of the technology. Projects like Bubi Chain and Juzix worked on developing blockchain infrastructure to build the ecosystem. In the meantime, many startups have proposed blockchain-based commercial platforms to solve real-life issues. For example, Qulian Technology provided enterprise-level blockchain products and application solutions such as supply chain finance and traceability, digital certificate, and energy assets.

3.1.3. Enterprise- and government-backed projects

While startups experimented with new and novel ideas associated with blockchain, existing industry leaders explored potential solutions using blockchain technologies. The three Internet tech giants in China, Baidu, Alibaba and Tencent (collectively known as BAT), have started projects related to blockchain.

Baidu became a member of an open source industry blockchain initiative named Hyperledger in October 2017. Baidu has launched its blockchain-as-a-service (Baas) platform, and Alibaba has successfully applied blockchain in areas such as healthcare and e-commerce. Alibaba built a supply chain tracking system using blockchain technology together with PwC in March 2017. In the same year, Tencent invented the TrustSQL platform to develop blockchain applications and provide enterprise service solutions. Tencent established the first digital private bank in China, WeBank. Blockchain Open Source (BCOS) platform was the first commercial blockchain technology platform to be introduced in China jointly by Wanxiang Blockchain Labs and WeBank. Ant Financial, the financial affiliate of Alibaba, and Baidu published a white paper to illustrate their blockchain strategic roadmap in 2018. Besides BAT, other corporations like Huawei, Xunlei and JD.com (logistics tech giant) have incorporated blockchain into their firms' strategic plan and released white papers related to blockchain projects.

To support blockchain startups, the municipal governments of Chinese cities launched blockchain-dedicated funds. Example, Xiong'An Global Blockchain Innovation Fund equivalent to US$1.6B was launched in Hangzhou in April 2018 , and a district government of Nanjing city launched another blockchain fund of US$1.4B in July 2018[xii].

3.1.4. Research

Research in technology has been a focal area for the Chinese national and local government bodies. The volume of blockchain related publications and the number of research institutes increased rapidly in 2016. The number of blockchain research institutes that opened in the first four months of 2018 was equivalent to those that opened in the whole of 2017, which was three times the number in 2016 [22]. Apart from the government-led independent research institutes, corporations and universities established more than 90 per cent of the research institutes in China.

In 2017, the PBoC launched the Digital Currency Research Institute that focused on the development and research of digital currencies. So far, the Institute had filed more than 63 patent applications, according to China's State Intellectual Property Office (SIPO) [23, 24]. Its ultimate goal is to introduce a state-backed virtual currency that would combine blockchain-based cryptocurrencies with the existing monetary system.

3.1.5. Hong Kong

Hong Kong has been zoned a special administrative region compared to other cities in China mainland. Under the "one country, two systems" constitutional principle, Hong Kong maintained its own governmental system, legal, economic and financial affairs, including trade relations with foreign countries. This separate constitution enabled Hong Kong to play a vital role in promoting blockchain development in China and even the rest of Asia.

The Hong Kong government defined cryptocurrencies as "securities", similar to that of the US Securities and Exchange Commission (SEC). ICOs and cryptocurrency came under the Securities and Futures Commission (SFC). In November 2018, SFC defined a regulatory framework for trading, managing and distributing cryptocurrencies [25] which would facilitate the maturity of the regulatory framework in the long run for digital assets.

Meanwhile, the Hong Kong government supported the development of blockchain technology and related projects. As early as November 2016, the Hong Kong Monetary Authority (HKMA), jointly with Hong Kong Applied Science and Technology Research Institute (ASTRI), released a technical white paper on DLT. In

the same month, HKMA-ASTRI FinTech Innovation Hub was launched to provide a neutral ground for the FinTech industry and startups in Hong Kong [26]. Later in March 2017, HKMA and seven banks commercialised a blockchain-based trade finance platform which was officially launched by HKMA on 31 October 2018, named "eTradeConnect". Developed by a consortium of twelve major banks in Hong Kong including HSBC and Standard Chartered Bank [27], eTradeConnect aimed to improve trade efficiency, improve trust among trade participants, reduce risks and facilitate trade counterparties by leveraging digitalisation and blockchain technology.

HKMA collaborated with other regions and countries, including Singapore and Abu Dhabi. HKMA and Monetary Authority of Singapore (MAS) have signed and exchanged a Co-operation Agreement in 2017 to strengthen co-operation on FinTech [28] such as the Hong Kong Trade Finance Platform (HKTFP), an HKMA-led trade finance proof-of-concept based on DLT. In June 2018, HKMA worked with regulators in Abu Dhabi to develop a cross-border trade finance system using DLT [29]. These collaborative initiatives revealed the economic, technological and geographical advantages and capabilities of Hong Kong in the development of blockchain.

Besides government-run FinTech and blockchain projects, financial institutions, research centres and various startups have landed their projects in Hong Kong. Example, Ant Financial of Alibaba Group joined GCash of Philippines to launch the world's first blockchain-based remittance service built on Alipay blockchain technology [30]. The Bank of China Hong Kong developed a blockchain-based system for real estate appraisals to avoid mortgage fraud [31]. Over 20 various FinTech startups emerged from Hong Kong. Example, startup Crypto.com released Asia's first cryptocurrency Visa card in Singapore in September 2018 and subsequently in the US in November.
Blockchain research centres or laboratories by Deloitte and China Blockchain Application Research Centre were established in Hong Kong. Hong Kong University of Science and Technology received US$20 million research grant for blockchain payment system. To attract blockchain talents, the Hong Kong government effected special immigration policy to expedite immigration for job seekers with blockchain expertise. It released a talent list on 28 August 2018 for eleven professions including blockchain technology [32]. The Hong Kong's Quality Migrant Admission Scheme (QMAS) that administered points-based tests for job seekers in Hong Kong accorded lower entry barrier to those with blockchain expertise.

3.2. Japan

3.2.1. Regulations and standards

Japan was the first country that recognised bitcoin as a legal payment option and has a national system to regulate cryptocurrency exchanges. A cryptocurrency exchange registered with the Financial Services Agency (FSA) of Japan was considered a legitimate entity in Japan. To-date, there were sixteen approved cryptocurrency exchange operators in Japan and cryptocurrencies on these exchanges could be exchanged for fiat monies or alternative cryptocurrencies. Basic guidelines for ICOs that focused on investor protection and anti-money laundering were released by a research group led by academics at Tama University [33, 34]. Still under deliberation by the FSA, many anticipated that these guidelines would eventually pass as a law in Japan.

The regulatory landscape in Japan for cryptocurrency exchanges and ICOs paved a promising future for the development of blockchain projects. In 2016, the Ministry of Economy, Trade and Industry (METI) engaged Nomura Research Institute to survey domestic and international blockchain applications [35]. As an outcome of the survey, METI published the first version of evaluation templates to assess blockchain applications and completed the first evaluation for blockchain applications in healthcare, supply chain & logistics, and smart property in 2018 [36, 37]. The process uncovered legal and technical issues of blockchain applications for respective industries.

3.2.2. Blockchain startups

Compared to the exponential growth in bitcoin trading, the number of blockchain ventures in Japan was small relative to other regions in Asia. In 2016, among the 167 FinTech startups in Japan, there were only 20 blockchain-related businesses [38]. This phenomenon in Japan could be attributed to the stronger public sentiment on the use of bitcoin for official payment than the application of the underlying blockchain technology.

Nevertheless, the blockchain startup scene in Japan was encouraging with generous support from the Japanese government. In 2017, METI sent three blockchain startups to the US as part of the Silicon Valley-Japan Bridge Project [39]. In the private sector, major industry players or financial institutions have announced investment funds, incubators or co-working space for blockchain startups. For example, SBI Holdings, a global rank-1 corporate blockchain investor, invested approximately US$460 million in AI and blockchain fund [40]. Mizuho Financial Group, one of the three major financial institutions in Japan, sponsored Neutrino, the first blockchain co-working space in Japan [41]. In short, blockchain startups in Japan received assistance and mentorship from the government, enterprises and large financial institutions. Foreign startups in Japan had similar access to funding, facilities and advice on regulatory matters [42].

3.2.3. Enterprise- and government-backed projects

Enterprise-backed projects in Japan focused on building applications in financial services and supply chain. The Japan Exchange Group, Inc. (JPX) tested the streamlining of processes in the securities market and ownership registry through a proof of concept (POC) with six other financial institutions in Japan [43]. NTT Data, one of the largest information technology companies, collaborated with Mitsubishi UFJ Financial Group (MUFG) and Singapore's National Trade Platform to launch a blockchain POC that would foster trade between Singapore and Japan [44]. With Skuchain, NTT DATA developed a business collaboration platform for Japanese manufacturers to boost supply chain efficiency [45].

The three financial institutions in Japan have implemented blockchain projects to streamline trading, payment, and other financial services. Mizuho Financial Group and Sumitomo Mitsui Financial Group (SMFG) respectively launched blockchain to streamline trade transactions [46,47]. On the other hand, MUFG introduced its MUFG Coin for commercial and retail customers, as well as to incentivise its employees to reduce overtime hours for healthier lifestyles [48].

At the government level, Japan's New Energy and Industrial Technology Development Organisation (NEDO) under the instructions of METI, worked on several blockchain-based projects. Among them included the use of internet-of-things (IoT) to streamline infrastructure for trade information sharing, where NEDO operated in partnership with NTT Data. The Ministry of Internal Affairs and Communications explored the application of blockchain solution to process government tenders and introduced a roadmap for incorporating DLT in e-government services in 2018 [49].

The Blockchain Study Group, established by Deloitte Japan, Mizuho Financial Group, SMFG and MUFG, promoted blockchain adoption and education. The focus of this study group was to conduct studies on interbank payment and a Know-Your-Customer advanced platform. The Japan Blockchain Association facilitated collaboration and conversations between blockchain startups and the Japanese government. Other associations such as the Japanese Bankers Association whose members comprised banks, bank holding companies and bankers' association analysed the implementation of blockchain for financial services [50].

3.2.4. Research

Major financial institutions and universities led the blockchain research and development landscape in Japan. In April 2016, the Bank of Japan (BOJ) established the FinTech Centre in its Payment and Settlement Systems Department [51]. The BOJ conducted a joint research project entitled "Stella" with the European Central Bank (ECB). The Stella project evaluated the performance of using Hyperledger Fabric to facilitate large value payments and the "delivery versus payment" environment using single and cross-ledger platforms, respectively [52,53]. In academia, Japan has five university nodes in the BSafe. network that promoted scientific and interdisciplinary social and economic research [54]. In addition, the more notable academic initiatives include the teaming of University of Tokyo and University of Aizu with two industry organisations to study smart currency [55], the establishment of BASE Alliance between Keio University and University of Tokyo [56], and the establishment of Blockchain Research Lab at Kyushu Institute of Technology [57].

3.3. Singapore

3.3.1. Regulations and standards

A confluence of factors – global financial centre, public-private partnerships, engagement and consultation, public education – had shaped Singapore's emergence as a leading technological hub of the world.

On the regulatory front, MAS, the central bank of Singapore, adopted a nurturing stance of regulation, one that was conciliatory but strict. In 2016, MAS introduced a "regulatory sandbox" to foster experimentation of innovative business models for financial institutions and FinTech companies [58].

The MAS did not regulate Crypto-tokens, digital tokens or virtual currencies. Instead, the MAS regulated activities on the use of virtual currencies that would fall under the regulator's ambit, such as money laundering and terrorism financing. Digital tokens structured like securities in ICO, also known as equity tokens, must satisfy the requirements of the Securities and Futures Act (SFA). Cryptocurrency exchanges were regulated under the SFA by the MAS when such exchanges allowed the listing and trading of digital tokens.

Although the MAS had not issued specific legislation related to ICOs, it monitored activities and developments in the space carefully. Example, MAS issued a directive and warning to an ICO issuer to terminate its digital tokens offering in May 2018 as MAS assessed those digital tokens to represent equity ownership and they failed to satisfy SFA requirements [59].

To upskill the workforce in digital skills and promote lifelong continuous learning, Singapore's Ministry of Education launched a nationwide SkillsFuture Initiative. This Initiative provided subsidies on training and courses, including courses on blockchain.

Singaporeans and permanent residents received up to seventy per cent in fee subsidy and to a maximum of 90 per cent subsidy for those aged above 40. Institutions of high learning and industry associations including local autonomous universities each undertook a digital skill including blockchain, to lead in capability development.

3.3.2. Blockchain startups

There were 270 FinTech startups, including blockchain startups in Singapore [60]. Blockchain startups spanned across industries from the supply chain and logistics, social networking, FinTech, insurtech, gaming [61].

This year-to-date, Singapore was ranked third at 8.14 per cent relative to the world's total ICO projects after the US and UK [62,63]. The conducive regulatory environment, open and transparent business practices as well as the availability of skilled workforce, contributed to making Singapore an appealing hub for blockchain innovators and startups.

3.3.3. Enterprise- and government-backed projects

There were multiple prototypes, and POCs announced and implemented by consortia of conglomerates. In 2016, Bank of America Merrill Lynch, HSBC and the-then Infocomm Development Authority of Singapore built a POC to streamline the paper-based import/export documentation using the Hyperledger blockchain. PSA International, IBM Singapore and Pacific International Lines collaborated in August 2017 to develop a trial for blockchain-based supply chain business network solution. Singapore Airlines completed its POC in early 2018 for the world's first blockchain-based airline loyalty digital wallet that would allow frequent flyers to instantly convert air miles into loyalty tokens.

Besides investments by the private sector, "Project Ubin" by MAS jointly with the network of financial institutions, was launched to improve transparency and efficiency of clearing and settlement of payments and securities with DLT. To-date, "Project Ubin" had completed software prototypes of three different models of decentralised inter-bank payment and settlements.

3.3.4. Research

To stimulate research and development in the use of technology to improve quality of life and enhance economic opportunities, the government of Singapore set aside US$14 million under the Research, Innovation and Enterprise 2020 plan [64].
In addition, IBM centre for blockchain innovation (ICBI) that was opened jointly with Singapore's Economic Development Board (EDB), worked with government agencies, academia and other industry players to advance Singapore's contribution to FinTech innovation and facilitate the adoption of blockchain technology for finance, trade and commerce as well as develop the local workforce capabilities [65].

The National University of Singapore established an academic research laboratory and think tank for blockchain technology, CRYSTAL (cryptocurrency strategy, techniques and algorithms) Centre [66]. The Singapore University of Social Sciences FinTech & Blockchain Group bridged academia and industry to build and develop capabilities and skills in FinTech and blockchain through the twin engines of education and research that would realise financial integration and inclusion objectives.

As a blockchain hub, there were open dialogue and exchanges between regulatory, government and industry bodies in Singapore. Furthermore, voluntary and self-regulatory groups like Singapore FinTech Association, ACCESS (Association of Cryptographic Enterprises and Startups, Singapore) and BEST (Blockchain Enterprise and Scalable Technologies) Association, actively promoted the exchange of knowledge and best practices to advance the industry.

3.4. South Korea

3.4.1. Regulations and Standards

The government of South Korea supported the development and application of blockchain technology and have announced plans to invest over US$900 million into blockchain initiatives by 2019. There were six pilot projects in the initiatives, including livestock history management, personal customs clearance, simple real estate transactions, online voting, international electronic document distribution, and maritime logistics [67]. To accelerate growth through innovation, the government announced plans to revise the existing tax regime that would motivate companies to focus on nascent technology development, like blockchain [68]. The strategy of the South Korean government was to construct an "Encrypted Valley" for the global blockchain industry in Industry 4.0.

The Korean Financial Services Commission (FSC) confirmed the prohibition of ICOs in January 2019. When the Korean Financial Investment Association established Korea's first blockchain alliance at the end of 2016, South Korean investors participated actively in cryptocurrency transactions and ICOs until September 2017. Subsequently, the FSC prohibited all ICOs and enforced their governance given the financial risks of cryptocurrency investments and transactions [69]. The Korean FSC started to restructure the regulation on cryptocurrency trading in 2018 as more cryptocurrency exchanges opened in the country; only twelve cryptocurrency exchanges have passed its security

checks, while another eleven failed [70, 71]. Following in August, the Blockchain Law Society issued a clear mandate to create a proper regulatory framework for the blockchain and associated cryptocurrencies.

3.4.2. Blockchain startups

South Korean blockchain startups covered a range of industries, such as FinTech, insurance, social media, entertainment, real estate. Some of the most promising blockchain startups in South Korea worked on blockchain infrastructure & services (e.g. Icon, Blocko, Deblock), FinTech (e.g. Proof Suite, theLoop), cryptocurrency exchanges (e.g. Upbit, Korbit, Coinone), and social media services (e.g. Foresting, Lucidity). The startup Coinplug, supplied multiple blockchain related services like digital asset exchange, an identity-based blockchain platform and online service platform. Coinplug held the most patents in blockchain in South Korea and was ranked seventh globally in 2018.

The startups in South Korea sourced funding from the local and global technology giants. For example, Blocko that provided a platform for blockchain solutions had secured US$8.9 million in Series B funding from Samsung SDS early in 2016. Cultural exports were integral to South Korean GDP. Muzika, a blockchain startup, had attracted over ten thousand musicians and 2 million users from 150 countries globally, as well as crypto and blockchain investment groups [72].

3.4.3. Enterprise- and government-backed projects

To develop skilled talent in blockchain, the Minister of Science and ICT in South Korea announced new initiatives valued at US$720,000 in addition to the original S$900 million, to train students, construct blockchain research centres and foster 10,000 professionals by 2022 [73]. In September 2018, the government established an open-source blockchain platform, dubbed Gold Ore. This platform signed an agreement with multiple international organisations, such as the Korean Standards Association, Japan Blockchain Consortium and others, to conduct blockchain-related training for the industry.

On the enterprise side, Samsung launched its blockchain platform hosted in the cloud, named "Nexledger", in 2017. Nexledger applications covered digital identity, digital payment, digital stamping, supply chain finance, global warranty and digital provenance [74]. Besides Samsung, the LG launched its blockchain service platform in May 2018, named "Monachain". This platform offered digital authentication, community token and supply chain management for the finance, public, telecommunications and manufacturing industries [75]. Hyundai Group had made a substantial investment on the internet of things (IoT) side of blockchain.

The South Korean internet company, Kakao launched its blockchain subsidiary, GroundX, in March 2018. To-date, Ground X had over 50 million monthly developers to create blockchain services on its global public blockchain. In May 2018, ICON and LINE co-founded Unchain to build LINE's blockchain network. Unchain would develop various DApp services and expand the blockchain ecosystem.

3.4.4. Research

In December 2016, a group of twenty-one financial investment companies and five blockchain technology firms signed a Memorandum of Understanding to form a distributed ledger solution as a blockchain consortium. This consortium marked the first attempt in South Korea where multiple financial firms leverage blockchain technology for development.

At present, most blockchain developers worked from universities in South Korea, including Seoul National University, Korea University, Sogang University, Yonsei University. These universities launched blockchain related courses. Decipher, a think-tank in blockchain research at the Seoul National University made up of master- and doctoral-level researchers had engaged in blockchain research for over three years. There had been various collaborations between university and industry to nurture skilled blockchain professionals, such as the collaboration between Korea University and Huobi.

3.5. Comparison across Countries

Table 1 summarises the status of blockchain development in each of the four countries.

4. Conclusion and Discussion

4.1. Conclusion

From the previous and current state analysis of infrastructure and programme, Asian countries like Japan, Singapore, and South Korea stood out in technological readiness, as well as digital and regulatory infrastructure. Although China had yet to make its way into front ranking in global surveys, the country performed the best in terms of patents granted normalised by population. Enterprise-backed blockchain projects contributed to the volume of patent applications led by Chinese technology firms such as the BAT, Huawei, Xunlei, and JD.com. Chinese provincial governments encouraged technology development using blockchain-dedicated funds.

The focus areas for blockchain-based solutions differed across countries. Solutions by enterprise-backed projects in Singapore were related to trading and finance like those on the streamlining of import/export documentation, supply chain solutions and inter-bank payment and settlements. In Japan,

Table 1. Blockchain development status summary

Four Enablers	China	Japan	Singapore	South Korea
(I) Regulation and standards	- ICO & cryptocurrency trading banned except in Hong Kong where cryptocurrencies treated as securities - Blockchain advocated by the government - Fintech committee by the central bank (BoC) and blockchain included - First batch of blockchain service providers officially registered	- First country to recognise bitcoin as a legal payment option - Legalised cryptocurrency exchanges - Working towards legalising ICOs - Devising evaluation framework for blockchain projects	- Cryptocurrency regulated if structured like a security - Cryptocurrency exchanges that offered listing and trading of digital tokens regulated under the SFA by the MAS - Cryptocurrency monitored for money laundering & terrorism financing activities - Fintech regulatory sandboxes launched	- ICO banned outright - Cryptocurrency exchanges legalised - Blockchain advocated as existing tax regime being revised to encourage blockchain companies)
(II) Blockchain startups	- Accounting for 28% of new blockchain startups globally in 2017 - 78% are in 4 major cities - Areas: technology applications & enterprise-level blockchain solutions (e.g., Bubi Chain, Juzix & Qulian)	- 20 out of 167 fintech startups are blockchain-related in 2016 - Supported by enterprises & governments (e.g. NTT Data, Skuchain, METI) - Areas: IoT, gaming & energy industry	- 270 FinTech start-ups including blockchain start-ups - Areas: applications in supply chain & logistics, social networking, fintech, insurtech, gaming, financial exchanges, cloud infrastructure, payment & remittances (e.g., Qtum, NEO & VeChain)	- Supported by big enterprises (e.g. Samsung sponsored Blocko early) - Coinplug ranked in 7th in blockchain patent filed - Areas: fintech, insurance, social media, entertainment & real estate
(III) Enterprise- and government-backed projects	- Big companies like BAT, Huawei, Xunlei & JD.com have started projects related to the blockchain (e.g. Tencent created the 1st digital private bank WeBank & the TrustSQL blockchain platform; Alibaba built a supply chain tracking system using blockchain together with PwC) - Government-backed blockchain funds launched in a few cities (e.g. $1.6B launched in Hangzhou & $1.4B in Nanjing) - HKMA & 12 banks released a blockchain-based trade finance platform eTradeConnect	- NEDO on IoT for trade information sharing - MIAC on government tenders & e-government services - Deloitte Japan, Mizuho, SMFG & MUFG on interbank payment and KYC platform - JPX & 6 financial institutions on streamlining financial services - NTT Data on supply chain efficiency	- MAS Project Ubin for settlement of payments & securities between financial institutions and the central bank led the project - A project between Bank of America Merrill Lynch, HSBC & IMDA on trade documentation using blockchain technology - Singapore Airline's blockchain-based airline loyalty digital wallet - Singapore Smart Nation Initiative to improve living with new and emerging technology	- Government-backed blockchain talent project (e.g. MOS & ICT planning to invest US$720k to construct blockchain research centres and foster 10,000 professionals by 2022 - The government established an open-source blockchain platform named Gold Ore - Tech giants are investing in blockchain development (e.g. Samsung, LG & Kakao launched blockchain platform Nexledger; LG launched blockchain service platforms)
(IV) Research	- Surge in the number of new blockchain research institutes observed from 2016 to 2018 - More than 90% of research institutes were established by corporations and universities - PBoC launched the Digital Currency Research Institute that focuses on the development & research of digital currencies	- Led by major financial institutions & universities - Bank of Japan's FinTech Centre for payment & settlement - BSafe.network led by the University of Tokyo forming a blockchain research network for with over 30 member universities worldwide - University & industry collaborations for applied research on smart currency & blockchain	- Supporting research & development in the national RIE 2020 plan - University, government & industry collaboration (e.g. the IBM centre for blockchain innovation, the Cryptocurrency Strategy, Techniques & Algorithm Centre at NUS, FinTech & Blockchain Group at SUSS) - Volunteer groups of self-regulatory organisations (e.g. SFA, ACCESS & BEST)	- Financial and tech firms assigned MOU for blockchain consortium development. - Blockchain training courses launched in many universities - Universities & industry collaborating on blockchain research & application (e.g. Korea University collaborating with Huobi and KEB)

enterprise-backed projects were related to information sharing by financial institutions and government agencies. Like China, technology firms in South Korea, such as Samsung, LG, and Hyundai, initiated various enterprise-backed projects on blockchain technology. These developmental activities created a value chain of activities and opportunities.

Blockchain startups in China and South Korea built applications across a wide spectrum from FinTech, insurance, social media, to real estate, and more. On the other hand, the startups in Japan and Singapore tended towards FinTech applications. English is the official business language in Singapore; this appealed to investors and blockchain entrepreneurs globally. Perceived as a gateway in the east to countries in the west, startups from China, such as Qtum, NEO, and VeChain, had registered their firms in Singapore. The source of funding and capital for startups at their early stage in China, Japan, and South Korea, were mostly domestic.

The existing regulations in China and South Korea prohibited the exchange and trading of cryptocurrencies and ICO. Meanwhile, Japan and Singapore adopted a more nuanced stance and issued clear policy statements.

The former legislation protected investors' interest and the latter statutory and regulatory approach could motivate blockchain startups in fulfilling their project objectives. All four countries nurtured investments and developments in blockchain technology. For example, blockchain was included in official documents released by the Chinese national government and the first batch of blockchain projects were endorsed with service provider licenses. Likewise, the Japanese government published an evaluation framework for blockchain-based projects. South Korea revised its tax regime to encourage blockchain companies. The central bank of Singapore launched FinTech regulatory sandboxes in 2016 to promote and nurture technology innovation.

Although there were many blockchain startups or projects backed by large enterprises and government, to-date no blockchain-giants had emerged. We anticipated Japan to lead on the regulatory infrastructure front being one of the first to accept cryptocurrencies by legalising cryptocurrency exchanges, and the publication of a government-led evaluation framework for blockchain projects. The abundant technical talent pool in China among the innovator group might accelerate the growth of the hub. In Singapore, the favourable environment for ICO financing could support the funding requirements of blockchain startups with strong offerings. Although a small city-state relative to China, Japan and South Korea, the domestic talent gap, particularly in technical know-how could be mediated by Singapore's language capability and proximity to countries in Southeast Asia.

4.2. Discussion

This essay contributed to the growing body of literature on blockchain and informed the state of blockchain development in Asia. We reviewed the stage of development in four different countries in Asia and found these countries to have possessed similar characteristics in their blockchain ecosystem: innovators and developers supported by regulatory and digital infrastructure, funding and capital, as well as programmes for workforce capability development against ready demand for distributed ledger or blockchain technology.

The performance of these four enablers would impact the speed of development of each hub given the nascent state of blockchain development.

On the regulation front of the infrastructure and programme enabler, we projected the pace of change to differ by countries.

The regulators of these four countries we have reviewed shared similar approach towards the blockchain technology – a deliberate and agile strategy to protect the public's interest while advocating technology innovation. Industry bodies could be the catalyst to initiate self-regulating organisations to network, exchange knowledge and best practices, promote standards, and engage the startups and regulators constructively.

As each of the four countries competes to attract and develop technical expertise in blockchain technology, they would have to harness their unique value propositions to develop capabilities and sustain the hub of activities.

4.3. Future Trends

Going forward, two factors shape the developments of these blockchain hubs – one factor at the network level facilitated by one or more catalyst firms and another within the network.

In the network paradigm of a hub, Dhanaraj and Parkhe identified the role of a catalyst firm in a hub that comprised of diverse stakeholder groups [2]. We drew parallel in forecasting the future developments of blockchain hubs. The presence of a catalyst firm in a blockchain hub would accelerate development to realise both economic and social impact of the hub. Such a catalyst firm could be the coordinator between regulators and startups to facilitate communication and knowledge sharing. Any organisation could step up to be the catalyst, such as an industry association, a research institute, a government agency or even a technology corporation.

The second influencing factor for the future of these blockchain hubs would be endogenous in the network. By this, we refer to the capabilities of the workforce in a blockchain hub. These capabilities of a blockchain hub shape the speed of its future development. Capabilities include technical skills and capabilities, as well as the language communication skills of the workforce to transcend cultural differences and collaborate with global teams.

4.4. Limitations

4.4.1. Biases from language

The data collected for analyses of this paper were predominantly in English. For example, a patent application might be filed in vernacular languages instead of English in countries like China, Japan, and South Korea. Google Trends was the primary source to gather search trends for ICOs. This approach introduced biases in our study of China, Japan, and South Korea, where official languages were non-English. We attempted to minimise such biases by collecting data from multiple sources. Future research could introduce expert opinion surveys in respective local languages for comparative analyses.

4.4.2. Temporal analysis and quantitative analysis

Although we had systematically investigated each of the four hubs separately, focusing on its regulation, standards and research development over time, this paper had not addressed agglomeration effects within the country. First-tier cities in China such as Beijing, Guangzhou, and Shanghai were key contributors to patents filed and granted. Subsequent research could extend beyond country-level analyses to study the agglomeration effects within the country.

This paper served as a qualitative analysis across blockchain hubs in Asia. Subsequent research using quantitive analysis could consider quantifying each of the enablers as inputs into an index to monitor and track the development of blockchain hubs through inter-temporal analysis, regionally and globally.

References:

[1] D. K. C. Lee, and L. Low, "Inclusive Fintech: Blockchain, Cryptocurrency And ICO", World Scientific, Singapore, 2018.

[2] C. Dhanaraj, and A. Parkhe, "Orchestrating Innovation Networks", The Academy of Management Review, vol. 31, no. 3, pp. 659–669, Jul. 2006.

[3] S. Chishti, and J. Barberis, The FinTech Book. Chichester : John Wiley & Sons, 2016.

[4] D. Andrews, G. Nicoletti and C. Timiliotis, "Digital technology diffusion: A matter of capabilities, incentives or both?", OECD Economics Department Working Papers, No. 1476, OECD Publishing, Paris, Jul. 2018. [Online]. Available: doi.org/10.1787/7c542c16-en.

[5] Asian Development Bank, Key Indicators for Asia and the Pacific 2018 (49th Edition). Manila: Asian Development Bank, 2018.

[6] D. K. C. Lee, M. Chwierut, W. Anderson, B. Lio, and B. Downes, "The Characteristics of Token Investors", in book "Inclusive Fintech: Blockchain, Cryptocurrency And ICO", World Scientific, Singapore, pp. 125-172, 2018.

[7] A. Kerya, "ICO Statistics: Countries, Traffic, and Investors", Medium.com, Jun. 2018. Accessed on: Oct. 6, 2018. [Online]. Available at URL: https://medium.com/@incryptico.com/ico-statistics-countries-traffic-and-investors-4e830e0438b0.

[8] T. Alford, "Bitcoin Adoption: Trading Volume by Country", TotalCrypto.io, Aug. 2018. Accessed on: Oct. 6, 2018. [Online]. Available at URL: https://totalcrypto.io/bitcoin-adoption-trading-volume-country/.

[9] A. Wright, and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015. Available at SSRN 2580664.

[10] A. Demirgüç -Kunt., L. Klapper, D. Singer, S. Ansar, and J. Hess, The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution. The World Bank, 2017.

[11] The World Bank. "Record High Remittances Sent Globally in 2018". Retrieved from World Bank Group - International Development, Poverty & Sustainability. Apr. 2018. [Online]. Available at URL: https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018.

[12] Startup Genome, "Global Startup Ecosystem Report 2019", San Francisco: Startup Genome LLC, 2019.

[13] Aliresearch and KPMG, "Welcoming a New Wave of Global Economy: Digital Economy Development Global Index 2018", Sep. 2018. Accessed on: Sep. 28, 2018. [Online]. Available at URL: http://www.199it.com/archives/774852.html.

[14] China Academy of Information and Communications Technology (CAICT), "White Paper on the Development of the Digital Economy in China", CAICT, Jul. 2017. Accessed on: Aug. 25, 2018. [Online]. Available: http://www.cac.gov.cn/files/pdf/baipishu/shuzijingjifazhan.pdf.

[15] L. Liu, and Q. Wang, "Analysis of Bitcoin Herd Behavior Based on Imitation and Infection Model", Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition), Vol.17, No.2, pp.27-33, 2015.

[16] Ministry of Industry and Information Technology (MIIT), "Announcement on preventing financial risks of ICOs", 2017. Accessed on: Sep. 26, 2018. [Online]. Available at URL: http://www.miit.gov.cn/n1146290/n4388791/c5781140/content.html.

[17] National Development and Reform Commission (NDRC), "The 13th five-year plan for economic and social development of the People's Republic of China (2016–2020)", Central Compilation & Translation Press, 2017. Accessed on: Sep. 20, 2018. [Online]. Available: http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf.

[18] M. Amsili, "Blockchain in China: Local is Everything", supchina, Aug. 2018. Accessed on: Sep. 20, 2018. [Online]. Available at URL: https://supchina.com/2018/08/28/blockchain-in-china-local-is-everything/.

[19] G. Sun, "Expectations on the Development of Blockchain in China", Caixin, Jun. 2017. Accessed on: Sep. 27, 2018. [Online]. Available at URL: http://opinion.caixin.com/2017-06-17/101102805.html.

[20] Wuzhen Think Tank, "The white paper on the development of China's blockchain industry", 2017. Accessed on: Sep. 23, 2018. [Online]. Available: http://sike.news.cn/hot/pdf/12.pdf.

[21] C. Liu, "Blockchain - A Guide for Officials," People's Daily Press, pp.132-134, 2018.

[22] X. Fei, and S. W. Li, "Blockchain Courses Among Global Universities and Blockchain Research Institutes in China", BlockData, 2018. Accessed on: Sep. 29, 2018. [Online]. Available at URL: https://www.8btc.com/article/195209.

[23] M. Xing, "63 patent applications filed by the PBoC digital currency research institute", Jun. 2018. Accessed on: Oct. 2, 2018. [Online]. Available at URL: http://finance.ce.cn/rolling/201806/29/t20180629_29567884.shtml.

[24] W. Zhao, "South Korea Plans Tax Perks for Blockchain Startups", coindesk, Jul. 2018. Accessed on: Sep. 28, 2018. [Online]. Available at URL: https://www.coindesk.com/south-korea-plans-tax-perks-for-blockchain-startups/.

[25] Securities and Futures Commission (SFC), "SFC warns of cryptocurrency risks", Feb. 2018. Accessed on: Sep. 1, 2018. [Online]. Available at URL: https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR13.

[26] Applied Science and Technology Research Institute (ASTRI), "HKMA-ASTRI Fintech Innovation Hub", Nov. 2016. Accessed on: Sep. 12, 2018. [Online]. Available at URL: https://www.astri.org/technologies/joint-research-laboratories/rd-centres/hkma-astri-fintech-innovation-hub/.

[27] HKMA, "Fintech Co-operation between the Hong Kong Monetary Authority and the Financial Services Regulatory Authority of Abu Dhabi Global Market", Jun. 2018. Accessed on: Sep. 10, 2018. [Online]. Available at URL: https://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180626-4.shtml.

[28] HKMA, "Fintech Collaboration between the Hong Kong Monetary Authority and the Monetary Authority of Singapore", Oct. 2017. Accessed on: Sep. 10, 2018. [Online]. Available at URL: https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20171025-4.shtml.

[29] HKMA, "The launch of eTradeConnect and the Collaboration with we.trade", Oct. 2018. Accessed on: Apr. 20, 2019. [Online]. Available at URL: https://www.hkma.gov.hk/eng/key-information/press-releases/2018/20181031-4.shtml.

[30] Business Wire, "AlipayHK and GCash Launch Cross-Border Remittance Service Powered by Alipay's Blockchain Technology", Jun. 2018. Accessed on: Aug. 8, 2018. [Online]. Available at URL: https://www.businesswire.com/news/home/20180625005561/en/.

[31] A. Antonovici, "Bank of China HK Uses Blockchain for 85% of Real Estate Valuations", Cryptovest, Apr. 2018. Accessed on: Sep. 10, 2018. [Online]. Available at URL: https://cryptovest.com/news/bank-of-china-hk-uses-blockchain-for-85-of-real-estate-valuations/.

[32] W. Zhao, "Hong Kong to Expedite Immigration for Blockchain Job Seekers", coindesk, Aug. 2018. Accessed on: Sep. 12, 2018. [Online]. Available at URL: https://www.coindesk.com/hong-kong-to-expedite-immigration-for-blockchain-job-seekers.

[33] Y. Hagiwara, and Y. Nakamura, "Japan Unveils Guidelines for Allowing Initial Coin Offerings", Bloomberg, Apr. 2018. Accessed on: Sep. 27, 2018. [Online]. Available at URL: https://www.bloomberg.com/news/articles/2018-04-05/japan-plans-first-step-toward-legalizing-initial-coin-offerings.

[34] Tama University, (2018), "Call for Rule-Making on ICO", Apr. 2018. Accessed on: Sep. 7, 2018. [Online]. Available: https://www.tama.ac.jp/crs/2018_ico_en.pdf.

[35] Nomura Research Institute, "Survey on Blockchain Technologies and Related Services FY2015 Report", Mar. 2016. Accessed on: Aug. 28, 2018. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf.

[36] Information Economy Division, Commerce and Information Policy Bureau, "Evaluation Forms for Blockchain-based System ver. 1.0", Ministry of Economy, Trade and Industry, 2017.

[37] Information Economy Division, Commerce and Information Policy Bureau, "Survey on Technology and Institution related to Distributed System", Ministry of Economy, Trade and Industry, 2018.

[38] T. Wilson, "Expert Shortage Hampers Japanese Financials in Blockchain Race", Aug. 2016. Accessed on: Oct. 2, 2018. [Online]. Available at URL: https://www.reuters.com/article/us-japan-fintech-blockchain-idUSKCN10S2GN.

[39] Ministry of Economy, Trade and Industry, "Japan Startup Selection" - The Participants of 2016 "HIYAKU Next Enterprise" Program", 2017. Accessed on: Sep. 30, 2018. [Online]. Available: http://www.meti.go.jp/english/press/2017/pdf/0105_001a.pdf.

[40] D. Cullinan, "World's First Bank-Backed Crypto Exchange Opens For Trading", BitcoinNews.com, Jul. 2018. Accessed on: Sep. 27, 2018. [Online]. Available at URL: https://bitcoinnews.com/worlds-first-bank-backed-crypto-exchange-opens-for-trading/.

[41] Mizuho Financial Group, Inc., "Collaborating to Create Japan's First Blockchain Coworking Space", May 2018. Accessed on: Sep. 30, 2018. [Online]. Available: https://www.mizuho-fg.com/release/pdf/20180518release_eng.pdf.

[42] Finolab, "About us - FINOLAB", 2018. Available at URL: https://finolab.tokyo/#aboutus.

[43] A. Santo, I. Minowa, G. Hosaka, S. Hayakawa, M. Kondo, S. Ichiki, and Y. Kaneko, "Applicability of Distributed Ledger Technology to Capital Market Infrastructure (Vol. 15)", Japan Exchange Group, Aug. 2016.

[44] NTT DATA Corporation, "MUFG and NTT DATA Lay Foundation for Digital Trade Between Singapore and Japan Using Blockchain", Dec. 2017. Accessed on: Sep. 28, 2018. [Online]. Available at URL: https://www.nttdata.com/global/en/media/press-release/2017/december/mufg-and-ntt-data-lay-foundation-for-digital-trade-between-singapore-and-japan-using-blockchain.

[45] NTT DATA Corporation and Skuchain, Inc., "NTT DATA will Develop a Business Collaboration Platform for Japanese Manufacturers in Cooperation with Skuchain in the U.S", Jan. 2018. Accessed on: Sep. 28, 2018. [Online]. Available at URL: http://www.skuchain.com/ntt-data-will-develop-a-business-collaboration-platform-for-japanese-manufacturers-in-cooperation-with-skuchain-in-the-u-s/.

[46] Sumitomo Mitsui Financial Group, "Demonstration Test of Blockchain Technology in Cross-Border Trade Operations", Dec. 2017. Accessed on: Aug. 28, 2018. [Online]. Available at URL: http://www.smfg.co.jp/news_e/e110076_01.html.

[47] I. Ueno, "Japanese Financial Institution and FinTech", Mizuho Financial Group, 2017.

[48] Mitsubishi UFJ Financial Group, "Fintech, Blockchain and Digital Currencies", Mar. 2016. Accessed on: Sep. 30, 2018. [Online]. Available at URL: https://www.mufg.jp/english/ourbrand/featuredarticle/2016_03.html.

[49] Nikkei, "Japan Looks to Blockchains for More Secure E-Government Systems", Asian Review, Jun. 2017. Accessed on: Sep. 27, 2018. [Online]. Available at URL: https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-looks-to-blockchains-for-more-secure-e-government-system.

[50] Japanese Bankers Association, "Report of the Review Committee for the Possibility and the Challenges of Utilizing Blockchain Technology", Japanese Bankers Association, 2017.

[51] Bank of Japan, "Message from Governor Kuroda on the Occasion of the Establishment of the FinTech Center", Apr. 2016. Accessed on: Sep. 29, 2018. [Online]. Available at URL: https://www.boj.or.jp/en/paym/fintech/message.htm/.

[52] European Central Bank and Bank of Japan, "Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment", Sep. 2017. Accessed on: Sep. 29, 2018. [Online]. Available: https://www.boj.or.jp/en/announcements/release_2017/data/rel170906a1.pdf.

[53] European Central Bank and Bank of Japan, "Securities Settlement Systems: Delivery-versus-Payment in a Distributed Ledger Environment", Mar. 2018. Accessed on: Sep. 28, 2018. [Online]. Available: https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf.

[54] S. Matsuo, "BSafe.network: Current Member Universities", Bsafe.network, May 2019. Accessed on: May. 10, 2019. [Online]. Available at URL: http://bsafe.network/member-university/.

[55] S. Takagi, H. Tanaka, M. Takemiya, and Y. Fujii, "Blockchain-Based Digital Currencies for Community Building", GLOCOM, 2017.

[56] Keio Research Institute at SFC, "Announcement of BASE Alliance Establishment", Jul. 2017. Accessed on: Sep. 18, 2018. [Online]. Available: https://www.kri.sfc.keio.ac.jp/ja/press_file/20170724_base_en.pdf.

[57] HAW International Inc., "Blockchain Technology Research Lab Established Within the Institute of Information Engineering Research at the Kyushu Institute of Technology", Mar. 2018. Accessed on: Oct. 1, 2018. [Online]. Available: http://www.chaintope.com/en/wp-content/uploads/sites/2/2018/03/0306_PRESS_BC_KIT_EN_2.pdf.

[58] Monetary Authority of Singapore, "Fintech Regulatory Sandbox Guidelines", 2016. Accessed on: Sep. 30, 2018. [Online]. Available: https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/FinTech-Regulatory-Sandbox-Guidelines-19Feb2018.pdf?la=en&hash=1F4AA49087F9689249FB8816A11AEAA6CB3DE833.

[59] J. Lee, "MAS Slaps Warnings on 8 Cryptocurrency Exchanges; Bars ICO Issuer", Business Times, May 2018. Accessed on: Sep. 8, 2018. [Online]. Available at URL: https://www.businesstimes.com.sg/banking-finance/mas-slaps-warnings-on-8-cryptocurrency-exchanges-bars-ico-issuer.

[60] Startup Genome, "Global Startup Ecosystem Report 2018", San Francisco: Startup Genome LLC, 2018.

[61] Techinasia.com, "Tech in Asia - Meet the 15 top-funded blockchain companies in Singapore", May 2018. Accessed on: Oct. 6, 2018. [Online]. Available at URL: https://www.techinasia.com/.

[62] ICO Watchlist, (2018), "ICO Statistics - By Country", 2018. Accessed on: Sep. 12, 2018. [Online]. Available at URL: https://icowatchlist.com/statistics/geo.

[63] W. A. Kaal, "Initial Coin Offerings: the Top 25 Jurisdictions and Their Comparative Regulatory Responses", CodeX Stanford Journal of Blockchain Law & Policy, U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-07, 2018. Available: dx.doi.org/10.2139/ssrn.3117224.

[64] U-W. Lee, "Record S$19b Set Aside for R&D Until 2020", Business Times, Jan. 2016. Accessed on: Sep. 1, 2018. [Online]. Available at URL: https://www.businesstimes.com.sg/government-economy/singapores-future-economy/record-s19b-set-aside-for-rd-until-2020.

[65] F. Ungku, "IBM to open first blockchain innovation center in Singapore", Reuters, Apr. 2016. Accessed on: Sep. 28, 2018. [Online]. Available at URL: https://www.reuters.com/article/us-ibm-fintech-singapore/ibm-to-open-first-blockchain-innovation-center-in-singapore-idUSKCN0ZS03Y.

[66] National University of Singapore, "NUS Computing forms academic blockchain think tank", Sep. 2018. Accessed on: Sep. 25, 2018. [Online]. Available at URL: https://news.nus.edu.sg/press-releases/CRYSTAL-centre.

[67] Y. Yoon, "Korean Gov't Unveils Blockchain Technology Development Strategy", Business Korea, Jun. 2018. Accessed on: Sep 8, 2018. [Online]. Available at URL: http://www.businesskorea.co.kr/news/articleView.html?idxno=23184.

[68] W. Zhao, "PBoC filings reveal big picture for planned digital currency", coindesk, Jul. 2018. Accessed on: Sep. 29, 2018. [Online]. Available at URL: https://www.coindesk.com/pboc-filings-reveal-big-picture-for-planned-digital-currency/.

[69] R. R. O'Leary, "South Korean Regulator Issues ICO Ban", coindesk, Sep. 2017. Accessed on: Sep. 1, 2018. [Online]. Available at URL: https://www.coindesk.com/south-korean-regulator-issues-ico-ban/.

[70] FSC, "FSC Reshuffles Organizational Structure", Jul. 2018. Accessed on: Sep. 7, 2018. [Online]. Available at URL: https://www.fsc.go.kr/eng/new_press/releases.jsp?menu=01&bbsid=BBS0048.

[71] K. Helms, "Only 12 out of 23 Korean Crypto Exchanges Pass Probe - Inspector Under Fire", Bitcoin.com, Jul. 2018. Accessed on: Sep. 12, 2018. [Online]. Available at URL: https://news.bitcoin.com/only-12-out-of-23-korean-crypto-exchanges-pass-probe-inspector-under-fire/.

[72] Muzika, "Muzika Project Teaser", 2018. Accessed on: Sep. 20, 2018. [Online]. Available: https://www.muzika.network/assets/mzk-teaser-en.pdf.

[73] J. Kim, "South Korean Gov't to Invest $200 Mln in Blockchain Initiatives", Cryptoslate, Jun. 2018. Accessed on: Sep. 6, 2018. [Online]. Available at URL: https://cryptoslate.com/south-korean-govt-to-invest-200-mln-in-blockchain-initiatives.

[74] Samsung SDS, Nexledger™ A Blockchain Platform and Solution, White paper, 2017.

[75] M. H. Cho, "LG CNS Launches Monachain Blockchain Platform", ZDNet, May 2018. Accessed on: Aug. 20, 2018. [Online]. Available at URL: https://www.zdnet.com/article/lg-cns-launches-monachain-blockchain-platform/.

[i] Consolidated information from World Intellectual Property Organisation and IPR Daily statistics on blockchain patents between 2008 to 2018.

[ii] Source: CBInsights (https://www.cbinsights.com/research/unicorn-startup-market-map/)

[iii] Special Administrative Region (SAR)

[iv] R&D spending as per cent of GDP of APAC countries, World Development Indicators by the World Bank.

[v] http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf

[vi] http://www.eiu.com/Handlers/WhitepaperHandler.ashx?fi=Technological_readiness_report.pdf&mode=wp&campaignid=TechReadiness

[vii] Data obtained from ICOWatchList.com. https://icowatchlist.com/statistics/geo
[viii] Search volume of a 1-year period from 7 Oct, 2017 to 7 Oct, 2018. https://trends.google.com/trends/explore?q=%2Fm%2F0138n0j1
[ix] Results are based on the Venture Capital & Private Equity Country Attractiveness Index by IESE Business School, University of Navarra. https://blog.iese.edu/vcpeindex/ranking/
[x] A full list of national currencies exchanged for the 24 hours of total bitcoin volume can be found at the Coinhills website: https://www.coinhills.com/market/currency/
[xi] https://news.8btc.com/1-6-billion-government-backed-blockchain-fund-launched-in-hangzhou
[xii] https://www.coindesk.com/another-1-billion-blockchain-fund-to-launch-with-government-backing

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
YW, JR, CL and SWL designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
YW, JR, CL and SWL deeply thank Professor David Lee for his guidance and Ms Sherry Li for her support.

Photo by Sean Pollock on Unsplash

THE JBBA

COMMENTARY

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(5)2019

Decentralisation is Coming: The Future of Blockchain

Mark Fenwick[1], Erik P.M. Vermeulen[2]
[1] Kyushu University, Japan
[2] Tilburg University, The Netherlands
Correspondence: E.P.M.Vermeulen@uvt.nl
Received: 31 July 2019 **Accepted:** 12 August 2019 **Published:** 16 August 2019

Abstract
Advocates of blockchain believe that distributed ledger technologies can provide us with a technological infrastructure to challenge the concentrated power of tech giants such as Amazon, Facebook and Google, and create a more equitable, sustainable and decentralized world. This paper considers these claims and concludes that they are preferable to defending the status quo or arguing that a solution might be found in more and better regulations. Nevertheless, the future remains highly uncertain and we are currently living in a rapidly evolving "space" between two competing realities: a centralized old-world reality and a fast-emerging, but, as yet, incomplete, decentralized reality. We remain optimistic that decentralization is coming but identify powerful competing forces seeking to preserve the status quo. As such, we must encourage more organizations – business, government, investors, charities – to experiment with distributed ledger technologies and to participate actively in the digital transformation. We need more experimentation to address the current shortcomings of decentralisation and to ensure the early arrival of mainstream applications of a technology that has the potential to solve some of the most pressing global challenges of a digital age.
Keywords: *Bitcoin, Blockchain, Crypto-Economy, Decentralization, Digital Transformation, Distributed Ledgers, Disintermediation, Ethereum, Satoshi Nakamoto, Smart Contracts, Technology*
JEL Classifications: *K20, K22, K24, L50, M21, O30, O31, O33, O35, Q55*

1. Introduction

Advocates of blockchain – let's call them the "Evangelists" – believe that decentralised ledger technologies have the potential to address many of the most pressing problems of the digital age. We are all familiar with the problems. The massive concentration of economic power in companies such as Amazon, Apple, Facebook, Google, etc. The large-scale abuse of privacy via the hoarding and selling of personal information online. The systematic (and state-sponsored) political misinformation operations and the calculated spreading of so-called "fake news."

The Evangelists believe that these and other problems can only be solved with more technology, rather than through more rules and regulations. And, in the strongest version of this story, Evangelists claim that blockchain technologies have the potential to transform capitalism and herald in a more sustainable, egalitarian, and decentralised world. In this piece, we would like to offer a defense of this Evangelist view. Not least because it offers a more compelling vision of the future than those in denial about the scale of the challenges created by the digital revolution or those arguing that more and better rules and regulations are the answer.

Nevertheless, it is easy to be skeptical or cynical in the face of such idealism. After all, the Evangelist narrative cuts against previous experience of disruptive technologies.[i] Historians have often noted that new technologies start in the hands of nerds and dreamers motivated by the desire to make the world a better place (the Apple of Steve Wozniak). But this rarely lasts, and successful technologies ultimately end up in the hands of powerful corporations driven the desire to maximize profits and shareholder value (the Apple of Steve Jobs). According to this view, the Internet story is just the latest chapter in a sorry tale of a human failure to ensure that technology works for the benefit of all. After all, the corporate giants of today are amongst the biggest companies that have ever existed and there is ever-increasing inequality in wealth distribution.[ii] Everything we know about the history of technology and capitalism should make us treat the Evangelist

position with caution.

Moreover, the transformative potential of distributed ledgers can sometimes be difficult to see through all the noise and hyperbole that surrounds the "Blockchain Revolution."[iii] It is unfortunate, for instance, that blockchain technologies have attracted greedy opportunists and fraudsters keen to make a quick profit. The result? A series of ICO scams and other scandals that discredited the technology in many people's eyes before it had any real-world impact on our everyday lives. But, once the blockchain hype fades, and the opportunists have moved on to the next "big thing," will these technologies be able to deliver on their potential and promise? Or, are the skeptics and nay-sayers right when they suggest that this is just hype "all the way down?"

The paper has three parts. In the next section ('The Rise of Centralized Platforms'), we describe the emergence of the new tech giants that leveraged the new possibilities of the Internet to develop a platform business model. Furthermore, we identify various pressures that create ever-more centralization and concentrations of economic power in the platform economy. The next section ('The Decentralized Alternative of Blockchain Evangelists') identifies the Evangelical alternative; a radically different account of the future that seeks to utilize distributed ledger technologies to realize the idealistic vision of the original architects of the Internet as a decentralized global communications network. In doing so, a genuine alternative to the current tech giants can be conceived. We conclude ('Experiments in Decentralization') with some brief reflections on the need for more participation in the development of blockchain technology, smart contracts, and cryptocurrencies to address the current shortcomings of decentralization and to ensure that we will soon see mainstream applications of the technology.

The takeaway? We are currently living in a fast-developing "space" between two competing realities: a centralized "old world" reality and a fast-emerging, but, as yet, incomplete, "decentralized reality." We are cautiously optimistic that decentralization is coming, but acutely aware of the competing forces that seek to preserve the status quo.

2. The Rise of Centralised Platforms

The Internet today comprises two connected, but distinct, layers. Firstly, there are a series of open source protocols, such as HTTP, GPS, IMAP, POP, SMPT, etc., that first allowed computers to communicate with one another across global networks and which still provide the basic infrastructure of the system. The key characteristic of such protocols is that no one owns them, and anyone can use them free of charge. There is no license fee involved in using HTTP to set up a web page, or in using SMTP to send an email, or GPS to identify location. Secondly, there is the web-based layer, which emerged later, and which sits on top of the protocols providing various services. Think Amazon, Facebook, Google, Twitter: this layer is operated by profit-seeking corporations that – in contrast to the authors of the protocols – have always sought to maintain tight control over their services and operations. The history of the Internet can be told as a story of a shift in power from the open protocol idealism of the early years to the closed, centralized and controversial capitalism that dominates today.[iv]

Many of the companies operating on this second layer provide what me might call a coordination function between two or more groups of users, and this business model is usually described as a "platform."[v] Some platforms facilitate connections between the buyer and seller of goods (eBay, Amazon, Alibaba); some facilitate connections between those wanting a service and those willing to provide it (Uber, Airbnb); and others simply facilitate connections (information exchange) between friends (Facebook), content creators and consumers (You Tube, Medium, Netflix) or app developers and users (Google, Apple). However, what is common to all platforms is that they coordinate connections between "creators" and "extractors" of value and the platform generates a profit from making these connections, either by taking a commission or advertising.

The emergence and growth of platforms is a significant economic and cultural event, not least because they have become a routinized feature of everyday life within a short period. To illustrate this rise, consider that it took the radio 38 years to reach 50 million users. It took television 13 years to achieve the same degree of market penetration. But Facebook "only" needed two years to gain the same number of users. Now, it has an active user base of over 2 billion.

Moreover, the global proliferation of digital technologies and communication networks means that platforms can be established anywhere. The emergence of hugely successful platforms in China (Alibaba) or Indonesia (Go-Jek) illustrate the universal appeal and adaptability of this business model. It also shows how less developed economies might employ platforms as a means of "leapfrogging" an earlier (industrial) phase of economic development and "jump" directly into the digital age.[vi] Go-Jek "only" needed three years to go from 100,000 orders a day (in 2015) to 100+ million orders across 18+ services in 2018.[vii]

What is clear, however, is that as platforms have scaled, they have struggled to maintain their initial promise and platforms that were once disruptive have lost much of their initial appeal. And it is hard to ignore the problems experienced and created by platforms. There

are too many recent examples of well-known platforms "forgetting" the importance of improving people's lives. Although there are a number of reasons why platforms have tended to become more centralized and more "corporate," and have experienced these kinds of difficulties, two factors are worth emphasizing:

Firstly, markets tend to prefer a single service provider. Take Airbnb as an example. When a new platform service like Airbnb starts to take off, there's a strong incentive for the market to consolidate around that single provider. The fact that more customers start to use the Airbnb app means that more room-providers are attracted to join the platform, which in turn attracts more people looking for a room, as there are now more choices of rooms. As such, platforms are acutely sensitive to network effects.[viii] The more users there are on one platform, the more everyone benefits (more and better choices, more ratings, etc.). In addition, individuals who already have the app installed and their details stored on Airbnb have a strong incentive to stay with that platform. The costs of migrating to a different provider become prohibitive, even if the company or individuals running the company are revealed to be engaged in dubious practices. Although many consumers may very well prefer multiple service providers, there are clear incentivizes pushing everyone to stick with one dominant player, once that dominant platform has emerged.

Second, the need to innovate continually, whilst at the same managing the legal risk created by rapid expansion, requires more centralized forms of organization and governance. Platforms often start with a simple, idealistic proposition ("let's bring people together"). But, over time, they add more and more features, making their technological infrastructure more complex.[ix] The downside of this is that more developers are then needed to accurately deal with the increased technology complexity and managing such complexity requires more centralized and hierarchical organizational forms with more elaborate control mechanisms. This is particularly true of companies that scale globally. And when platforms become more prominent, they need to attract more investors and investment to fund further innovation. Again, this transforms the incentives of platform owners and short-term performance becomes critical. To improve financial performance or save costs, platforms may feel the need to change the rules of the game from one day to the other (without consulting the users of the platform) and the belief that such agility is better achieved with hierarchical and centralized governance structures can easily gain ascendancy.

We might say that platforms have exhibited a tendency towards two different types of centralization. On the one hand, "cartelization," in which fewer and fewer players dominate the market for a particular service, and, on the other hand, "corporatization," in which there is an ever-greater internal concentration of authority based on a clear and closed hierarchy.

If we accept this story of the inevitable decline of platforms, how should we respond? Again, there are competing views. Some claim that our only hope is to use the power of the Leviathan (the state or regional organizations, such as the EU) to rein in these corporate giants, through more and better rules and regulation.[x] Think anti-trust laws, data protection laws or laws controlling online speech. According to this line of thinking, we can't fix the problems with more technology. Recently, we can hear more and more talk around this "top-down," regulatory solution.

3. The Decentralised Alternative of the Blockchain Evangelists

The Evangelists, however, take a different view. These are not problems that can easily be solved by more or even smarter regulation, as the power and reach of the Internet giants is just too great for any regulation to be meaningful or effective. The size of many platforms makes them largely immune to state action[xi]. Instead, the Evangelists recognize the importance of technology-based solutions that can provide us with the vision and direction to build something better. This is a view that needs to be taken seriously and it is in this context that we need to think about distributed ledger technologies, such as blockchain, and smart contracts.[xii]

The key claim of Evangelists is that things can be different and that distributed ledger technologies have the potential to bring about a transformation to a better world.[xiii] To understand why and how, it is helpful to briefly go back to the origins of blockchain and the original white paper by Satoshi Nakamoto.[xiv] In this first statement, Nakamoto proposed a system for a digital currency that did not require a centralized trusted authority to verify transactions. Two key elements characterize the general system that was proposed in the Bitcoin whitepaper:

Firstly, a database scattered across many computers, with no single authority controlling and verifying the authenticity of the data. Secondly, the "work" of maintaining the database – what we now refer to as "mining" – was rewarded with small payments, in the form of tokens. If you used a part of your computer's power to maintain the integrity and security of the database, you would receive a reward in the form of tokens that could then be used to "buy" services or sold to third parties for profit. These tokens would grow increasingly difficult to earn over time, ensuring a certain amount of scarcity in the system. If you helped in the beginning (and helped the database to develop and grow) you would receive a larger reward, thus incentivizing early stage participation.

Evangelists believe that this combination of ideas are revolutionary.[xv] Firstly, they provide a way of agreeing on the contents of a database without anyone being in charge of, owning or otherwise controlling that database. Secondly, they provide a mechanism for rewarding people that made the database more valuable, but – crucially – without those people being paid by an owner of the database or owning shares in the corporation that controls the database. There would be no owner or controlling corporation of such decentralized databases. Nakamoto provided a model for supporting open protocols that wasn't available when the first tech giants emerged. And, for this reason, they have the potential to challenge the tech giants and change the world.

But, how does this technology have potential to transform capitalism and how is it connected to the protocol layer of the Internet described above? A comparison with Airbnb can be used to illustrate the possibilities of a distributed ledger model. A new open protocol could be created that contains a request: "I would like a room in PLACE between DATES." A decentralized blockchain database might then record the metadata of all users, such as personal information, past trips, credit card details, preferences and user and host rankings. The protocol for transmitting this request out onto the Internet would be completely open. Anyone (individuals, private companies, public authorities) who wanted to develop an app for responding to such requests would then be free to do so. In this model, when you transmit your request, you would not need to commit ex ante to a single provider (as you do now with Airbnb), but you would instead be free to announce your wishes to the world via the secure protocol and wait for competing offers from diverse providers of accommodation, ranging from anyone with a spare room though to large multinational hotel companies.

Tokens would be vital in allowing such a protocol to develop and scale, and early adopters would be rewarded with tokens that they could then use to either buy accommodation services themselves or sell on an exchange for real world currencies. Moreover, early adopters (app developers, providers of accommodation, etc.) would receive a proportionately larger share of tokens for entering and helping to develop the new ecosystem. As the protocol developed it would then attract outside investors, which would give the token a greater monetary value that, in turn, would encourage more participation.

Critics might argue that one company or group of companies might monopolize the new protocol, in the same way that the tech giants of today dominate various sectors of the Internet economy. Indeed, fully-fledged decentralized blockchain networks do not exist yet. Consider the technical and operational shortcomings of the Bitcoin blockchain. In discussions with mathematicians and other technologists, the following weaknesses are usually highlighted. Bitcoin's proof of work protocol has led to "mining pools" because of economies of scale and unbalanced reward structures. The anonymity in the blockchain network means that it is prone to "Sybil attacks" and "51% attacks."

Still, there are advantages in an open source plus decentralized database model that makes such a process of "cartelization" much less likely. For a start, it wouldn't present the same opportunities for abuse and manipulation that you find in the closed, centralized systems of Amazon, Facebook, etc. If a particular service provider did something I didn't like, it would be much easier to switch to an alternative service provider, as my information would not be retained by the service provider on a centralized database, but a decentralized, open source database connected to the protocol. The open standard would have a discipling effect on platform operators, as it would facilitate a level of migration (to other providers or simply opting out altogether) that is simply impossible today.

Tokens would also give a blockchain-based open protocol a number of advantages, in that it would provide an infrastructure to reward content creators. This seems preferable to the current situation on many platforms – especially social media platforms – where most content providers act without compensation, while the platform companies receive all the economic value of that content by selling advertising.

Finally, there are the potential security gains of a decentralized network. Would our personal information or transactions be more secure in a distributed blockchain than behind the elaborate firewalls of giant corporations like Google or Facebook? An openly readable ledger means anyone can check the integrity of transactions. The distributed cooperation component implies that "attackers" must be able to "out-compute" the entire network (which is practically impossible).

4. Experiments in Decentralisation

The takeaway from all of this? We are currently living in a fast developing "space" between two co-existing realities: a centralized "old world" reality and an emerging but incomplete new "decentralized reality." The centralized reality with its hierarchical organizations, rules, regulations, and institutions still prevails. It appears unlikely that we will soon say goodbye to our familiar, centralized procedures and organizations anytime soon.

Nevertheless, a more decentralized reality has already started to emerge.[xvi] As we have seen, trust in the "centralized companies" is already declining (mainly due to the concentration of power, wealth and

information), and distributed ledger technologies, including blockchain, are viewed by many as offering a superior long-term model. These technologies have the potential to create real level playing fields, transparency and applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

We have already passed the "tipping point" in our experimenting with decentralized technologies.[xvii] There's simply no going back. So, instead of being locked into the traditional "centralized" world or remaining trapped in the space between the two realities, it is better to see how digital technologies are shaping the "new world" and affecting all of our relationships.

As such, it is necessary to become actively involved in the further development of blockchain and smart contracts and the creation of a decentralized reality. Only, if we build the new reality together, will we ensure that a decentralized world can reach its full potential and offer greater transparency, convenience, and trust. When we co-create the future together in this way, new jobs, opportunities, possibilities will inevitably emerge. And incorporating multiple perspectives – business, mathematics, and law – will be essential to make sure that we make the right decisions in our journey towards a better decentralized world.

The broader context for this project is a number of significant cultural shifts. Digital technologies have already changed our expectations. Consumers have become smarter, better connected, and more demanding. They love the "speed" and "convenience" offered by digital technologies and they are not willing to give it up. The consumers' "voice" has become more powerful than ever before. As a result, their relationship with business has changed dramatically. Even business-to-business companies need to take consumer views more seriously.

Who, when and where people "trust" has also changed. Whereas in the past, we relied heavily on institutions, intermediaries, and other third parties, we increasingly place our trust in digital systems and algorithms. It appears that we have less and less confidence in "old world" institutions. The speedy development of distributed ledger technology (including blockchain), smart contracts and artificial intelligence will only further automate trust. Institutionalized trust is replaced by "digital trust." It is obvious that the automation of "trust," "faith," and "confidence" has a tremendous impact on worker-employer relationships, the meaning of leadership, and how management operates. The opportunity to communicate and interact with peers directly (through social media and without the interference of third parties) makes us more entrepreneurial and creates new opportunities to be creative.

Our "new" relationship with digital technology also makes it possible to have peer-to-peer connections, communications, interactions, and transactions. Algorithms and data-analytics help us find partners, assistants, sponsors, help, accommodation, etc. Of course, these digital systems aren't flawless, but the fact is that we increasingly rely on more decentralised, peer-to-peer systems. The convenience of these new systems attracts us. The looser (digital) connections and interactions are so much faster and more comfortable than the old "formal" ways of making fixed appointments and ritualized meetings. The Millennial generation, in particular, appears to understand this. They view decentralization as a given for autonomy, responsibility, and happiness. Millennials – and this is a mindset, more than a generation – just seem more attuned to the freedoms and possibilities of a flatter world. They understand that hierarchical structures and an overreliance on formal procedures often discourage open and honest discussion, leading to either indifference, apathy or burnout.

"Fully-fledged" decentralization doesn't exist yet. But the decentralization trend is evident, and we must be better prepared. There is no time for procrastination, and we need to become smarter about decentralization in order to ensure that the Evangelist vision of the future comes to fruition. Of course, current technologies and developments aren't perfect (misuse of data, fake news, etc.). But these issues cannot be solved by traditional and centralized means (regulations, etc.). We must collaborate to find decentralized and tech-driven solutions now.

---

[i] See, for example, Carlota Perez, Technological Revolutions & Financial Capital (2002); Timothy Wu, The Master Switch: The Rise and Fall of Information Empires (2010).

[ii] See Scott Galloway, The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google (2017).

[iii] Don Tapscott & Scott Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World (2016).

[iv] William Craig, 15 Biggest Internet Controversies of the Past Decade, FX Blog, (2018) available at: https://www.webfx.com/blog/web-design/15-biggest-internet-controversies-of-the-past-decade/.

[v] See Geoffrey G Parker, Marshall W. Van Alsyne & Shandgeet Paul Choudry, Platform Revolution: How Networked Markets are Transforming the Economy and How to Make them Work for You (2016); Alex Moazed & Nicholas J. Johnson, Modern Monopolies: What it Takes to Dominate the Twenty First Century Economy (2016).

[vi] The World Bank, for example, organized a Disrupting Development event on this theme in Bali in October 2018, available at: https://live.worldbank.org/disrupting-development.

[vii] Erik P. M. Vermeulen, Three Ways to Grow Your Business in a Digital Age, Medium (2017) available at: https://hackernoon.com/3-ways-to-grow-your-business-in-a-digital-age-86e8bb3f33d1.

[viii] See Paul Belleflamme & Martin Peitz, Platforms and Network Effects, Handbook of Game Theory & Industrial Organization 286-317 (2018); Nirmala Reddy, How to Harness the Power of Network Effects, Forbes (2018) available at: https://www.forbes.com/sites/forbescoachescouncil/2018/01/02/how-to-harness-the-power-of-network-effects/#2b41823462e8.

[ix] Platforms often use open source software and a "microservices" architecture to accelerate growth, be adaptable to change, and give more value to the end-users of the services. Think of these platforms as a collection of loosely coupled applications which are configured to interact through internal and external application programming interfaces (APIs). The API approach provides flexibility and windows to new and other platforms. It allows the platforms to attract innovative ideas from third-party developers. The downside is that more developers and more automation are needed to accurately deal with the increased technology complexity. This require more investments (more of which later) and a more centralized organization with more control and governance mechanisms.

[x] See, for example, Scott Galloway, The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google (2017).

[xi] Mark Fenwick, Joseph A. McCahery, & Erik P. M. Vermeulen, (2019). The End of 'Corporate' Governance: Hello 'Platform' Governance. European Business Organization Law Review, Vol. 20, No. 1, 171–199; Mark Fenwick & Erik P. M. Vermeulen, A Sustainable Platform Economy & the Future of Corporate Governance. European Corporate Governance Institute Law Working Paper, No. 441/2019, p. 1-38 (2019) available at: https://doi.org/10.2139/ssrn.3331508.

[xii] Mark Fenwick & Erik P. M. Vermeulen, Time for Regulators to Open the 'Black Box' of Technology, Lex Research Topics in Corporate Law & Economics Working Paper, No. 2019-2 (2019) available at: https://doi.org/10.2139/ssrn.3379205.

[xiii] Mark Fenwick & Erik P. M. Vermeulen. A Primer on Blockchain, Smart Contracts & Crypto-Assets, Lex Research Topics in Corporate Law & Economics Working Paper, No. 2019-3, p. 1-20, (2019) available at: https://doi.org/10.2139/ssrn.3379443.

[xiv] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), available at: https://bitcoin.org/bitcoin.pdf.

[xv] Steven Johnson, Beyond the Bitcoin Bubble, New York Times Magazine (January 16, 2018).

[xvi] See Mark Fenwick, Wulf Kaal, & Erik P. M. Vermeulen, Why Blockchain Will Disrupt Corporate Organizations: What Can be Learned from the Digital Transformation, Journal of the British Blockchain Association, 1(2), 1-11, (2018) available at: https://doi.org/10.31585/jbba-1-2-(9)2018.

[xvii] See, for example, Mark Fenwick, Wulf A. Kaal, Erik P.M. Vermeulen, The Unmediated & Tech-Driven Corporate Governance of Today's Winning Companies, University of St. Thomas (Minnesota) Legal Studies Research (2017) available at: https://doi.org/10.2139/ssrn.2922176; Mark Fenwick & Erik P. M. Vermeulen, Technology & Corporate Governance, The Texas Journal of Business Law (2019) vol. 48(1), 1-22.

Photo by Laurianne Huggins on Unsplash

THE JBBA

PERSPECTIVE

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(10)2019

Is Blockchain Part of the Future of Art?

Stylianos Kampakis
University College London, UK
Correspondence: stylianos.kampakis@gmail.com
Received: 30 July 2019 **Accepted:** 13 August 2019 **Published:** 17 August 2019

Art is an important part of our culture, and economy. The global art market reached $67 billion in 2018[i]. While some individuals might purchase art solely for their own enjoyment, for others it can be a status symbol or an investment.

However, the world of art is not without its problems. Two of the most important challenges are are fraud, and ownership of digital assets. However, blockchain is promising to solve both of these issues soon.

Fraud in artwork usually shows up in the form of forging. While it is not easy to estimate the total amount of money exchanged in forged art, it is clear that individuals and museums might be losing millions of dollars every year because of forging. In 2018, it was reported that a museum in France[ii] dedicated to the art of Étienne Terrus, discovered that most of the artworks were not real. There are also plenty other famous cases of forgery last year, such as that of an exhibition about Amedeo Modigliani in Genoa, where 21 of the 30 artworks were confirmed as fakes[iii]. While these paintings might have been worth millions of dollars (if they were authentic), the fakes were practically worthless.

These are only two of the forgery cases that took place in 2018. It is easy to find more examples, but what is shocking, is that a large part of the forgeries is never uncovered. It is possible that a forged artwork exchanges hands many times, until the final owner realizes that the actual value is zero.

Given blockchain's ability to help in the provenance of goods, it is a natural ally in the battle against art forgery. The problem of authenticity in art, is not different to the problem of provenance in supply chains. A work can be identified through a single identifier which can be, for example, an image hash, such as perceptual hashing. The ownership of the work can be stored on the blockchain. A smart contract or a Ricardian contract can be used in order to transfer ownership of the artwork.

There are different companies working on that problem right now, like Vastari and Thomas Crown Art. While no standard solutions have emerged, we are likely to see one in the next few years.

Another important problem that blockchain is aiming to solve, is the ownership of digital assets. While for physical assets the only problem is forgery, digital assets can be copied an unlimited number of times. Therefore, until blockchain came about, it was impossible to create digital collectibles.

The first instance of a blockchain-based collectible was the Rare Pepe Wallet, in 2016, based on an internet meme[iv]. However, the most monumental moment for crypto collectibles was the creation of Cryptokitties in 2017. Cryptokitties is by far the most successful game of crypto collectibles. In this game, the users own cats that have certain attributes, like colour or weird features like wings. The cats can mate with each other creating new cats with unique combinations of attributes. There are in total 4 billion cats that can be bred.

The game combines elements of collectible card games, with the breeding mechanism that could only exist inside a computer. The game reached a total number of 1 million transactions in October 2018.

At the time of writing, there are multiple exchanges for crypto-collectibles and blockchain-based artworks: opensea.io, digitalobjects.art, rareart.io, pixura.io, Known Origin, Maecenas and Makers Place are some of them. Artists can easily secure ownership their artworks on blockchain through Mintable or Pixura. On some of those exchanges, you can find collectibles and artwork that have reached higher price tags. Some artworks on Digital Objects can go up to $1000. On Open Sea, there are collectibles that are sold for 10 ethers or more, which, at the time of writing, amounts to more than $3000. Finally, a digital card of Elon Musk was recently sold for over $50,000.

Ethereum has fully supported crypto-collectibles,

through the ERC-721 standard. Much like the ERC-20 standard describes how to setup smart contracts for fungible tokens, the ERC-721 standard, describes how to setup a smart-contract for non-fungible tokens. That is, all tokens that are using this standard are unique. The aforementioned exchanges are all based on this standard.

So, to answer the question that was set out in the beginning of the article: Yes, blockchain is definitely going to play a key role in the future of art, and we saw in this short article two ways in which it is going to disrupt the world of art. It is clear that there are still some barriers to the widespread adoption of blockchain.

Cryptocurrency prices can still fluctuate rapidly, and the speculative bubble that burst in December 2018 might have hurt the credibility and popularity of cryptocurrencies. Also, buying Ethereum and exchanging is something that is not easy for everyone. While in practice, tools like the Metamask Chrome extension or the Brave browser make it easy to use Ethereum, audiences that are less familiar with technology might find this challenging. Given that a large part of high net-worth art buyers might be of older age, this can become a significant barrier.

However, given the usefulness of blockchain and its rising popularity, we expect that in the next few years accessibility will increase, and use cases will multiply. Therefore, blockchain for art is here to stay.

Disclaimer: *The author of this article is personally involved in this space, by using generative adversarial networks to create works of art and sell them on blockchain.*

[i] https://www.artsy.net/article/artsy-editorial-global-art-market-reached-674-billion-2018-6

[ii] https://www.theguardian.com/global/2019/jun/15/french-art-museum-full-of-fakes-etienne-terrus

[iii] https://www.telegraph.co.uk/news/2018/01/10/modigliani-paintings-thought-worth-tens-millions-denounced-fakes/

[iv] https://rarepepewallet.com/

Photo by Ciprian Boiciuc on Unsplash

FOR AUTHORS

We are now accepting manuscripts for
Volume 3, Issue 1 (March 2020).

Please submit your article by using the document template provided in the link below. Please do NOT include any author/institute identifiable details in the manuscript as this document is sent to the reviewers for a 'double blind' review. The details including author(s), affiliations, correspondence email, acknowledgements/COI/ if any, should be provided as a separate document.

https://www.britishblockchainassociation.org/jbba-template

(Max. word count = 5000 words, excluding references)

Step-by-step guide to manuscript submission:

1. Author submits the article via JBBA Scholastica site by using the above template, which must include: an article header, an abstract (max 300 words), a conclusion, and references (in IEEE referencing style). The abstract should reflect both content and emphasis of the paper. Please use 'British English' when spelling words, for example, write 'centralisation' with an 'S', and not 'centralization' with a 'z'. The article submission fee is $10 per artcile and is paid directly to Scholastica.
2. The article will undergo quick initial screening by the Managing/ Associate Editor-in-Chief. If it was deemed 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.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.
3. 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

4. The author(s) is/are informed of the review outcome by the Managing Editor. The final decision for all manuscripts is taken by the Editor-in-Chief or an Associate EIC. 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. 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.
5. We aim for a turnaround time of 5 weeks from submission to publication.

References

References should follow **IEEE** style referencing. IEEE referencing style, also known as the numerical system, uses numerical citations in square brackets to refer to a reference list at the end of the paper. You may wish to chose the resources below to easily cite the references in IEEE format:

http://www.citationmachine.net/ieee
OR
http://www.citethisforme.com/citation-generator/ieee

Here is an example of indicating relevant reference in the text:

"...The theory was first put forward in 1987 [1]."
"...Scholtz [2] has argued that....."
"...Several recent studies [3, 4, 15, 16] have suggested that..."
"...For example, see [7]."

Check out the link below for more information on IEEE referencing:

https://libguides.murdoch.edu.au/IEEE/text

Here is an example of how an IEEE reference list should appear at the end of the paper:

[1] T. Kaczorek, "Minimum energy control of fractional positive electrical circuits", Archives of Electrical Engineering, vol. 65, no. 2, pp.191–201, 2016.
[2] P. Harsha and M. Dahleh, "Optimal management and sizing of energy storage under dynamic pricing for the efficient integration of renewable energy", IEEE Trans. Power Sys., vol. 30, no. 3, pp. 1164–1181, May 2015.
[3] A. Vaskuri, H. Baumgartner, P. Kärhä, G. Andor, and E. Ikonen, "Modeling the spectral shape of InGaAlP-based red light-emitting diodes," Journal of Applied Physics, vol. 118, no. 20, pp. 203103-1–203103-7, Jul. 2015. Accessed on: Feb. 9, 2017. [Online]. Available: doi: 10.1063/1.4936322
[4] K. J. Krishnan, "Implementation of renewable energy to reduce carbon consumption and fuel cell as a

back-up power for national broadband network (NBN) in Australia," Ph.D dissertation, College of Eng. and Sc., Victoria Univ., Melbourne, 2013.
[5] C. R. Ozansoy, "Design and implementation of a Universal Communications Processor for substation integration, automation and protection," Ph.D. dissertation, College of Eng. and Sc., Victoria Univ., Melbourne, 2006. [Online]. Accessed on: June 22, 2017. [Online]. Available: http://vuir.vu.edu.au/527/

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.

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.

The JBBA accept articles in the following categories:

- **Original Scientific Research (Qualitative, Quantitative)**
- **Systematic Reviews**
- **Meta-analysis**
- **Conference Research Abstracts**
- **Comparative studies**
- **Case Studies & Essays**
- **Book Reviews**
- **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.
Editor-in-chief has overall responsibility for the content, production and strategic direction of the JBBA.

Time to publication

On average, papers receive a decision in **4 weeks** from first submission and accepted articles are published online and indexed in an additional 14 days.

Article Processing Charge

If your article is accepted for publication, we will ask you to pay the Article Processing Charge (APC) of **£685** (£585 for members of the British Blockchain Association). For full details about the APC and our waiver policies, please visit the 'About us' section of the journal:

https://jbba.scholasticahq.com/about

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.

Plagiarism Policy

We have a very stringent plagiarism policy in place and all articles are screened on **Viper** Plagarism Checking Tool for detection of plagiarism. We accept a plagiarism score of less than 10%. This allows the highest possible level of scholarly integrity and transparency in contents published by the JBBA.

General Guidance for Authors

The editors request that all articles shall be submitted via Scholasticahq portal using the word template document provided via the above link and must include an abstract. We prefer text in Garamond font, size 12, double spacing except for references at the end of the paper, which should be single space.

The Journal allows authors to deposit a copy of their own work at an instituitional repository.

The JBBA does not publish the work that has been published elsewhere. The only exception to that rule are original research papers published as "pre-print repositories" on SSRN or ResearchGate. 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. 500 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. The text of accepted manuscripts can sometimes be edited to enhance communication between the author and the reader.

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

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.

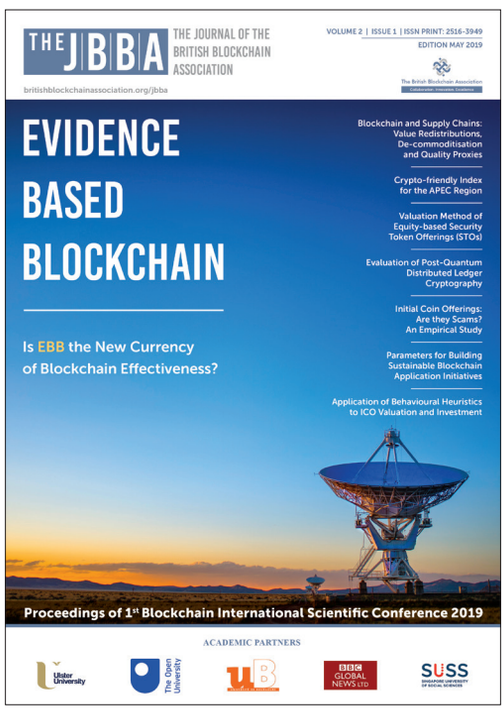
Those named as authors of a paper should have made a substantial contribution to the paper, or to a more general project of which the paper is a part, and anybody who has made such a contribution should be offered authorship.

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

THE BRITISH BLOCKCHAIN ASSOCIATION IS WORKING IN COLLABORATION WITH

Volume 1 - Issue 1
Edition July 2018

Volume 1 - Issue 2
Edition December 2018



Volume 2 - Issue 1
Edition May 2019

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

www.britishblockchainassociation.org

admin@britishblockchainassociation.org

Follow us on:

FELLOWSHIP

of

The British Blockchain Association of The United Kingdom (FBBA)

An award of the Fellowship is recognition of exceptional achievement and contribution to Blockchain and allied disciplines. The Fellowship demonstrates a commitment to excellence, leadership, advancing standards and best practice, evidenced by a track record of outstanding contribution to the discipline of Blockchain or other Distributed Ledger Technologies.

FELLOWSHIP BENEFITS

- The use of 'FBBA' post-nominal
- Exclusive opportunity to officially represent the BBA by playing an active role in the direction and governance of the Association
- Privilege to take on a leadership role within the BBA and the profession as a whole
- Opportunity to represent the BBA at International Blockchain Conferences
- Significant discounts on BBA conferences and events
- Opportunity to join the Editorial Board of the JBBA
- Free copy of the JBBA posted to your mailing address

The new Fellow appointments will be made twice a year (September and March).

Next Round of Fellowship Applications has been commenced (Applications submission Deadline: 30 January 2020)

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

The British Blockchain Association

Advocating Evidence Based Blockchain

www.britishblockchainassociation.org

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION