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

VOLUME 2 | ISSUE 1 | ISSN PRINT: 2516-3949
EDITION MAY 2019

The British Blockchain Association
Collaboration. Innovation. Excellence

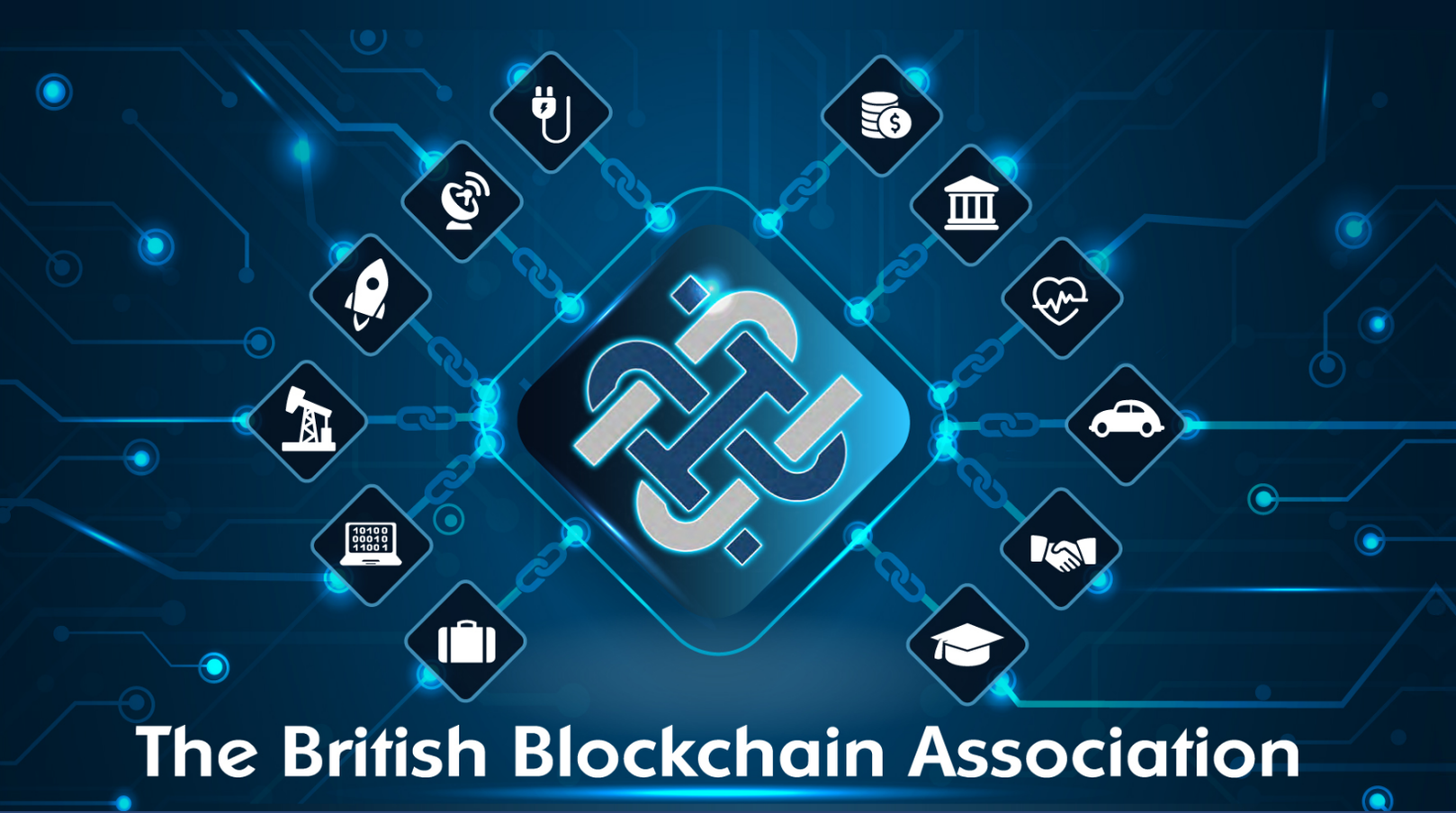
EVIDENCE BASED BLOCKCHAIN

Is EBB the New Currency of Blockchain Effectiveness?

Proceedings of 1st Blockchain International Scientific Conference 2019

ACADEMIC PARTNERS

Ulster University · The Open University · Université de Bourgogne · BBC Global News Ltd · SUSS Singapore University of Social Sciences



The British Blockchain Association

MEMBERSHIP BENEFITS

Find Solutions

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

Get Educated

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

Network

Become a part of a global blockchain community uniting organizations and individuals.

Influence

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

Promote

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

Reduce Costs

Get member only discounts and perks on valuable products and services.

WORKING IN COLLABORATION WITH:

appg BLOCKCHAIN | Department for International Trade | British Embassy Lisbon | GCPSE Global Centre for Public Service Excellence | UNDP Empowered lives. Resilient nations. | ENTERPRISE ETHEREUM ALLIANCE | Isle of Man Government Reiltys Ellan Vannin

OUR MEMBERS INCLUDE:

Web3 Labs | QADRE | Baker McKenzie. | NORDIC BLOCKCHAIN ASSOCIATION | GRANDEO | SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES | patientory association | pillar. | KAMBIO VENTURES | pl^g

Join Now at britishblockchainassociation.org/membership

BritishBlockchainAssociation.org

TABLE OF CONTENTS

1ST BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
12 MARCH 2019, LONDON

Photos by Haziqah Noor-ul-Islam


The British Blockchain Association
Collaboration, Innovation, Excellence
The World's Most Powerful Voice on
THE JBBA
OUR MEMBERS
Follow us on:


The British Blockchain Association
Collaboration, Innovation, Excellence


The British Blockchain Association
Collaboration, Innovation, Excellence
The World's Most Powerful Voice on Blockchain
THE JBBA
OUR MEMBERS
Follow us on:
To sponsor our events contact us at:
www.britishblockchainassociation.org
admin@britishblockchainassociation.org


The British Blockchain Association
Collaboration, Innovation, Excellence

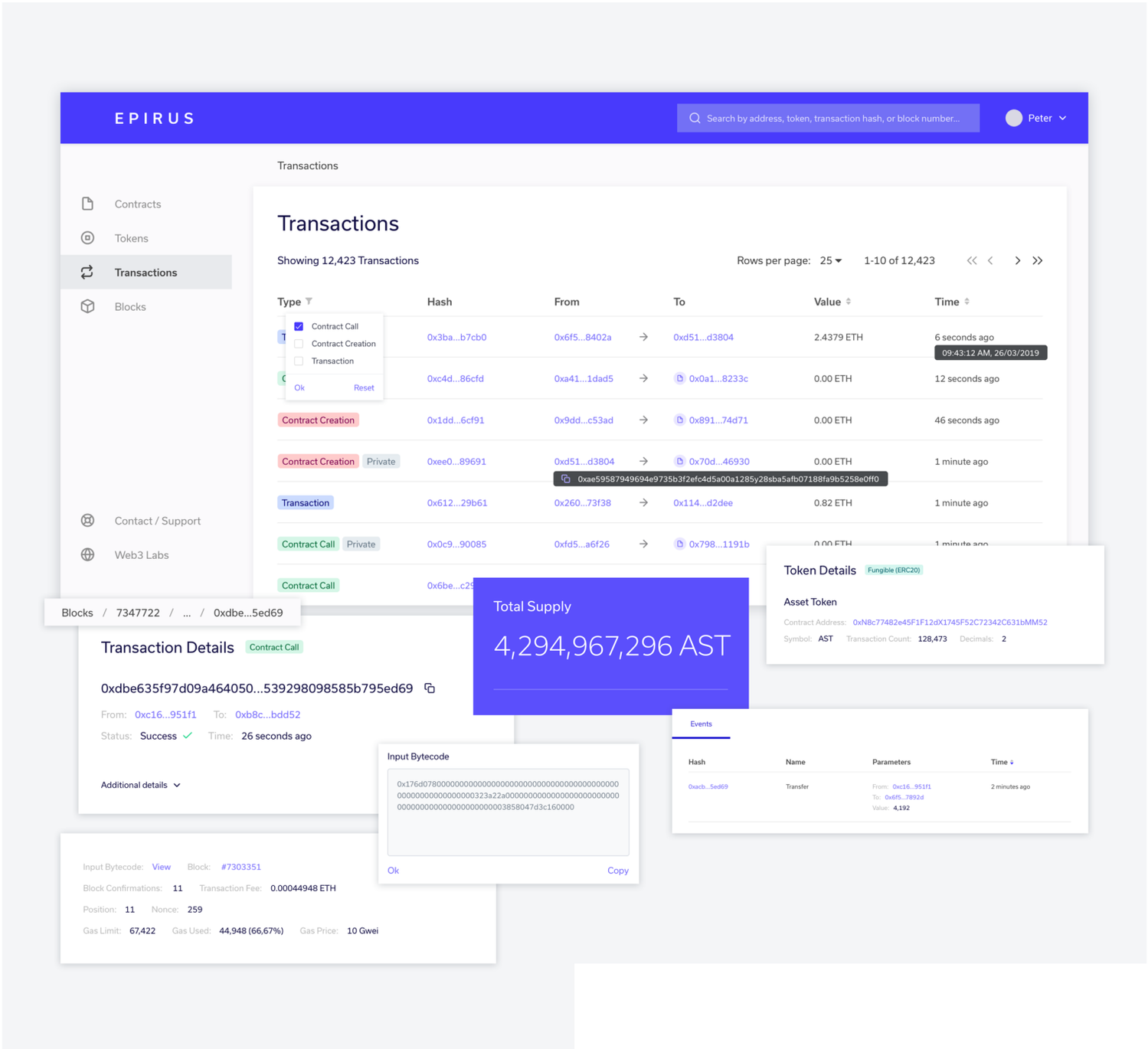

The British Blockchain Association
Collaboration, Innovation, Excellence
The World's Most Powerful Voice on Blockch
THE JBBA
OUR MEMBERS
Follow us on:


The British Blockchain Association
Collaboration, Innovation, Excellence


Panel Discussion 3: Role of Enterprises in supporting
Chair: Alastair Marke, The BBA & Blockchain C
BBA International Scientific Conference 201


BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2019
1ST BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE


BLOCKCHAIN INTERNATIONAL SCIENTIFIC CONFERENCE
#ISC2019
Panel Discussion 1: Evidence Based Blockchain & Scientific Publishing
Chair: Dr. Naseem Naqvi, Editor in Chief, The JBBA
BBA International Scientific Conference 2019



The Enterprise Blockchain Explorer

The Epirus Platform provides all of the business metrics you need to support your blockchain and smart contract applications.

For more information email hi@web3labs.com
or visit web3labs.com

Web3 Labs

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

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

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

Advertising

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

Photo by Martin Adams on Unsplash

EDITORIAL

Dr. Naseem Naqvi
Editor-in-Chief

It gives me great pleasure to present to you the 3rd Edition of the Journal of the British Blockchain Association.

This volume draws most of its contents from the proceedings of the **Blockchain International Scientific Conference (ISC2019)** held in London on 12 March. The event was a big success and was supported by many governmental, academic and international institutions including The BBC, The Open University, Edinburgh Napier University, Ulster University, University of Burgundy and Web3 Labs, to name a few. It was held under the title: **"Scholars in Blockchain building Evidence based Frameworks"**. The ISC2019 was accredited for 6 CPD (Continuing Professional Development) credits by the UK CPD Certification Services. The conference proved to be an excellent forum for exchange of scholarly ideas, ground-breaking research and academic networking.

Prize winner Maxwell Stanley from University of Essex, UK, presented his research on "*The Application of Behavioural Heuristics to ICO Valuation and Investment."* Robert Campbell of Capitol Technology University, USA, shared his work on *"Evaluation of Post-Quantum Distributed Ledger Cryptography"* (full text of the research is published in this issue) and Alfio Puglisi of Kings College London, UK, showcased his research abstract entitled, *"Capital Mobility in light of Emerging Technologies: the case of Crypto-Asset Investment"*.

The research papers that were accepted for publication in this issue are timely and topical – I believe these are of paramount significance to global blockchain community: Articles included in this edition are: *Distributed Ledgers and Post-Quantum Computing, Crypto Indices for APEC region, Blockchain & De-commoditisation of Supply Chains, Valuation frameworks for Security Token Offerings, Parameters for building sustainable Blockchain Applications, Application of Behavioural Heuristics to ICO Valuation and Investment and An Empirical Study on Initial Coin Offerings.*

We are committed to immediate and full Open Access of all contents published via the JBBA. The journal is now being read in over 150 Countries and territories. I was pleased to see that many PhD and MSc scholars have started citing the research published in the JBBA and the articles are being hosted on the websites of some of the most prestigious international universities.

Earlier this year, we awarded the **Fellowship of the British Blockchain Association** to individuals that have made exceptional contributions in the field of blockchain and cryptocurrencies. I would like to once again welcome our inaugural Fellows and looking forward to work very closely with them to advance Evidence Based Blockchain and The JBBA.

We have also launched The JBBA YouTube Channel. There are plans to upload cutting-edge scholarly contents including latest journal updates, debates, reviews and commentaries from researchers, reviewers and editorial board members.

The journal continues to attract high quality submissions from a very diverse global community of blockchain scholars. It will continue to play a central role in advancing Evidence Based practices and dialogue in the field of Distributed Ledger Technologies.

Lastly, I would like to thank our editors, reviewers, authors and readers who have shown faith in our collaborative efforts in order to build a very close-knit community of blockchain scholars. We invite researchers from the field of Blockchain, Distributed Ledgers and Cryptocurrencies to submit their work to us and thus be involved in one of the fastest growing areas of research today.

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

Until next time,

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

May 2019

Photo by J. Zamora on Unsplash

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*

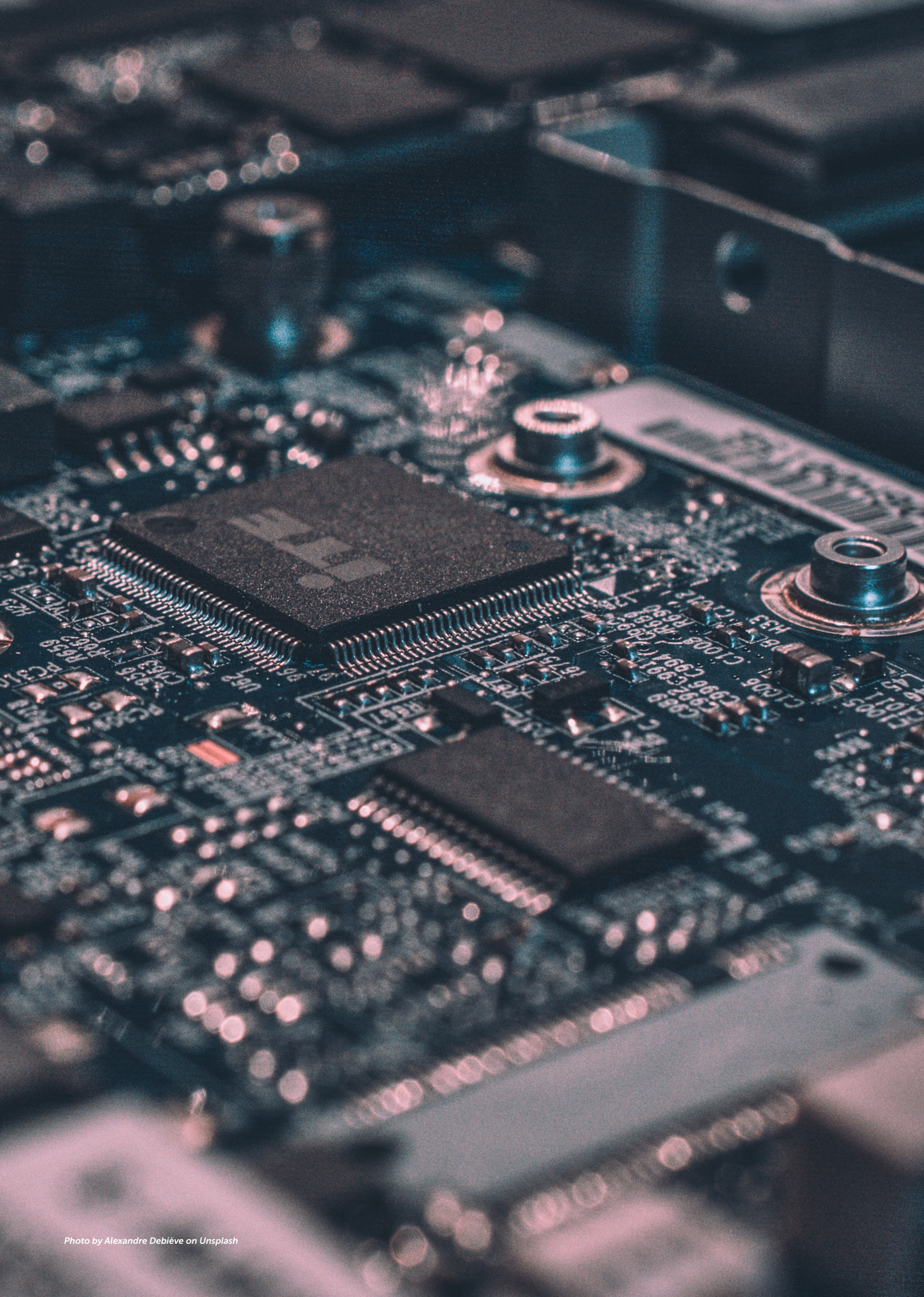


Photo by Alexandre Debiève on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-1-(4)2019

Evaluation of Post-Quantum Distributed Ledger Cryptography

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

Received: 8 January 2019 **Accepted:** 26 February 2019 **Published:** 16 March 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 would like to acknowledge Dr. Ian McAndrew for his supervision and guidance in preparing this research.

Abstract

This paper evaluates the current cybersecurity vulnerability of the prolific use of Elliptical Curve Digital Signature Algorithm (ECDSA) cryptography in use by the Bitcoin Core, Ethereum, Bitcoin Cash, and enterprise blockchains such as Multi-Chain and Hyperledger projects Fabric, and Sawtooth Lake. These blockchains are being used in media, health, finance, transportation and government with little understanding, acknowledgment of the risk and no known plans for mitigation and migration to safer public-key cryptography. The second aim is to evaluate ECDSA against the threat of Quantum Computing and propose the most practical National Institute of Standards and Technology (NIST) Post-Quantum Cryptography candidate algorithm lattice-based cryptography countermeasure that can be implemented near-term and provide a basis for a coordinated industry-wide lattice-based public-key implementation. Commercial quantum computing research and development is rapid and unpredictable, and it is difficult to predict the arrival of fault-tolerant quantum computing. The current state of covert and classified quantum computing research and advancement is unknown and therefore, it would be a significant risk to blockchain and Internet technologies to delay or wait for the publication of draft standards. Since there are many hurdles Post-Quantum Cryptography (PQC) must overcome for standardisation, coordinated large-scale testing and evaluation should commence promptly.

Keywords: *ECDSA, blockchain, post-quantum, lattice-based cryptography, cybersecurity, distributed ledger, qTESLA, Ring Learning with Errors, critical infrastructure*

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

1. Introduction

Rapid advances on a global scale in Quantum Computing technologies and the threat it poses to most standardized encryption prompted NIST to put out an international call for candidate quantum-resistant public-key cryptographic algorithms to evaluate for standardization. NIST will conduct efficiency analysis on their reference platform delineated in the *Call for Proposals*; NIST invites the public to perform similar tests and compare results on additional platforms (e.g., 8-bit processors, digital signal processors, dedicated complementary metal oxide semiconductor (CMOS), etc.) and provide comments regarding the efficiency of the submitted algorithms when implemented in hardware.

This research has two goals: the first is to examine the vulnerabilities in current Asymmetric Digital Signature Cryptography (ASDC) as used in private key generation in Bitcoin Blockchain technology in the PQC era. The second goal is to independently test and evaluate candidate NIST algorithms to assist in the process of selection of acceptable candidate cryptosystems for standardisation and the proposal of potential replacement of ADSC in private key generation in blockchain and distributed ledger technology. Most blockchain and distributed ledger technologies use an asymmetric digital signature scheme for private key generation such as, ECDSA, which has been cloned often from the Bitcoin Blockchain. These digital signature schemes are being implemented in critical sectors of government and the economy. Evaluations will include cryptographic strengths and weaknesses of NIST candidate pool of submitted algorithms. It is expected that the analysis will consist of required performance parameters that include:
Public Key, Ciphertext, and Signature Size, Computational Efficiency of Public and Private Key Operations, Computational Efficiency of Key Generation, and Decryption Failures against NIST provided Known Answer Test values (KAT).

Blockchain and Distributed Ledger cryptography private key generation cyber-security concepts are poorly understood, and often misrepresented. There is a misconception that Blockchain technology can't "be hacked," resulting in a general endorsement for critical sectors and industries [1]. The author believes that the technology offers excellent cyber-security promise for many areas, but the limitations and strengths must be defined. This work examines the weakness of the ECDSA and its current vulnerability and uses in the Bitcoin Blockchain or Distributed Ledger Technology (DLT). Many industries are rapidly adopting versions or mutations of the first of the Bitcoin Blockchain technology in essential sectors such as information technology, financial services, government facilities, healthcare, and Public Health Sector seemingly, without cybersecurity due diligence, a proper comprehension of the cryptography vulnerabilities or plans for addressing quantum computing threats [2]. The ECDSA is the foundation of Public Key Infrastructure (PKI) for many Internet applications and open source projects, and it's the primary source for public-key cryptography. The second part of this paper offers the most practical and near-term first-round candidate NIST Lattice-Based Post-Quantum Cryptography solution with a recommendation for immediate coordinated (academia, the private sector, government) independent testing, verification, and validation (IV&V) and test framework for sharing results [3]. This framework aids in speeding the approval of PQC standards that are vital to global cybersecurity. The scope of this work evaluates the lattice-based digital signature scheme qTESLA, based on the verifiable hardness of the decisional Ring Learning With Errors (R-LWE) [4]. Quantum computing's threat adversely affects the cybersecurity of financial services such as payment systems, general network communications systems, business functions including cloud computing, Internet of Things (IoT) and critical infrastructure. Further, the author believes that currently estimated timelines for the availability of large-scale fault-tolerant quantum computers are underestimated due to unpredicted global progress and the veil of secrecy surrounding classified research programs led by organizations and governments around the globe. It is, therefore, essential to begin work and testing the most likely candidate algorithms for normalization.

2. Implications in this work

Current encryption systems and standards such as Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Digital Signature Algorithm (DSA), and ECDSA impact everything from defense, banking, healthcare, energy, telecommunications, intelligence, Internet and the Blockchain. The compromise, disruption or non-availability of one of these sectors would severely impact the health and safety of U.S. national security, public health, safety or its economy.

Blockchain technology is a revolutionary technology that has great potential in many applications. This technology has gained global interest in all industry sectors based on cryptography-based algorithms that are considered vulnerable today but will be increasingly threatened by accelerated advances in quantum computing.

3. Significance of the findings

The time to test and validate new post-quantum cryptology is now, given it takes at least ten years to build and deliver a new public key infrastructure. The pace at which quantum computing advancements can be anticipated is uncertain. The ability to transition to post-quantum cryptology appears to be very complicated, and there are many unknowns concerning establishing, standardizing and deploying post-quantum cryptography systems. All of this must be completed before the arrival of large-scale quantum computers because the cybersecurity of many vital services will be severely degraded.

4. Bitcoin and Distributed Ledger Technology

The Bitcoin Cryptocurrency (BTC) is the first widespread application of blockchain technology. The critical elements of Blockchain and DLT have been in existence for decades, and they include fault-tolerance, distributed computing, and cryptography. Succinctly, the first iteration of this technology is a decentralized distributed database that keeps records of transactions relatively secure and in an append-only mode, where all peers eventually come to a consensus regarding the state of a transaction. The Bitcoin Blockchain like others operates in an open peer-to-peer (P2P) network, where each node can function as a client and a server at the same time. The nodes in the system are connected over TCP/ IP and once a new node is connected that node broadcast peer IP addresses via Bitcoin address messages. Each address maps to a unique public and private key; these keys are used to exchange ownership of BTCs among addresses. A Bitcoin address is an identifier of 26 to 35 alphanumeric characters [5] . Since the advent of BTC along with its choice of a data structure, called a block, modified blockchain technologies, makes use of different data structures such as Directed Acyclic Graph (DAGs). Therefore, recent versions of the newest blockchains can longer accurately be called blockchains, and it is more appropriate to use the term Distributed Ledger (DL) that applies to all version of the blockchain. Presently, according to Crypto-Currency Market Capitalizations [6], there are more than 2000 alternate cryptocurrencies, and most make use of the Bitcoin Blockchain or are clones with minor differences in the private key generation cryptography and structure. The primary configuration changes include the underlying hash function, block generation times, data structures

and method of distributed consensus. However; the critical task of generating private keys in blockchains remains unchanged across most blockchain adaptions, and this work asserts that the foundation of the current cryptocurrency markets and all the private and public sectors using this technology are vulnerable to the same cybersecurity weaknesses.

5. ECDSA, libsecp256k1 and OpenSSL

The ECDSA algorithm is part of public-key cryptography and is also the cryptography the Bitcoin blockchain uses to generate the public and private keys. The ECDSA is used in critical infrastructure, secure communications over the Internet, cellular and Wi-Fi and in many blockchain forks in use today. Specifically, the Bitcoin blockchain uses the ECDSA and the Koblitz curve *secp256k1* [7] which have significant weaknesses which include general algorithm structure, side-channel attacks, and threats from quantum computers. The Koblitz Curve was not adopted for standardisation by NIST due to the non-random structure of the algorithm. The Bitcoin creator selected a non-NIST P-256 approved curve to serve as a source of entropy. Entropy is defined in this case as the randomness inserted by an operating system or application for use in cryptography that requires random data. OpenSSL is an open-source software library used in BTC technology and ECDSA applications to secure communications and many critical infrastructures. OpenSSL [8] provides software Pseudo Random Number Generator (PNRG) based on a variety and type of hardware and software sources. Its core library is written in the C programming language. The process starts once the Bitcoin Core client is installed, and the user receives a set of ECDSA key pairs, called Addresses. The PRNG starts in the state unseeded and this state; it has zero entropy. A call to RAND bytes is made, and it will transfer automatically into the state seeded with a presumed entropy of 256 bits and is feed to the PRNG through a call to RAND add. The keys generated from this process are necessary to transfer BTC from one Address to the other. Next, the client needs to sign a specific message (called Transaction) with the private key of the user. The public key is used to check if the given user has rights to BTC [9].

The ECDSA algorithm relies 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.

The Koblitz curve secp256k1 is non-verifiably random and is defined by Standards for Efficient Cryptography Group (SECG), instead of the NIST 186-3 DSS Standard using the elliptic curve secp256r1. The security of the ECDSA algorithm and protocols relies on a source of distributed random bits.

6. Fault Attack on Bitcoin's Elliptic Curve with Montgomery Ladder Implementation.

This Montgomery Ladder Fault Attack method is a fault attack on elliptic curve scalar product algorithms and can be used when the (y-coordinate) is not used. The bit security of the elliptic curve parameters in most cases can be significantly reduced. The Fault attack is a robust side-channel technique that is used to break ECDSA cryptographic schemes. The idea is to inject a fault during the computations of implementation and to use the faulty outputs to deduce information on the secret key stored in the secure component [10]. Table 1 gives the resultant bit security after the Montgomery Ladder Fault Attack.

Table 1: Curve parameter security according to Montgomery Ladder Fault Attack [10]

Values *secp*	P1363 IPSEC	X9.62 X9.63	NIST	Strength	Security
256k1	c/c	c/r		128	**50**
256r1	c/c	r/r	r	128	121

The bold font indicates the scep256k1 security is below 2^{60} since these computations can be easily performed with classical computers. The mention 'r' denotes parameters explicitly recommended in the standard, while the mention 'c' denotes parameters in conformance with the standard. The column "Strength" refers to the standard. Clearly, implementations without protections, the attacker can compute the discrete logarithm in the twist with a cost of 2^{50} operations and retrieve the secret scalar for n = 256.

7. Algorithm Security Strength

Breaking a cryptographic algorithm can be defined as defeating some aspect of the protection that the algorithm is intended to provide. For example, a block cipher encryption algorithm that is used to protect the confidentiality of data is broken if, with an acceptable amount of work, it is possible to determine the value of its key or to recover the plaintext from the ciphertext without knowledge of the key.

The approved security strengths for 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. NIST Special Publication 800-57 Part 1 Revision 4: Recommended for Key Management as shown in Table 2 [11]. The Fault Attack on Bitcoin's Elliptic Curve with Montgomery Ladder Implementation yields security strength of only 50 bits as shown in Table 1.

8. NIST and Post-Quantum Cryptography

In December 2016, NIST formally announced its Call for Proposals (Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms), [12]. This call solicited proposals for post-quantum

Table 2: Comparison of conventional and quantum security levels of typical ciphers [12].

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

digital signature as well as public-key encryption and Key Encapsulation Mechanism (KEM)/Encryption for evaluation. In response, there were 82 total submissions, and 69 were accepted, and five withdrew. The results and categories included 19 Signatures and 45 KEM Encryption. The Signature category which produces private keys included five Lattice-based submissions, and this work focuses on qTESLA's submission which is based on the verifiable hardness of the decisional Ring Learning With Errors (R-LWE) problem [4]. Public Key Systems based on R-LWE is computationally superior over LWE systems because of reduced overhead, greater capacity for message space and smaller public key sizes.

9. Selected algorithm for test and evaluation: qTESLA

The author's considerations for the selection qTESLA, are "reasonable" key and ciphertext sizes, and to a lesser extent the number of CPU cycles required for encryption, decryption, and verification, and potential incorporation into constrained devices such as smartphones and emerging IoT devices. Additional considerations included trust, metrics, parameters, migration, compatibility, and efficient and secure implementation. This submission utilizes two approaches for parameter generation. The first approach is called "heuristic qTESLA," and it uses heuristic method parameter generation and the second approach is called "provably-secure qTESLA," and its parameter generation is provably-secure. qTESLA includes five parameter sets that correspond to two security levels located in Table 3.

Table 3: Adapted from The NIST Post-Quantum Crypto "Competition" [13].

Values *secp*	P1363 IPSEC	X9.62 X9.63	NIST	Strength	Security
256k1	c/c	c/r		128	**50**
256r1	c/c	r/r	r	128	121

Security levels:

A. Heuristic qTESLA:

- qTESLA-I: NIST"s security category 1.
- qTESLA-III-speed: NIST"s security level 3 (option for speed).
- qTESLA-III-size: NIST"s security level 3 (option for size).

B. Provably-secure qTESLA:

- qTESLA-p-I: NIST"s security category 1.
- qTESLA-p-III: NIST"s security category 3 [4].

The security of lattice-based systems is provably secure under worst-case hardness assumptions. In the author's view, it is not likely that current PQC will be direct replacements for current standards and will likely impact the entire category of Internet protocols, such as Transport Layer Security (TLS) and Internet Key Exchange (IKE).

System parameters can be viewed in Table 4 and Table 5 on the page number 17.

10. Informal 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, and d be system parameters that denote the modulus, the bound constant for error polynomials, the bound constant for the secret polynomial, 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 is w well-rounded if w is $([q/2] - L_E)$-short and [w]L is $(2^{d-1} - L_E)$-short, where $[w]_L$ denotes the unique integer in $(-2^{d-1}, 2^{d-1}] \subset Z$ such that $w = [w]_L$ modulo 2^d. Also, $[w]_M$ is the value represented by all but the d least significant bits of $(w - [w]_L)$. Let $R = Z[x]/(x^n + 1)$ and $R_q = Z_q[x]/(x^n + 1)$. The hash oracle H() maps from {0, 1}* to H, where H denotes the set of polynomials $c \in R$ with coefficients in {-1, 0, 1} with exactly h nonzero entries.

Algorithm 1: Informal description of the key generation.

Require - , n/a

Ensure: Secret key sk = (s; e_1, …., e_k, a_1, …, a_k), and public key pk = (a1, …, ak, t1, … tk)

1. $a_1, \ldots, a_k \leftarrow R_q$ invertible ring elements.
2. Choose $s \in R$ with entries from D σ. Repeat step if the h largest entries of s sum to L_S.
3. For i = 1, …, *k*: Choose $e_i \in R$ with entries from D σ. Repeat step at iteration *i* if the h
4. largest entries of e_i sum to L_E.

Table 4: Description and bounds of all the system parameters [4]

Parameter	Description	Requirement
λ	security parameter	-
q_h, q_s	number of hash and sign queries	-
n	dimension (n – 1 is the poly. degree)	power of two
σ, ξ	standard deviation of centered discrete Gaussian distribution	$\sigma = \xi/\sqrt{2\ln 2}$
k	#R-LWE samples	-
q	modulus	$q = 1 \mod 2n$, $q > 4B$ For provably secure parameters $q^{nk} \geq \lvert\Delta S\rvert \cdot \lvert\Delta L\rvert \cdot \lvert\Delta H\rvert$ $q^{nk} \geq 2^{4\lambda+nkd}\, 4q_s^3\, (q_s + q_h)^2$
h	# of nonzero entries of output elements of Enc	$2^h \cdot \binom{n}{h} \geq 2^{2\lambda}$
L_E, η_E L_S, η_S	bound in checkE bound in checkS	$\eta_E \cdot h \cdot \sigma$ $\eta_S \cdot h \cdot \sigma$
B	interval of randomness is chosen during signing	$B \geq \frac{k \cdot n\sqrt{M} + 2L_{S-1}}{2\left(-1-kn\sqrt{M}\right)}$, near a power of two
d	number of rounded bits	$\left(i - \frac{2L_E+1}{8^d}\right)^{kn} \geq 0.3$, $d > \log_2(B)$
b_{GenA}	number of blocks requested to SHAKE128 for GenA	$b_{\text{GenA}}\, \varepsilon\mathbb{Z} > 0$
$\lvert\Delta H\rvert$ $\lvert\Delta S\rvert$ $\lvert\Delta L\rvert$		$\sum_{j=0}^{h} \sum_{i=0}^{h-j} \frac{\binom{k}{2}\binom{n}{i}^{2^{2i}} (k^n - 2i)^{2j}}{(4(-B-L_s)+1)^n (2^d+1)^{nk}}$
δz δw δ_{keygen}	acceptance probability of z acceptance probability of w acceptance probability of key pairs	experimentally experimentally experimentally
sig size pk size sk size	theoretical size of signature theoretical size of public key theoretical size of secret key	experimentally experimentally experimentally
$\varkappa$	output length of hash function H and input length of GenA, PRF_1, PRF_2, Enc and ySampler	$\varkappa \geq \lambda$

Table 5: Parameters for each of the proposed heuristic and provably-secure parameter sets with qh = 2128 and qs = 264; M = 0.3 [4]

Parameter	qTESLA-I	qTESLA-III-speed	qTESLA-III-size	qTESLA-p-I	qTESLA-p-III
λ	95	160	160	95	160
$\varkappa$	256	256	256	256	256
n	512	1024	1024	1024	1024
σ, ξ	23.78, 27.9988	10.2, 12	8.49, 9.9962	8.5, 10	8.5, 10
k	1	1	1	4	5
q	4205569 $\approx 2^{22}$	8404993 $\approx 2^{22}$	4206593 $\approx 2^{22}$	485978113 $\approx 2^{29}$	1129725953 $\approx 2^{30}$
h	30	48	48	25	40
L_E, η_E	1586, 2.223	1147, 2.34	910, 2.23	554, 2.61	901, 2.65
L_S, η_S	1586, 2.223	1233, 2.52	910, 2.23	554, 2.61	901, 2.65
B	2^{20} -1	$2^{21} - 1$	2^{20} - 1	$2^{21} - 1$	2^{23} - 1
d	21	22	21	22	24
b_{GenA}	19	38	38	108	180
$\lvert\Delta H\rvert$ $\lvert\Delta S\rvert$ $\lvert\Delta L\rvert$				$\approx 2^{435.8}$ $\approx 2^{23551.6}$ $\approx 2^{94208.0}$	$\approx 2^{750.9}$ $\approx 2^{51199.7}$ $\approx 2^{2560000}$
δ_w	0.31	0.38	0.25	0.33	0.34
δz	0.44	0.56	0.37	0.78	0.81
δ_{sign}	0.14	0.21	0.09	0.26	0.28
δ_{keygen}	0.45	0.60	0.39	0.59	0.44
sig size	1376	2848	2720	2848	6176
pk size	1504	3104	2976	14880	39712
sk size	1216	2112	2112	4576	12320
classical bit hardness	104	178	188	132	247
quantum bit hardness	97	164	169	123	270

5. For $i = 1, \ldots, k$: Compute $t_i = a_i s + e_i \in R_q$.
6. Return sk = (s; e1, … ek; a1, … ak) and pk = (a1, … ak, t1, …, tk).

Algorithm 2: Informal description of the signature generation.

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

Ensure: Signature (z; c)

1. Choose y uniformly at random among B-short polynomials in R_q.
2. $c \leftarrow H([a_1 y]_M, ..., [a_k y]_M, m)$.
3. Compute $z \leftarrow y + sc$.
4. If z is not $(B - L_s)$-short then retry at step 1.
5. For $i = 1, ..., k$: If $a_i y - e_i c$ is not well-rounded then retry at step 1.
6. 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

1. If z is not (B - LS)-short then return reject.
2. For i = 1, …, k: Compute wi ← aiz - tic ∈ Rq.
3. If c ≠ H([w1]M, …, [wk]M, m) then return reject.
4. Return accept [4].

Performance of post-quantum qTESLA algorithms analysis

To evaluate the performance of the provided implementations written in portable C, the author ran benchmarking suite on three machines powered by: (i) an Intel® Core™ i7-6500 CPU @ 2.50 GHz x 4 (Skylake) processor (see table 4) (ii) an Intel® Core™ i5-6400T CPU @ 2.20GHz (VMWARE)(Haswell) processor (see table 5) (iii) an Intel® Core™ i7-2630QM CPU @ 2.00GHz × 8 (Haswell) (see table 6) all running Ubuntu 18.04.1 LTS. For compilation, GCC version 7.3.0 was used in all test.

11. Analysis

The author argued that the uncertainties had not been appropriately addressed. For example, there is the possibility that additional quantum algorithms or techniques will be developed, which will lead to new and unanticipated attacks. Also, it is difficult to calculate the impact of those programs that are highly classified, and its performance characteristic is not public. Rapid and unpredictable advancements in quantum computing, are endangering or making current encryption schemes obsolete. It has been established that the most significant threat posed by quantum computers is directed towards current RSA, ECC digital signature scheme systems on which Bitcoin, Distributed Ledger and much of Internet-based technology uses.

It has been settled that the current RSA and ECC based public key cryptography are broken, and the AES cryptography is adversely reduced in bit security by quantum computing era. It is the author's view that recommendations such as doubling the AES key size need to be examined while considering the constraints of present systems. Current AES-128 is reduced to 64-bit security, and AES-256 would have 128-bit security.

An example of the impact of doubling the key size for AES-256 to AES-512 is not well documented and verified. This alternative algorithm (AES-512) would most likely use input block size and a key size of 512-bits. An increasing number of rounds and key schedule would adversely impact performance constraints, especially for constrained devices. The higher the key size, the more secure the ciphered data, but also the more rounds needed. In the hardware perspective, a bigger key size also means a larger area and power consumption due to more operations that need to be done. More focus and examination need to be done for AES in the PQC era, especially for constrained devices.

The author specifically, examined the ECDSA that are in use in Bitcoin and Distributed Ledger technologies. Secondly, evaluated NIST Candidate PQC for standardisation and possible replacement in blockchain

Table 6: ECDSA; signature and key sizes are given in bytes [4].

Software/ Scheme	Computation Assumption	Bit Security	Key Size (bytes)	Signature Size (bytes)
ECDSA (P-256)	Elliptic Curve Discrete Logarithm	128	pk: 64 sk: 96	64

and other public key cryptography Internet-based technologies. Table 6 gives the ECDSA (P-256) parameters used as the benchmark for comparison regarding the number of quantum security bits, and the size of the public key, secret key and signature key as an independently controlled variable. According to NIST, the use of schemes with less than 112-bit security is deprecated and will eventually be disallowed for use by U.S. government institutions to handle sensitive data. It is noted that that speed at which the encryption and decryption occurs is also an important parameter.

Table 7: Intel® Core™ i7-6500 (Skylake) CPU @ 2.50 GHz x 4

Scheme	Keygen	Sign	Verify	Total (sign + verify) median
qTESLA-I	1321.3	402.4	82.6	485
qTESLA-III-speed	2987.6	551	168.8	719.8
qTESLA-III-size	5042.8	1035.8	170.4	1206.2
qTESLA-p-I	5370.1	1033.2	423.4	1456.6
qTESLA-p-III	25791.8	4223.2	2134	6357.2
Scheme	**Keygen**	**Sign**	**Verify**	**Total (sign + verify) average**
qTESLA-I	1501.7	557.3	87.1	644.4
qTESLA-III-speed	3349.9	747.2	172.9	920.1
qTESLA-III-size	5329.7	1448.6	171.8	1620.4
qTESLA-p-I	5545.3	1328.9	428	1756.9
qTESLA-p-III	27570.3	5254.8	2156.4	7411.2

Table 9: Intel® Core™ i7-2630QM CPU @ 2.00GHz × 8

Scheme	Keygen	Sign	Verify	Total (sign + verify) median
qTESLA-I	1729.3	494	105.7	599.7
qTESLA-III-speed	3900.5	708.6	223.2	931.8
qTESLA-III-size	6047	1350.2	220.5	1570.7
qTESLA-p-I	6987.2	1328.2	563.8	1892
qTESLA-p-III	36254.2	5204.5	2858	8062.5
Scheme	**Keygen**	**Sign**	**Verify**	**Total (sign + verify) average**
qTESLA-I	1972	672	108	780
qTESLA-III-speed	4367.9	929	224.4	1153.4
qTESLA-III-size	6994.3	1858.8	225.2	2084
qTESLA-p-I	7343	1683	5689	2252
qTESLA-p-III	3739	6430	2882	9312

The following results cannot be compared directly with the vendor qTESLA's submitted results, but; specific observations can be made with alternative applications and platforms. It is the author's view that if the key sizes are not manageable and practical for use in conventional and constrained devices, then the time or speed becomes less critical metric compared to key size.

Table 7, Table 8 and Table 9 gives the results of the independent tests on respective platforms and performance is measured (in thousands of cycles) of the reference implementation. Results for the median and average (in the first and second table respectively) are rounded to the nearest 103 cycles. Signing is performed on a message of 59 bytes.

12. Recommendations

The PQC Standardisation process is complex, arduous and requires coordinated involvement (academia, private and public sector) and requires significant IV&V before formalization. Successful PQC must be resistant to both classical and quantum attacks. Multiple tradeoffs will have to be considered such as security, performance, key size, signature size, and side-channel resistance countermeasures. Other important considerations are the capability to migrate into new and existing applications such as TLS, IKE, code signing, PKI infrastructure.

It is necessary to begin a coordinated international campaign to mitigate the uncertainties of breakthroughs and the unknowns regarding classified programs. The aim should include, information sharing between the academic, public and private sector toward the common goal.

It is critical to devise and initiate the incorporation of cutting edge yet practical PQC to prevent a disastrous impact on global privacy, security and economy before the arrival of large-scale fault-tolerant quantum computing.

13. Conclusion

qTESLA's submission for NIST Security Categories I and III as tested on platforms described in this work are more than two orders of magnitude larger for the public-key for qTESLA-p-1 (128-bit security) and qTESLA-p-III (192-bit security). The qTESLA-p-1 secret key is 56 times the size of ECDSA's secret key and qTESLA-p-III is two orders of magnitude larger.

It is essential to come to a consensus on how to assess quantum security. Currently, there is not a clear agreement on the best way to measure quantum attacks. It is, nevertheless, fundamental that work continues with alternatives that will produce smaller key sizes, comparable to the current ECDSA algorithms. The major drawback with qTESLA is the large key sizes which make it unlikely to be accepted in its current configuration. However, there is ongoing research being done to make it potentially a more viable candidate, both by reducing the key sizes and providing more efficient implementations (see tables 7, 8, 10).

The qTESLA's "Heuristic" submission for NIST Security Categories I and III are qTESLA-I, qTESLA-III-space, and qTESLA-III-size. The vendor claims that their heuristic approach is the security level of an instantiation of a scheme by the hardness level of the instance of the underlying lattice problem. Also, the claim is that it corresponds to these parameters regardless of the tightness gap of the provided security reduction if the corresponding R-LWE instance is intractable.

These claims and the necessary proof are beyond the scope of this work and cannot be independently verified and validated and is not the author's aim. It is important to note that; the results of qTESLA's heuristic algorithm were captured and are analyzed against its provably secure submissions. The heuristic algorithms were tested on the same platforms identified in the provably secure submission. qTESLA-I's public-key size vs. qTESLA-p-1's public-key size is a reduction of 90%. The secret key size at the same bit security level is reduced by 60%, and the signature size is reduced by 52%. Observations for public keys; qTESLA-III-size vs. qTESLA-p-III is reduced by 92%; secret key size reduction is 66%; signature size reduction is 56% (see Table 10).

The difference in the heuristic key sizes are dramatically reduced and compares more favorably to ECDSA (P-256) parameters. While the heuristic values are dramatically reduced compared to the provably secure values, the key sizes are still large compared to current standard ECDSA (P-256) sizes. For example; the best result for the secret key size for qTESLA-III-size (4160) vs. ECDSA (P-256) secret key size (96) is a 4233% increase and would prove problematic in

existing systems.

Table 10: qTESLA Public-Key, Secret key, and Signature Size

Scheme (Bytes)	Public-key	Secret key	Signature Size
qTESLA-I	1504	2112	1376
qTESLA-III-speed	3104	4160	2848
qTESLA-III-size	2976	4160	2720
qTESLA-p-I	14880	5184	2848
qTESLA-p-III	39712	12352	6176

14. Future Work

The author selected qTESLA's submission which is 1 of 5 NIST Candidate PQC digital signature schemes. Additional work needs to be done in verifying and validating and testing vendors results. Concrete PQC parameters for testing and validation need to be created for the promotion of a baseline. The parameters should be modified to determine the best tradeoffs while maintaining required security. Moreover, the organization of guidelines and standards are necessary for the wider cryptography community to aid in PQC standardisation create efficient, high-quality implementations.

Continued measurements of current PQC scheme implementations should be performed, such as performance and memory usage on the ARM and CMOS platforms. Many embedded devices have ARM and CMOS architecture and have limited computational and memory resources. NIST currently plans a Post-Quantum Cryptography Round 2 call tentatively schedule in 2019 and will offer additional opportunities for IV&V and research.

References

[1] S. . M, A. H. D, M. . M, P. . P and S. . Balaji, "Decentralized digital voting application," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, no. 3, pp. 1725-1728, 2018

[2] E. . Feig, "A Framework for Blockchain-Based Applications.," , 2018. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1803.html. [Accessed 7 1 2019]

[3] D. Moody, L. Feldman and G. Witte, "Securing Tomorrow's Information Through Post-Quantum Cryptography", Csrc.nist.gov, 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/itl-bulletin/2018/02/securing-information-through-post-quantum-cryptography/final. [Accessed 7 1 2019].

[4] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, and F. Pawlega, "Revisiting TESLA in the Quantum Random Oracle Model," Post-Quantum Cryptography Lecture Notes in Computer Science, pp. 143–162, 2017. [Accessed 7 1 2019].

[5] G. O. Karame, "On the Security and Scalability of Bitcoin's Blockchain," , 2016. [Online]. Available: https://dl.acm.org/citation.cfm?id=2976756. [Accessed 7 1 2019].

[6] "Cryptocurrency Market Capitalizations," , . [Online]. Available: https://coinmarketcap.com/currencies/bitcoin-cash/. [Accessed 8 1 2019].

[7] N. T. Courtois, G. . Song and R. . Castellucci, "Speed Optimizations in Bitcoin Key Recovery Attacks," Tatra mountains mathematical publications, vol. 67, no. 1, p. 103, 2016.

[8] J. Ooms, "Toolkit for Encryption, Signatures and Certificates Based onOpenSSL," , 2016. [Online]. Available: https://cran.r-project.org/web/packages/openssl/index.html. [Accessed 7 1 2019].

[9] J. A. Dev, "Bitcoin mining acceleration and performance quantification," , 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6900989. [Accessed 30 12 2018]

[10] P.-A. R. L. D. R. F. V. Fouque, "Fault Attack on Elliptic Curve with Montgomery Ladder Implementation," 2008

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

[12] 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].

[13] D. Moody, "The NIST Post-Quantum Crypto "Competition" "The Ship Has Sailed"," in Asiacrypt 2017, Hong Kong, 2017.

Photo by Hieu Vu Minh on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

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

Valuation Method of Equity-based Security Token Offerings (STO) for Start-Up Companies

Jay Pazos
University of Chicago Booth School of Business, USA
Correspondence: jpazos@uchicago.edu
Received: 5 October 2018 **Accepted:** 17 January 2019 **Published:** 25 January 2019

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

In this paper, we develop a novel valuation method of equity-based securities token offerings (STO) for start-up companies. The closed-form discount rate function discovered in this paper is time-dependent and piecewise. The first part of the function is exponential; the second part is a power function. The reason is that, in the early years, the probability of survival of start-up firms descends more rapidly than in late years. The probability of survival function discovered has a remarkably good fit with empirical data- for the total of firms and ten industry sectors for which data is available. For the total of firms, we found that the highest discount rate has a 27.0 to 31.8% range when the liquidation value of the non-surviving start-up project is zero; this is considerably higher than observed discount rates of projects for mature firms (7.5%) but considerably less than some published discount rates for start-up projects financed by Venture Capital firms (40.6 to 70% range). To demonstrate the model, we work a valuation example in section six. A valuation method for equity STOs will help to develop a more transparent market for start-ups wanting to raise capital. Most importantly, our results show that for many start-up firms, equity STOs could be an economical alternative to raise capital.

Keywords: *discount rate, Valuation, startup, security token, security token offering, STO, Venture Capital*
JEL Classifications: *D02, D71, H11, P16, P48, P50*

1. Introduction

An equity token is a new security class, initially created with the purpose of providing early access to capital for start-ups and growth companies. Equity tokens are digital representations of company shares, and their holders are collectively the owners of the company. By definition, equity STOs are classified as securities in most jurisdictions; this certainty of classification is good for all stakeholders. One fundamental characteristic of equity tokens is that they live in a blockchain, and because of that, equity STOs trade in exchanges with blockchain facilities located in jurisdictions that permit their existence and trading.

For the valuation of companies, the DCF method is many times preferred to others because it enables the understanding of the dynamics of the business at a level of detail not present in other techniques. For the valuation of equity STOs of start-up firms using the DCF method, we need to build a framework that calculates the discount rate and forecasts the cash flows. Before we forecast cash flows, we need to dimension the opportunity facing the firm: first considering the broadest market measure: the Total Addressable Market (TAM), from there we narrow it down to the Serviceable Available Market (SAM) and finally to the Serviceable Obtainable Market, the market that the start-up can realistically address. Later by taking into account variables such as the growth of SOM, the price and price growth of the provided good and the sales growth curve profile, we can develop a forecast. A good forecast doesn't pose any theoretical difficulty in its method, and it is of paramount importance for quality valuations. The main obstacle to build a framework for valuing start-ups using the DCF method is to calculate the project's discount rate. In the corpus of financial theory, there is no explicit formula, that we are aware of, to calculate the discount rate for start-ups, we will dwell into this issue in section 2.

In sections 3 and 4, we will go to great lengths to develop a discount rate formula for start-up firms. In section 5, we will explain our views regarding how cash

flows should be calculated to arrive at the valuation of the firm. In section 6 we go through a worked example.

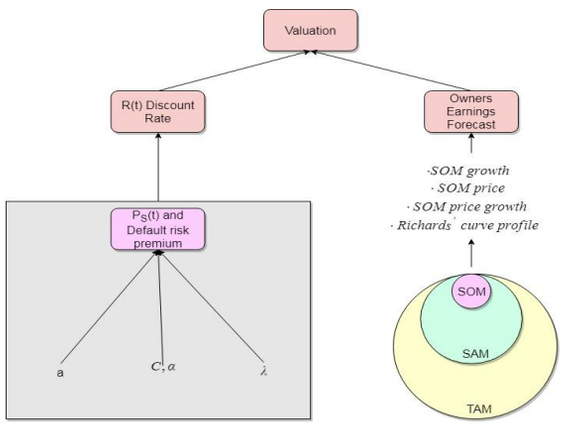


Figure 1: Map of valuation model.

2. Discount Rates Variations for Start-ups

The long-standing issue about variations in discount rates was well captured by John H. Cochrane [1] in his August 2011 Presidential Address to the American Finance Association, he stated in his conclusion:

"Discount rates vary a lot more than we thought. Most of the puzzles and anomalies that we face amount to discount-rate variations we do not understand. Our theoretical controversies are about how discount rates are formed. We need to recognize and incorporate discount-rate variation in applied procedures. We are only beginning these tasks. The facts about discount-rate variation need at least a dramatic consolidation. Theories are in their infancy."

The fact that venture capitalists use high discount rates was addressed by Sanjai Bhagat [2] in 2014. In Bhagat's paper summary, he explained:

"Venture capitalists typically use discount rates that are high compared to historical rates of return on common stock and other financial assets. Such high discount rates also cannot be explained in the context of any existing asset pricing theory"
In another study, Aswath Damodaran [3] mentions in a 2009 paper that Venture Capital firms have typical target rates of return of 50-70% for start-ups and suggests that these target rates must have incorporated some survival risks, Damodoran says:

"How do we know that these rates of return have survival risks built into them? In addition to the intuitive rationale that they decrease as firms move through the life cycle and the chance of failure drops, the actual returns by the venture capitalists at every stage of the process are much more modest..."

Although Damodaran's doesn't offer any formula to quantify his intuition, we believe that he steers in the right direction. The probability of survival is a determinant of the formula of discount rates for start-ups as it will be shown in the next sections.
In this paper, we pose the hypothesis that we have found a novel closed-form expression of the discount rate to value start-up companies. In a quest to falsify our hypothesis, we have made extensive use of Google Scholar to search in past literature for any previous formula that calculates the discount rate for start-ups, and we have found none. This doesn't mean that our hypothesis is correct, it only means that, until today, we have not been able to falsify our hypothesis. However, others may in the future.

3. Using historical data to determine the probability of survival function

Our objective in this section is to look at historical data and determine if we can find a probability of survival function that describes well the empirical data.

In this manuscript, we use empirical data from the Knaup and Piazza [4] (K&P) study that presented data over a 7-year period. The K&P study examined a cohort of establishments from the Bureau of Labor Statistics (BLS) Quarterly Census of Employment and Wages (QCEW) program.

We believe that the (K&P) study data is an excellent starting point to determine the probability survival function, some important characteristics of the study data are related to the comprehensiveness of the QCEW program. As presented in the K&P study, they are as follows:

- At the time the K&P study was performed, the QCEW program contained information on 8.9 million U.S. business establishments in both the public and private sector
- The monthly business establishment data is compiled on a quarterly basis for State unemployment insurance tax purposes and are edited and submitted to the BLS.
- The QCEW program collects information covering approximately 98 percent of non-farm payroll employment in the United States.
- The data generated by the QCEW program serve as the sampling frame for a range of BLS establishment surveys and as a benchmark for the Current Employment Statistics survey
- Outside researchers use QCEW microdata to investigate topics in the field of labor economics, and such data are the largest single input to the Bureau of Economic Analysis personal income accounting program. QCEW program data also are used to generate gross job flows in the Business Employment Dynamics (BED) data series.

- The QCEW program has linked data from the first quarter of 1990 through the most current quarter; the data usually are available seven months after the end of the reference quarter. The coverage and frequency of the data are unique in the Federal statistical systemin that they allow the tracking of the start-up, growth, and failure of a particular establishment concurrently with the timing of those events.

The (K&P) study follows a selected cohort of establishments from birth through 28 quarters of their lifetime, from March 1998 to March 2005, creating the basis for the 7-year survival study. The cohort data for the companies studied is in our opinion robust, and as presented in the K&P study, it has the following characteristics:

- Company births are defined as those establishments which are new in the reference quarter and show no positive employment for the previous four quarters
- Each microdata record is tested for four quarters before the reference quarter, to prevent seasonal establishments from appearing in the birth cohort.
- New establishments have no ties to any establishments that existed before the reference quarter. This approach eliminates changes in ownership from the cohort, as well as new locations of existing firms, which might be expected to behave differently from independent establishments.
- Another reason for not including new locations of existing firms is that they often represent administrative changes in the data rather than actual new locations. To include them would have risked skewing the data in terms of both survival analysis and average employment.
- The study tracked the original 212,182 new establishments across the US for the second quarter of 1998 (beginning in March of that year). The cohort accounts for approximately all births during that quarter, a typical quarter from 1992 to the end of the series.
- In the birth quarter, establishments are equivalent to firms. In subsequent quarters, establishments may be acquired by or merged with another firm, spin off a subsidiary, or open additional locations.
- Establishments that were involved in such succession relationships also were tracked across time, by following the successor establishments. Data on these successors were aggregated and assigned a unique identifier that was linked to the original birth establishment.

The resulting survival rates from the K&P study are summarized in Table 1.

One salient point present in each of the industry sector series is that the survival rates descend at a decreasing rate. The descent is high in the early years and low in the later years. In this paper, we propose the hypothesis that there is an exponential function relationship in the early years and a power function relationship in the late years. The reason for this is to accommodate for the difference in descent rates between early and late years. First, we need some definitions:

- Let $P_s(t)$ be the probability of survival of the firm at time = t;
- Let $P_s(0)$ be the probability of survival of the firm at time = 0;
- Let t be the number of years from the date of incorporation of the firm;
- Let C and α be some constants in the power function;
- Let λ be some constant in the exponential function;

Table 1: Survival rates from the year of incorporation- US companies 1998-2005 period.
(Source: Knaup & Piazza [4] and Aswath Damodaran [5])

Survival Rates from year of Incorporation

Industry sector	Incorporation	year 1	year 2	year 3	year 4	year 5	year 6	year 7
Natural Resources and Mining	100%	82.33%	69.54%	59.41%	49.56%	43.43%	39.96%	36.68%
Construction	100%	80.69%	65.73%	53.56%	42.59%	36.96%	33.36%	29.96%
Manufacturing	100%	84.19%	68.67%	56.98%	47.41%	40.88%	37.03%	33.91%
Trade, Transportation and Utilities	100%	82.58%	66.82%	54.70%	44.68%	38.21%	34.12%	31.02%
Information	100%	80.75%	62.85%	49.49%	37.70%	31.24%	28.29%	24.78%
Financial Activities	100%	84.09%	69.57%	58.56%	49.24%	43.93%	40.34%	36.90%
Professional and Business Services	100%	82.32%	66.82%	55.13%	44.28%	38.11%	34.46%	31.08%
Education and Health Services	100%	85.59%	72.83%	63.73%	55.37%	50.09%	46.47%	43.71%
Leisure and Hospitality	100%	81.15%	64.99%	53.61%	43.76%	38.11%	34.54%	31.40%
Other Services	100%	80.72%	64.81%	53.32%	43.88%	37.05%	32.33%	28.77%
Total for all firms	**100%**	**81.24%**	**65.77%**	**54.29%**	**44.36%**	**38.29%**	**34.44%**	**31.18%**

- Let a be the transition point in time when the probability of survival function $P_s(t)$ changes from exponential to power characteristics.

The proposed exponential equation for the early years has the form: $P_s(t)=P_s(0)\cdot e^{-\lambda\cdot t}$ and the proposed power function for the late years has the form: $P_s(t)=C\cdot t^{-\alpha}$. The piecewise function expressing the probability of survival looks as follows:

$$P_s(t)=\begin{cases} P_s(0)\cdot e^{-\lambda\cdot t} & \text{if } t\le a \\ C\cdot t^{-\alpha} & \text{if } t>a \end{cases}$$

We know that at the time of incorporation of the firm, the probability of survival is exactly 1.00, that is: $P_s(0)=1.00$; Hence:

$$P_s(t)=\begin{cases} e^{-\lambda\cdot t} & \text{if } t\le a \\ C\cdot t^{-\alpha} & \text{if } t>a \end{cases} \quad (1)$$

We need to find the values of parameters λ, C and α in equation (1); let us consider the first part of equation (1): $P_s(t)=e^{-\lambda\cdot t}$ if $t \le a$. If we know one point in the function, at $t = a$, that is, point: $(a, P_s(a))$. Then it is trivial to derive λ:

$$\lambda=-\frac{ln(P_s(a))}{a} \quad (2)$$

now, let us consider the second part of the equation (1): $P_s(t)=C\cdot t^{-\alpha}$ if $t > a$. Also, if we know two points in this function, at $t = a$ and $t = b$, that is, points: $(a, P_s(a))$ and $(b, P_s(b))$, it is trivial to derive C and α:

$$C=P_s(a)\cdot a^{\alpha} \quad (3)$$

and

$$\alpha=\frac{ln(\frac{P_s(a)}{P_s(b)})}{ln(\frac{b}{a})} \quad (4)$$

With the available information in Table 1, together with equations (2), (3) and (4) above and taking 3 points in each curve when t = 0, t = a, and t = 7 we can find the values for the parameters λ, C, and α for each industry sector and the total of all firms. The only question that remains is which value for variable a, the transition year, we should consider.

If we assume variable a is an integer; we only need to try 6 cases for a: from $a = 1$ to $a = 6$ years and observe which case offers the smoothest transition from exponential to a power function.

We did that and found that we obtain the smoothest curves when the transition point is at $t = a = 3$. The calculated results for the parameters are presented in Table 2[i].

For the *Total of All Firms* case, substituting parameters a, C, α and λ in equation (1), the probability of survival function looks as follows:

$$P_{s-total}(t)=\begin{cases} e^{-0.2036\cdot t} & \text{if } t\le 3 \\ 1.1141\cdot t^{-0.6544} & \text{if } t>3 \end{cases} \quad (5)$$

In Figure 2 we plot equation (5), the black dots are the results of using the empirical data from Knaup and Piazza [4] study in Table 1 where time t (Years form incorporation) is in the range $0 \le t \le 7$ for *Total for All Firms*. We get that for time $t \le 3$ years the blue line represents the first part (exponential function) in equation (5), and for time $t > 3$ years, the red line represents the second part (power function) in equation (5). We can observe the quality of the fit and the appropriateness of using a piecewise function with a transition point at t=3. Fitting the empirical data with an exponential or a power function alone would not have been as good.

In Figures 4 and 5 of the Appendix, we can confirm the appropriateness of piecewise function (1) to fit the

Table 2: Parameters that define exponential and power functions- transition point at time t = 3

Power and Exponential Functions Parameters

Industry Sector	C	α	λ
Natural Resources and Mining	1.1103	0.5692	0.1736
Construction	1.1373	0.6854	0.2081
Manufacturing	1.167	0.6125	0.1875
Trade, Transportation and Utilities	1.1415	0.6696	0.2011
Information	1.2131	0.8162	0.2345
Financial Activities	1.0657	0.5450	0.1784
Professional and Business Services	1.1593	0.6765	0.1985
Education and Health Services	1.0391	0.4450	0.1502
Leisure and Hospitality	1.0725	0.6312	0.2078
Other Services	1.1868	0.7282	0.2096
Total for All Firms	1.1141	0.6544	0.2036

empirical results for all ten industry sectors.

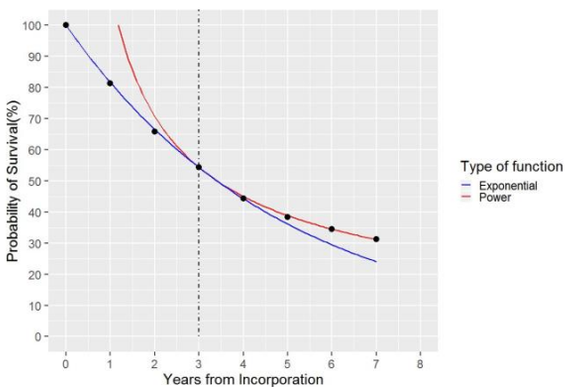


Figure 2: Probability of survival for the total for all firms-1999-2005 period

In section 4, parameters *a*, *C*, α and λ will serve us to calculate the discount rate necessary for valuation.

4. Method for Calculating the Discount Rate

First, let us consider some definitions for our model:

- Let r_f be the risk-free rate. For our long-term analysis, we use the returns earned by Treasury bonds;
- Let r_e be the equity risk premium. As expressed by equation (6) below;
- Let *D* be the default risk premium. It measures the additional return demanded by investors for compensation of the higher default rates historically experienced by start-ups.

There are different, some very elaborate, methods for calculating the equity risk premium. Since they don't add to the purpose of this paper, we will use the classic Capital Asset Pricing Model (CAPM) method as described by Sharpe [6] and Lintner [7] :

$$r_e = \widehat{r_e} = \widehat{\beta_a} \cdot (\widehat{r_m} - r_f) \quad (6)$$

Where, $\widehat{r_e}$ is the expected equity risk premium for the project, $\widehat{\beta_a}$ is the expected Beta of the project and $\widehat{r_m}$ is the expected market return.

Now, let r be the discount rate to value a mature firm's project, then:

$$r = r_f + r_e \quad (7)$$

A most relevant issue is that start-ups have a much higher probability of default than mature firms Hence, let R be the discount rate to value the start-up project that incorporates default risk premium D; the formula looks as follows:

$$R = r_f + r_e + D \quad (8)$$

and from equations (7) and (8) we get the following expression:

$$R = r + D$$

For valuation purposes, we will incorporate the default risk via two independent methods. Method 1 incorporates the default risk as an additional risk premium in the discount rate, as in equation (8); method 2 incorporates the default risk as a probability of survival. Both valuations should throw the same result.

Note that for valuation we cannot use a method that combines methods 1 and 2, that is: a method that uses R for the discount rate and incorporates the probability of survival in the calculation as this would be double counting the default risk.

Before we start describing methods 1 and 2, let us first define some variables:

- Let V be the valuation of the firm;
- Let t be the time from the date of incorporation of the firm to its exit;
- Let EV be the expected Exit Value at time=t. It can be a multiple used by industry based on expected earnings or sales or a terminal value based on future earnings. The exact definition is not important as this variable will disappear in the derivation;
- Let $P_s(t)$ be the probability of survival of the firm at time = t;
- Let LV be the liquidation value of the firm if the firm doesn't survive;
- Let r be the discount rate as calculated in equation (7). It doesn't include default risk premium D;
- Let R be the discount rate as calculated in equation (8). It includes the default risk premium D.

Method 1: One way of valuing a start-up is to forecast its sales or earnings sometime in the future, and then, by using a sales or earnings multiple for the industry sector, calculate an exit value (EV). Later, by discounting EV using R, one would obtain the start-up's valuation. This is a common method used in the Venture Capital industry. The formula would be as follows:

$$V = \frac{EV}{(1+R)^t} \quad (9)$$

Method 2: Another way of valuing a start-up would be by applying the probability of survival to the exit value EV and, then, by using r as the discount rate, one gets the start-up's valuation. The complete word equation that considers a liquidation value if the firm doesn't survive is as follows:

Valuation = Probability of survival x Discounted Exit Value using discount rate r + (1-Probability of survival) x Liquidation Value of the firm which expressed in terms of the above variables looks as follows:

$$V = P_s(t) \cdot \frac{EV}{(1+r)^t} + (1 - P_s(t)) \cdot LV \quad (10)$$

now, let F be a fraction of the liquidation value in terms of valuation V, that is: $F = \frac{LV}{V}$ then:

$$LV = F \bullet V$$

Substituting for LV in equation (10) we get:

$$V = P_s(t) \cdot \frac{EV}{(1+r)^t} + (1 - P_s(t)) \cdot F \cdot V$$

rearranging we get:

$$V - (1 - P_s(t)) \cdot F \cdot V = P_s(t) \cdot \frac{EV}{(1+r)^t}$$
$$V \cdot (1 - (1 - P_s(t)) \cdot F) = P_s(t) \cdot \frac{EV}{(1+r)^t}$$

and, thus,

$$V = \frac{P_s(t) \cdot \frac{EV}{(1+r)^t}}{1 - (1 - P_s(t)) \cdot F}$$

rearranging again, we get:

$$V = \frac{P_s(t) \cdot EV}{(1+r)^t \cdot (1 - F + F \cdot P_s(t))} \quad (12)$$

Since valuation V in equations (9) and (12) is the same, by equaling both equations we obtain the following expression:

$$\frac{\cancel{EV}}{(1+R)^t} = \frac{P_s(t) \cdot \cancel{EV}}{(1+r)^t \cdot (1 - F + F \cdot P_s(t))}$$

variable EV disappears, then, rearranging we get:

$$\frac{(1+r)^t \cdot (1 - F + F \cdot P_s(t))}{P_s(t)} = (1+R)^t$$

taking the *t(th)* root to both sides, we get:

$$1 + R = \sqrt[t]{\frac{(1+r)^t \cdot (1 - F + F \cdot P_s(t))}{P_s(t)}}$$

and, by further rearranging we get:

$$R = -1 + (1+r) \cdot \sqrt[t]{\frac{1-F}{P_s(t)} + F} \quad (13)$$

But we know from equation (1) that Ps(t) is a piecewise function. This makes, discount rate R, a piecewise function too.

Let us consider first the part when $t \leq 3$. Substituting $P_s(t)$ by $e^{-\lambda \bullet t}$ in equation (13), we get the following expression:

$$R = -1 + (1+r) \cdot \sqrt[t]{\frac{1-F}{e^{-\lambda \cdot t}} + F}$$

alternatively,

$$R = -1 + (1+r) \cdot \sqrt[t]{e^{\lambda \cdot t} \cdot (1-F) + F}$$

Now let us consider the second part when t > 3. Substituting $P_s(t)$ by $C \cdot t^{-\alpha}$ in equation (13), we get the following expression:

$$R = -1 + (1+r) \cdot \sqrt[t]{\frac{1-F}{C \cdot t^{-\alpha}} + F}$$

alternatively,

$$R = -1 + (1+r) \cdot \sqrt[t]{\frac{t^{\alpha}}{C} \cdot (1-F) + F}$$

The complete, piecewise function, for time-dependent discount rate R(t), is as follows:

$$R(t) = \begin{cases} -1 + (1+r) \cdot \sqrt[t]{e^{\lambda \cdot t} \cdot (1-F) + F} & \text{if } t \leq a \\ -1 + (1+r) \cdot \sqrt[t]{\frac{t^{\alpha}}{C} \cdot (1-F) + F} & \text{if } t > a \end{cases} \quad (14)$$

Equation (14) establishes the time dependency of the discount rate. From now onwards we will use R and R(t) indistinctly, both represent the same time dependency. From equations (7) and (8) we get the equation for the default risk premium:

$$D(t) = R(t) - r \quad (15)$$

It is interesting to observe what happens in equation (14) when F = 1, that is, when the firm doesn't survive, but the liquidation value is equal to valuation. In such case, $R(t) = r$, thus, $D = 0$. This makes sense since if the firm gets as much from liquidation as for valuation, the default risk premium should indeed be zero.

On the other hand, if the firm doesn't survive and the liquidation value is zero, that is, $F = 0$, then, we should get the highest value for R(t). We will consider next this case for the total of all firms.

We have established the transition point in time, from exponential to a power function, at year 3. Hence, $a = 3$. From table 2 we obtain the values for the parameters: $C = 1.1142$, $\alpha = 0.6544$ and $\lambda = 0.2036$. Additionally, we assume the following values:

- Start-up covers its initial financial needs by

selling equity; hence, debt is zero. Hogan and Hutson [8] found that the use of debt was rare in their study of new-technology firms. This sounds intuitively correct as start-ups have no previous record on which to base a credit application.

- Let the risk-free rate be $rf = 2.86$[ii]
- The implied equity risk premium is: $\widehat{r_m} - r_f = 4.68\%$. From Damodaran's [iii]web page Sept. 1st. 2018. The beta for the total of all firms is taken as for the market, that is 1.00. Hence, $r_e = 1.00 \bullet 4.68 = 4.68\%$ from equation (6);
- From previous items, $r = r_f + r_e = 2.86 + 4.68 = 7.54\%$;
- Let F (the fraction of Liquidation Value/ Valuation) be 0%, as we want to evaluate the highest R(t). Note that F is endogenous to the project and requires a careful analysis of the expected liquidation value of the assets for the case in which the firm doesn't survive.

From equation (14), $R(t)_{F=0}$, the R(t) function for the total of all firms when $F = 0$ is as follows:

$$R(t)_{F=0} = \begin{cases} -1 + (1 + 0.0754) \cdot e^{0.2036} & \text{if } t \leq 3 \\ -1 + (1 + 0.0754) \cdot \sqrt[t]{\frac{t^{0.6544}}{1.1142}} & \text{if } t > 3 \end{cases} \quad (16)$$

In Figure 3 we plot $R(t)_{F=0}$ and observe how $R(t)_{F=0}$ varies with time. The black dots are the results of using the empirical data from Knaup and Piazza [4] study using equation (13). The R(t) piecewise function uses the thick blue color exponential function line for the $t \leq 3$ leg and the thick red color power function curve for the $t > 3$ leg. Once again, the piecewise R(t) function seems to be the appropriate choice

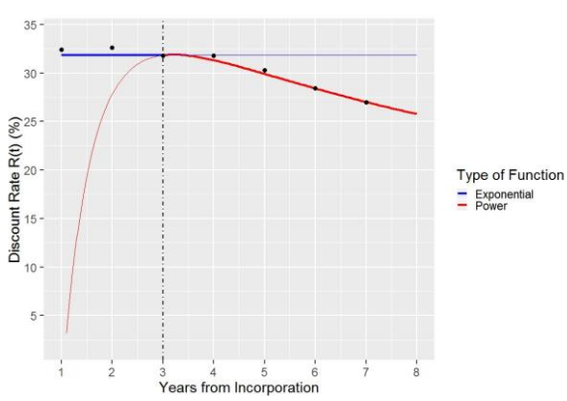


Figure 3: Plot of R(t) for Total of Firms when F=0

For years 1 to 7: $R(t)_{F=0}$ = {31.8,31.8,31.8,31.3,29.9,28 .4,27.0}

From Figure 3, we observe that for years 1 - 7, the range for the discount rate is 27.0 - 31.8% for the case of the total of firms when F = 0. This range is considerably higher than r (7.54%), the discount rate for a project in a mature firm, but much lower than the target rates applied by VC firms.

In their 1981 New England survey Wetzel [9] and Seymour reported a median compound annual rate of return demanded of 50% for start-ups by 102 individual venture investors. In 1987 Plummer [10] and Walker reported a demanded range of discount rates of 40.6 to 59.6% for start-ups by 288 venture capital firms. In their 1991 paper, Ruhnka [11] and Young reported a mean rate of return demanded of 54.8% for start-ups by 72 venture capital firms. In his 2009 paper, Damodaran [3] mentions that typical target rates of return in VC firms for start-up projects are in the 50-70% range. From these four studies, we get from VCs a demanded rate of return in the 40.6-70% range for start-ups. We believe that the difference with our maximum range of 27.0-31.8% can be attributed to at least three factors:

- Illiquidity risk premium. Venture capital firms can only exit investments at specific moments in time: IPOs, mergers and acquisitions;
- Diversification risk premium. Some VC's can only invest in one sector;
- VCs provide additional services: many VCs participate in the start-ups' company boards and offer specialized services, like: coaching, advice on managerial matters, and a Rolodex full of industry contacts. These services represent costs that need to be covered for in the discount rate.

For some start-ups, the additional services provided by VC's maybe a good reason to pay for higher discount rates; others may prefer the more economic equity STO alternative. We recommend further studies on the factors that influence the difference between the ranges.

So far, we have considered that the financing for the start-up is done exclusively by selling equity and, thus, the firm has no debt. This is a reasonable assumption since Hogan and Hutson [8] found that the use of debt was rare in their study of new-technology firms. This sounds intuitively correct as start-ups have no previous record on which to base a credit application. Nevertheless, if the start-up had debt, the calculation of the discount rate to be used for valuation poses no technical difficulties; it would be equal to the weighted average of the discount rate for the un-levered firm (as calculated using equation 14) and the cost of debt. The formula would be the same as for the standard Weighted Average Cost of Capital (WACC).

5. Cash-Flow Forecast and Valuation

There is little we can add to the theory of forecasting cash-flows; it is a pretty straightforward endeavor. On

the other hand, it is the task that should take most of the valuation time. It is essential that the evaluator finds, as precisely as possible, the size of the Serviceable Obtainable Market (SOM). The quality of valuation depends on finding a good measure of SOM. We don't think we can stress this enough.

We want to add that the market penetration of the products and services sold by the start-up firm will, most likely, evolve following a generalized logistic function curve (S-shaped curve), also known as Richards' [12] curve. If this is not the case, the developer should explain why her forecast departs from this assumption. Valuation, then, would be as follows:

$$V = \sum_{i=1}^{t} \frac{CF\ to\ firm_i}{(1+R)^i} + \frac{T}{(1+R)^t} \qquad (17)$$

where the terminal value T is evaluated as follows:

$$T = \frac{CF\ to\ firm_{t+1}}{R-g} \qquad (18)$$

some definitions are as follows:

- *CF* to $firm_i$ is the cash flow to the firm in year i;
- t is the time horizon for which the firm is going to be evaluated
- R is the discount rate R(t) as defined by equation (14) and evaluated at year t for the corresponding industry sector
- *CF* to $firm_{t+1}$ is the estimated cash flow to the firm in year t+1;
- g is the stable growth rate for *CF to Firm* from year t+1 onwards.

Substituting equation (18) into (17) we get the following valuation formula:

$$V = \sum_{i=1}^{t} \frac{CF\ to\ firm_i}{(1+R)^i} + \frac{CF\ to\ firm_{t+1}}{(1+R)^t \cdot (R-g)} \qquad (19)$$

We will use equation (19) for our worked example.

6. A worked example:

Isabel and Claire (I&C) are two young and able entrepreneurs co-founders of InsuBlock, a Blockchain life insurance company, their application is based on the Ethereum smart contracts platform. I&C have protected the intellectual property of their invention with four key patents, so they expect to start sales with a sustainable competitive advantage. I&C have a working prototype on their website, and their products are all internet based. The series of Cash Flows to firm forecast (in Millions of US dollars) for the next eight years is as follows:

CF to Firm = {0.5, 5.7, 8.8, 12.9, 18.7, 26.0, 34.3, 36.2} for years 1 to 8.

After year 8, the company is expected to continue with a steady CF to Firm annual growth of 3.5%. Insublock is considered a firm in the Financial Activities industry sector, and if the firm doesn't survive, it is believed that 10% of the initial valuation can be salvaged by selling its four patents. The company has no debt and wants to raise capital in an equity STO. The outstanding number of shares is 10 million.

Now, let's look at the value of the parameters and variables for valuation:

- We consider InsuBlock in the Financial Activities industry sector, hence, from table 2: $C = 1.0657$, $\alpha = 0.5450$, and $\lambda = 0.1784$
- t=7 since the 8th year cash flow to the firm is used to calculate the terminal value;
- F= 0.10;
- g = 0.035;
- r_f =2.85% [iv]
- Implied equity risk premium, $\widehat{r_m} - r_f = 4.68\%$ and the unlevered beta, $\widehat{\beta_a}$, for the life insurance sector is 0.81, this is from Aswath Damodaran's[v] web page Sept. 1st. 2018. Hence, re = 0.81 • 4.68 = 3.79% from equation (6)
- $r = r_f + r_e = 2.85 + 3.79 = 6.64\%$

Since $t > 3$, we will use the second part of the R(t) function in equation (14). The discount rate is as follows:

$$R(7) = -1 + (1 + 0.0664) \cdot \sqrt[7]{\frac{7^{0.5450} \cdot (1-0.1)}{1.0657} + 0.1}$$
$$= 21.82\%$$

We can now calculate the valuation of the company using equation (19)

Valuation=

$$\frac{0.5}{(1+0.2182)^1} + \frac{5.7}{(1+0.2182)^2} + \frac{8.8}{(1+0.2182)^3} + \frac{12.9}{(1+0.2182)^4} + \frac{18.7}{(1+0.2182)^5} + ($$

$$\frac{34.3}{(1+0.2182)^7} + \frac{36.2}{(0.2182-0.035)\cdot(1+0.2182)^7}$$

= $88.13 Million

$$\text{Price per share} = \frac{88.13}{10} = 8.81\ \$/\text{share}$$

With the above valuation, Isabel and Claire can now decide if they want to go ahead with the equity STO, and if so, which fraction of the total number of shares they want to float.

Conclusions and Recommendations

A valuation framework for equity-based STOs will allow for more transparent markets. A significant difficulty to build a DCF valuation framework is the lack of a closed-form expression of discount rates for start-up firms. In this paper, we developed a method to calculate such a discount rate; it incorporates the default risk premium present in all start-ups. The discount rate function discovered in this paper is time-dependent and piecewise. The first part of the function is exponential; the second part is a power function. The reason is that, in the early years, the probability of survival of firms descends more rapidly than in late years. The discount rate function discovered has a remarkably good fit with empirical data- for the total of firms and for the ten industry sectors for which data is available.

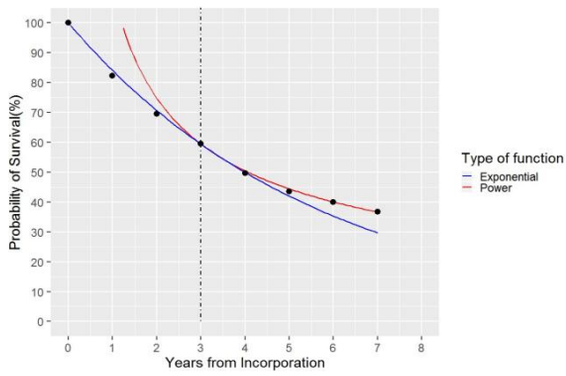
The methods to forecast the cash flows to the firm are straightforward, but the quality of the valuation will depend on the precision to measure the Serviceable Obtainable Market. Discount rates vary by industry sector. Each industry sector has its discount rate characteristics represented by parameters C, α, and λ. For future direction, we would like to suggest further work in adding data for more sectors and finer granularity of data by adding sub-sectors. Also, it would be useful to extend the model by considering variable "a" as continuous and evaluate the new optimum transition point. As the discount rate function is time-dependent, it would be useful to study its maxima-minima characteristics. A final recommendation would be of studies on the factors that influence the difference in target discount rates demanded by VC firms on start-ups and the results obtained in this manuscript.

For the total of firms, the highest discount rates were in the 27.0 to 31.8% range when the liquidation value of the non-surviving start-up project is set to zero. This range is considerably higher than observed discount rates of projects for mature firms(7.5%) but considerably less than some published discount rates for projects financed by Venture Capital firms which are in the 40.6 to 70% range. This discovery represents a positive development for the offerings of equity-based security tokens. A valuation method for equity STOs will help to develop a more transparent market for start-ups wanting to raise capital. Most importantly, our results show that for many start-up firms, equity STOs are an economical alternative to raise capital.

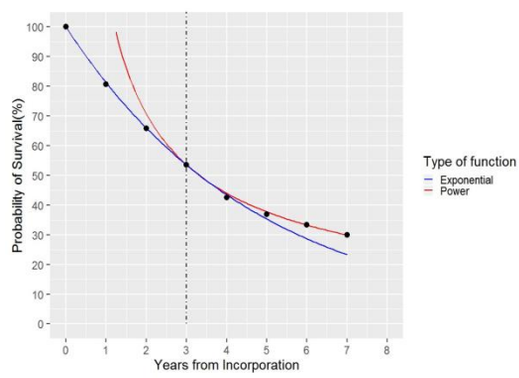
8 Appendix

Probability of survival for the ten industry sectors in the Knaup & Piazza [4] study.

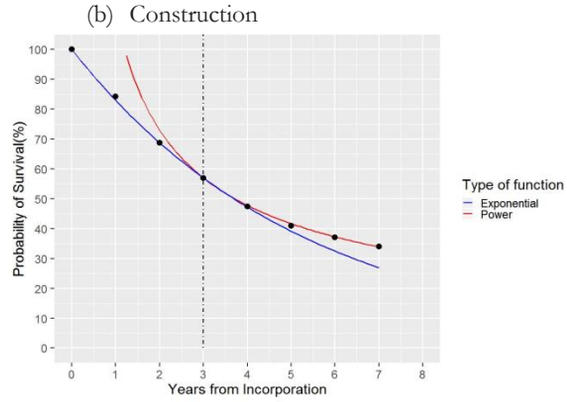
Part 1 - Probability of survival by industry sector. 1999-2005 period



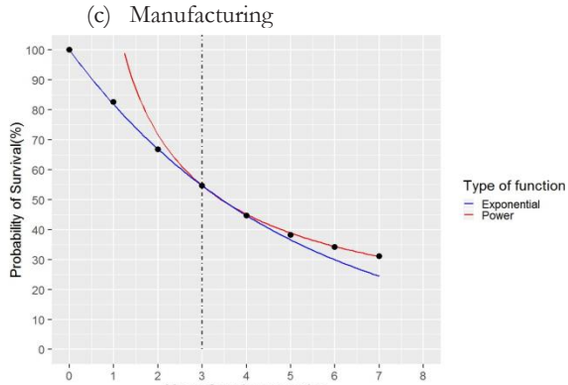
(a) Natural Resources and Mining



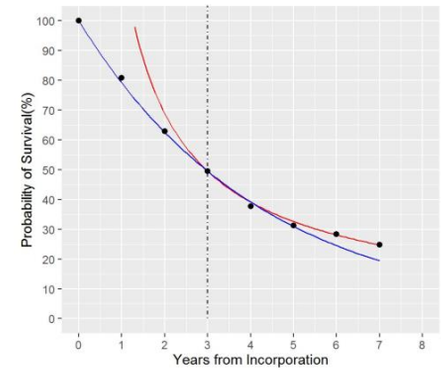
(b) Construction



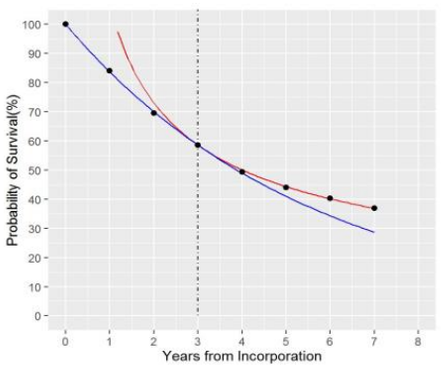
(c) Manufacturing



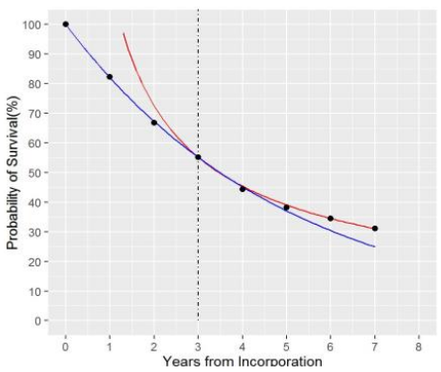
(d) Trade, Transportation and utilities



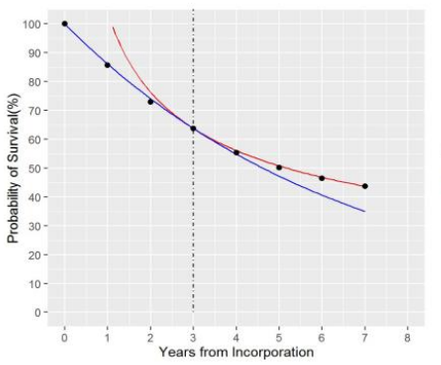
(e) Information



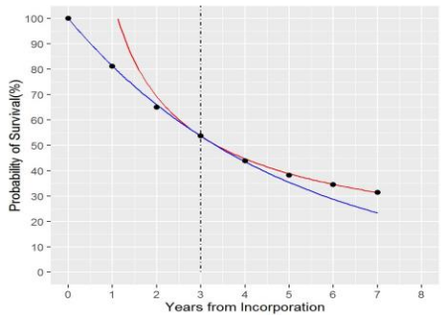
Part 2 - Probability of survival by industry sector. 1999-2005 period



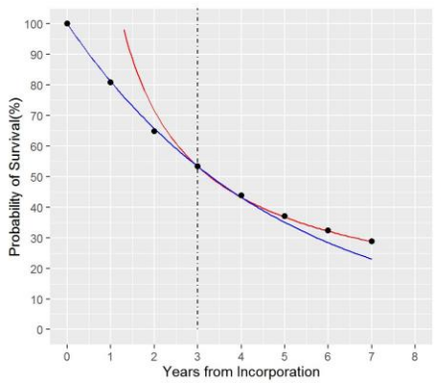
(a) Professional and Business Services



(b) Education and Health Services



(c) Leisure and Hospitality



(d) Other Services

References

[1] J. H. Cochrane, "Presidential address: Discount rates," The Journal of Finance, vol. 66, no. 4, pp. 1047–1108, 2011.

[2] S. Bhagat, "Why do venture capitalists use such high discount rates?" The Journal of Risk Finance, vol. 15, no. 1, pp. 94–98, 2014.

[3] A. Damodaran, "Valuing young, start-up and growth companies: estimation issues and valuation challenges," 2009.

[4] A. E. Knaup and M. C. Piazza, "Business employment dynamics data: survival and longevity, ii," Monthly Lab. Rev., vol. 130, p. 3, 2007.

[5] A. Damodaran, Investment Valuation: Tools and techniques for determining the value of any asset. John Wiley & Sons, 2012, vol. 666.

[6] 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.

[7] J. Lintner, "The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets," in Stochastic Optimization Models in Finance. Elsevier, 1975, pp. 131–155.

[8] T. Hogan and E. Hutson, "Capital structure in new technology-based firms: Evidence from the Irish software sector,"

Global Finance Journal, vol. 15, no. 3, pp. 369–387, 2005.

[9] W. E. Wetzel and C. R. Seymour, Informal risk capital in New England: Report and survey results. University of New Hampshire, 1981.

[10] J. L. Plummer and J. Walker, QED report on venture capital financial analysis. QED Research, 1987.

[11] J. C. Ruhnka and J. E. Young, "Some hypotheses about risk in venture capital investing," Journal of Business Venturing, vol. 6, no. 2, pp. 115–133, 1991.

[12] F. Richards, "A flexible growth function for empirical use," Journal of Experimental Botany, vol. 10, no. 2, pp. 290–301, 1959.

[i] λ was calculated by using the point at $t = a = 3$ with the exponential function. And, a and C were calculated by using points at $t = a = 3$, and $t = b = 7$ with the power function.

[ii] Yield 10 year Treasury on Sept. 1st. 2018.

[iii] http://pages.stern.nyu.edu/~adamodar/

[iv] Yield 10 year Treasury on Sept. 1st. 2018

[r] http://pages.stern.nyu.edu/~adamodar/

Photo by Liam Burnett-Blue on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

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

Toward a Crypto-friendly Index for the APEC Region

Mikayla Novak, Anastasia Pochesneva
RMIT Blockchain Innovation Hub, RMIT University, Australia
Correspondence: mikayla.novak@rmit.edu.au

Received: 30 October 2018 **Accepted:** 20 December 2018 **Published:** 29 December 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

This paper presents a new index concerning the extent of public policy accommodation towards usage of blockchain technology. The coverage of the index is for the 21 Asia-Pacific Economic Cooperation (APEC) member states, representing a significant bloc of global production, trade and economic development. The crypto-friendly index includes indicators related to four general categories of blockchain policy: (i) extent of policy restrictiveness toward cryptocurrency initial coin offerings; (ii) extent of policy restrictiveness toward cryptocurrency exchanges; (iii) taxation treatment toward cryptocurrencies; and (iv) type and extent of general public policy interest in blockchain-related activity. Based on data and information available as at October 2018, the index results reveal considerable diversity exists amongst APEC countries in terms of their degree of crypto-friendliness. Jurisdictions such as Hong Kong, Singapore, Australia, the United States and Canada are seen as relatively crypto-friendly locations, whereas jurisdictions such as China, Vietnam and Peru have the greatest scope for pro-blockchain policy improvement. This paper suggests future avenues for index refinement, as well as the potential for additional research into the concept of crypto-friendliness using this and similar policy indexes.

Keywords: *APEC region, blockchain, crypto-friendliness, index, ranking*
JEL Classifications: *C80, K2, K34, O38, P50*

1. Introduction

Blockchain technology is a distributed, digital, peer-to-peer ledger that records, verifies and validates data on its public database without recourse to a centralised authority, or intermediary, to manage the data. High-powered cryptoeconomic incentive mechanisms securely verify data blocks entered on the blockchain and ensure that all parties reach consensus about facts needed to propagate economic, financial, political, social and other projects. As such, the blockchain represents a contemporary refinement of ledger technologies that record and disseminate transactional and other facts underpinning multi-person coordination.

Blockchain is widely touted as a ledger technology suitable for transforming the operational and governance environments of business, government and civil society. It is supposed that blockchain will not only bring about production efficacies and cost savings but will, ultimately, bring about better governance [1]. What started out as the technology underpinning the Bitcoin crypto-currency has mushroomed into fields as diverse as financial management, personal identity, property titles, supply chain relationships, even voting. Irrespective of their backgrounds, ideals and interests, people can leverage the blockchain to develop robust and self-executing contracts, to track payments from sender to receiver in real time and launch new investment projects. Whereas interest in blockchain and its applications have exploded in recent years there are many factors which will, ultimately, have a bearing upon the rate of adoption and practical uses of this technology. One of the more pivotal of these factors is the stance of public policy treatment toward blockchain. The significance of policy here is that it territorially influences the set of viable blockchain-enabled activities within, and amongst, political jurisdictions. Even at this relatively early stage of blockchain diffusion, policymakers in some countries are enacting policy change either to encourage internal blockchain activity, or to attract blockchain investment from other places. Policymakers in other locations, still, are acting to repel blockchain usage in their jurisdictions.

We suggest that differing degrees of policy accommodation toward blockchain can be referred

to as variations in "crypto-friendliness" extended by policymakers amongst jurisdictions. So-called "crypto-friendly" jurisdictions see blockchain as a lucrative opportunity for economic development, proactively clarifying regulatory and tax treatments of cryptocurrency and other blockchain applications, and trialling blockchain uses in fields predominated by public sector activity. Policymakers in countries hostile toward blockchain-related activity have, by contrast, instigated bans or strict limitations with respect to blockchain engagement by developers and users. We label hostility or aversion toward blockchain as examples of "crypto-unfriendliness." In other words, the degree of observed crypto-friendliness by a country is situated on a crypto-friendly (policy accommodation) versus crypto-unfriendly (policy suppression) spectrum.

The theoretical basis for crypto-friendliness is being developed by blockchain researchers [2, 3, 4, 5]. This paper takes the crypto-friendliness literature one step further, presenting an index measure of the degree of crypto-friendliness observed amongst Asia-Pacific Economic Cooperation (APEC) member countries. Drawing from a range of information sources, including blockchain analysts, crypto-currency specialists and mainstream business media outlets, we develop indicators of public policy positions toward blockchain. From these indicators it is possible to construct a holistic index ranking the degree of crypto-friendliness across countries. This crypto-friendly index provides some insight for blockchain developers, information technology and other businesses, governments and other interested parties in terms of which APEC countries are demonstrating crypto-friendly blockchain leadership and which countries have scope for public policy improvements.

The structure of this paper is as follows. In Section 2 we outline the methodology and information sources used in the development of the crypto-friendly index. In Section 3 we provide the results of our index analysis (applicable as at October 2018), indicating countries within the APEC region maintaining policies which are relatively crypto-friendly or crypto-unfriendly. A brief conclusion, primarily focused upon potential research resulting from the development of the crypto-friendly index, follows.

2. Methodology

A range of policy categories are established for the 21 APEC member countries. Within those categories are a range of indicators which reflect specific kinds of policy treatment of blockchain and its applications (particularly crypto-currencies). Scores are allocated to each indicator, as specified below, and these are aggregated across the categories to provide an overall crypto-friendly index value. This overall index value can be used to help inform assessments about the degree of crypto-friendliness maintained by each jurisdiction.

The following provides descriptions of each indicator utilised for each category of the crypto-friendly index. Country-specific policies and information sources are also disclosed (see Supplemental Material). It should be noted that information used to inform the indicators are applicable to policies imposed by the central government of each country, excluding sub-national jurisdictions.

Category A: ICO restrictiveness

One of the pivotal activities undertaken within crypto-currency markets is fundraising for development and other projects through the creation and sale of digital tokens. This process is commonly known as an "initial coin offering" (ICO), and is serving as a mechanism to facilitate the growth of blockchain-enabled ventures. As explained by Van Rijmenam and Ryan, "[a]n ICO is increasingly being used by Blockchain start-ups to raise money by distributing a percentage of the initial coin supply. Basically, with an ICO a start-up plays the role of a bank; it digitally creates money out of nothing and sells that to 'investors'. The tokens, or crypto-coins, which are sold during the crowd sale will be used on the platform to pay for transactions and distribute value across the stakeholders. 'Investors' who purchase these coins during the ICO do not get a share in the start-up, but they hope that the price of the coin will rise and as such they can get a (substantial) return on their investment" [6, pp. 24-25].

According to statistics supplied by ICO Data [7], the aggregate global amount of funds raised through ICOs has risen substantially over the last few years. In 2014 over US $16 million was raised through two ICO ventures, rising to over US $6 billion in 2017 (through 873 ventures). The aggregate value of ICOs from January to September 2018 (US $7 billion, and 1,095 ventures) has surpassed the total for the entirety of the previous calendar year. Part of this growth is attributed to the fact that, in addition to ICO engagement by the "crypto community," legacy businesses with established services and products are using ICO fundraising to finance their business activities [8].

As with other forms of investment ICOs carry with them considerable risks and uncertainties. Aside from the uncertainties surrounding the potential for a given ICO venture to achieve an insufficient return, there is a fear that ICOs may be surrounded by misrepresentation, fraud and manipulation [9]. Expected future returns may be inflated by ICO proponents, and a lack of transparency may surround the identity of those advancing an ICO and the degree of information provided to potential investors. There may also be concerns that ICOs are being used as a vehicle to finance illicit activities.

It is for these, and other, reasons that governments have indicated a growing interest in regulating ICO activities. Although regulatory settings in this financial space, and in similar contexts, are designed to filter out unproductive and malign activities, there is the additional risk that overly prescriptive ICO regulations may limit the potential of blockchain participants to raise sufficient funds for productive and licit purposes. This provides the basis for establishing a crypto-friendliness index category to track the degree of ICO restrictiveness by country.

Indicator 1: ICO regulatory stance

This indicator represents the general stance of regulators toward ICO activities in blockchain spaces, ranging from "allowed," "restricted," to "disallowed" as well as "neutral/no regulation." Countries which allow ICOs are allocated a score of 3, restricted countries are given a score of 1 and disallowed countries a score of 0. Countries which are regarded as neutral or having no regulation are allotted a score of 2, reflecting the notion that ICOs are permitted to take place even if unregulated. The score allocation reflects the generic view that countries allowing ICOs to operate within their jurisdiction are more crypto-friendly in this regard.

Indicator 2: Regulatory treatment by nature/purpose of ICO raising

APEC member countries which regulate ICOs can potentially make distinctions in regulatory treatment on the basis of the perceived nature and/or purpose of given ICO ventures. For example, regulators may distinguish between ICOs on the basis of their economic function – e.g. whether ICOs are seen as genuine investments involving the creation of assets, or are used to develop tokens used merely as a means of payment or value transfers. Countries which do regulate on the basis of the nature and/or purpose of ICO raising appear to be attempting to do so in order to facilitate an environment of productive fundraising through the blockchain, and are given a score of 1. Countries which do not provide such regulatory treatment are allocated a score of 0.

Category B: Crypto exchange restrictiveness

Another important feature of the blockchain ecosystem has been the development of "crypto exchanges." These virtual facilities enable users to trade crypto-currencies for traditional, "fiat" currencies or other crypto-currencies. For instance, a crypto exchange may enable individuals and organisations to buy and sell Bitcoin for Ether, Litecoin or any other crypto-currency, or buy and sell Bitcoin for US dollars, Japanese yen and so on. As explained by Rainer Böhme and colleagues, "most crypto exchanges operate double auctions with bids and asks much like traditional financial markets, and charge a commission ranging from 0.2 to 2 percent. Some exchanges offer more advanced trading tools, such as limit or stop orders. At present, many trades in bitcoin are accompanied by one or even two conversions from and/or to conventional currencies. Furthermore, price quotes in bitcoin are almost always computed in real time by reference to a fixed amount of conventional currency" [10, p. 220].

In a similar vein to exchange mechanisms for traditional currencies, securities and other financial instruments, crypto exchanges play an important role in facilitating transfers toward higher valued uses within the blockchain environment. According to data supplied by BitInfoCharts [11], the average transaction value of Bitcoin in September 2018 was US $23,709 whereas for Ethereum it was US $661 (data as at 20 September 2018). Much of the value exuded by such trades is conducted through crypto exchange platforms.

Many crypto exchanges are centralised, third-party intermediary platforms which are reasonably easy to use and provide ease of access. A problem with such exchanges is that they are either vulnerable to attack from malign sources or, lacking direct accountability (and control by) crypto-currency traders, susceptible to mismanagement. The Mt. Gox Bitcoin exchange, established in 2010 to become the largest crypto-currency exchange at the time, suspended trading, closed its website and exchange service, and filed for bankruptcy by 2014. It was reported that about 850,000 Bitcoins belonging to customers and the exchange were missing, presumed stolen, with a value in excess of US $450 million at the time [12]. The Binance crypto exchange temporarily halted trading in February 2018 in light of a potential phishing scam [13]. Alongside the potential of lax security and inadequate investor protections, crypto exchanges may fail due to a lack of liquidity or ambiguous clearance and settlement procedures.

Policy interest in crypto exchange platforms arise from a desire to protect investors and customers who trade in cryptocurrencies. Similarly, to regulations applicable to ICOs, governments have shown an inclination to regulate crypto exchanges in various ways. The issue is whether crypto exchange regulation facilitates the buying and selling of crypto-currencies to the interest of all participants, or whether regulation unduly hampers the development of crypto exchanges.

Indicator 3: Crypto exchange regulatory stance

This indicator represents the general stance of regulators toward crypto exchange activities, ranging from "allowed," "restricted," to "disallowed" as well as "neutral/no regulation." Countries which allow crypto exchanges to operate are allocated a score

of 3, restricted countries are given a score of 1 and disallowed countries a score of 0. Countries which are regarded as neutral or having no regulation is allotted a score of 2, reflecting the notion that crypto exchanges can establish operations albeit in an unregulated manner. The score allocation reflects the generic view that countries allowing crypto exchanges to operate within their jurisdiction are deemed to be relatively more crypto-friendly.

Indicator 4: Application of Anti-Money Laundering (AML)/ Counter Terrorism Financing (CTF)/Know Your Customer (KYC) regulation

This indicator scores jurisdictions based on their implementation of AML, CTF and/or KYC regulation. A score of 1 is allocated to countries that have implemented such regulations, whereas a score of 0 is given to those countries that have not introduced AML, CTF and/or KYC. The imposition of such regulations is aimed at providing assurance to blockchain users that crypto exchanges are not channelling funds for illicit purposes, or at risk of being used for illicit purposes, thus providing a signal concerning the propriety of crypto exchange platforms.

Category C: Cryptocurrency tax treatment

In modern societies governments compulsorily acquire revenue from several sources to fund the production and provision of public goods and other essential services. One means through which the public sector acquires its revenue is through taxation – according to the OECD, taxes are compulsory unrequited payments to general government "in the sense that benefits provided by government to taxpayers are not normally in proportion to their payments" [14, p. 313].

In the interest of maintaining a diverse revenue base that is more robust to economic and other shocks, governments ordinarily impose taxation simultaneously upon a range of activities and sources. The OECD revenue classifications include reference to: taxes on income, profits and capital gains; social security contributions; taxes on payrolls and the workforce; taxes on property (including immovable property or on net wealth, gifts and estates); and taxes on goods and services (including excises and customs duties).

Governments have progressively investigated and, in some instances imposed, taxes on cryptocurrencies to prevent losses of potential taxation revenue resulting from the trading of cryptocurrency. As illustrated by the rise of certain forms of regulation upon cryptocurrency markets, governments have particularly revealed a concern about any "revenue leakage" resulting from the capability of cryptocurrency holders to avoid tax liabilities imposed within the conventional, non-blockchain economy. Given the multiple uses to which crypto-tokens are used it has been challenging for taxation authorities to incorporate cryptocurrencies into the framework of existing tax rules and legislation.

The extent of taxation policy interest in cryptocurrencies to date have largely surrounded the definition of tokens for tax policy purposes, and the treatment of income or, more generally, financial gains attained from cryptocurrency trades. The following indicators relate to taxes imposed by central governments only and exclude consideration of cryptocurrency tax regimes by sub-national levels of government.

Indicator 5: Taxation status of cryptocurrency

Certain countries have established definitions of cryptocurrencies within the context of existing taxation legislation and formal guidelines. In the broadest sense, cryptocurrencies to date have either been defined as akin to currency (albeit a privately issued form of currency not issued by the state), as a commodity like other commodities existing within the economic system, or as a form of property (or asset) like a financial security. Variations in the legal status of cryptocurrency have implications for when notifications of taxation liability are activated by fiscal authorities. Countries whose tax authorities or finance ministries have declared that cryptocurrency will be treated in a certain way are allocated a score of 1. By contrast, countries which have yet to declare a tax interpretation for cryptocurrency is allocated a score of 0 because of their uncertainty that a lack of clarity in tax treatment provides to domestic cryptocurrency users.

Indicator 6: Capital gains tax rate on cryptocurrency

Certain countries impose capital gains taxation on the capital gains (or profit) arising from the sale or disposal of an asset purchased or otherwise acquired. It is assumed that the cryptocurrency has been held as a long-term investment and the capital gains tax rate is applied to individual holders of cryptocurrency only. The capital gains tax rate selected is applicable to an earner bearing the top-tier marginal income tax rate. Capital gains tax rates are grouped into "low" (rates of 0-20 per cent), "medium" (20-40 per cent) and "high" (40+ per cent). Countries with low capital gains taxes are allocated a score of 2, medium tax-rate countries 1, and high taxing countries are given a score of 0. This scoring arrangement reflects the economic insight that capital gains taxes are assessed as being economic inefficient, distorting decisions to invest [15, 16, 17]. Note that if a country has not issued a formal declaration of cryptocurrency the capital gains tax rate is not applicable to the token and is thus allotted a 0 score.

Category D: General policy interest

There exist other measures which could be used to gauge the degree of governmental accommodativeness

toward blockchain. These measures, by and large, relate to the preparedness of political actors to countenance the use of distributed ledger technologies in conventional fields of public sector activity – including public administration and service delivery (including judicial, legal and social services).

Indicator 7: Existence of public sector use cases

Countries that have trialled or permanently established blockchain use cases applicable to public administration or government service delivery are adjudged to be crypto-friendly. These countries receive a score of 1 for that category. Countries that have not instigated public sector use cases (including announcements of use cases that have yet to be trialled or otherwise implemented) receive a score of 0.

Indicator 8: Existence of regulatory "sandboxing" trials or policies

Several countries have instigated trials or permanent arrangements that enable participants to experimentally interact with each other, under closed conditions and with simulated (not actual) regulatory environments applying. During the testing period the participants are exempted from some, or all, actually-existing regulations in place [3]. These arrangements are known as "sandboxes," and are used by regulators to learn about the effect of regulatory ideas under experimental conditions. Countries that have trialled or established sandboxing arrangements for blockchain applications (including FinTech) are assigned a score of 1, whilst those countries that have not engaged in sandboxing are given a score of 0.

3. Results

Variations in the degree of crypto-friendliness across countries are highly likely to be informed by policy differentials. In essence, jurisdictions toward the crypto-friendly end of the blockchain policy spectrum are more likely to proactively clarify the tax treatment of blockchain tokens and assets, and to not tax those instruments punitively. Measures attempting regulatory certainty with respect to crypto-economic activities, without undermining the growth and development of blockchain use and adoption, are also consistent with crypto-friendliness. Other features of a crypto-friendly policy environment include the facilitation of use cases, and the instigation of "sandboxing" or other regulatory trials of blockchain (including fintech applications, which typically incorporate blockchain elements).

The opposite of a jurisdiction pursuing crypto-friendliness in policy terms is a jurisdiction opting for crypto-unfriendliness, the latter posing an aversion toward the legitimisation of widespread economic coordination within the emerging crypto-economy. Policies consistent with this approach may include outright bans on blockchain application use by end-users or intermediaries (e.g. in relation to cryptocurrencies), stringent regulatory treatment (e.g. licensing blockchain participants, requirements to de-anonymise users), heavy or overtly discriminatory taxes, and the discouragement of use cases.

The results of the crypto-friendly index for the APEC region are illustrated in Table I, with the information in the Table affirming a clear dispersion amongst APEC member-states with respect to their crypto-friendliness. The assessment that is made here is that countries such as Singapore, Hong Kong, Australia, the United States, Canada, Japan and New Zealand are amongst the most crypto-friendly countries within the trading bloc. Malaysia, the Philippines and Chinese Taipei are also notable for their relatively high ranking on the crypto-friendliness index. Features which arguably distinguish these countries from their APEC counterparts are their accommodative regulatory approaches toward ICO and crypto exchange activities.

At the other end of the spectrum – i.e. countries which rank relatively low on the crypto-friendliness scale – are countries such as China, Vietnam, Peru, Chile, Brunei Darussalam and Indonesia. Most of these countries have assumed an openly hostile regulatory approach toward cryptocurrencies, and the use of blockchain more generally. In particular, ICO issuance and trades through crypto exchanges have either been explicitly banned within some of these jurisdictions, or such activities have been severely restricted through stringent regulation. It is also notable that crypto-unfriendly jurisdictions have yet to introduce formal guidelines or legislation to impose taxation upon cryptocurrency purchases or sales, which may create ambiguities or uncertainties amongst blockchain participants in relation to how the activities will be taxed into the future (if at all).

Conclusion

This paper presents a crypto-friendly index of blockchain policy accommodativeness for APEC-member countries. This composite index, which provides relative rankings for 21 countries, is based on an analysis of formal policies in relation to the treatment of ICOs and crypto-currency exchanges, as well as an assessment of the tax treatment of cryptocurrencies and the existence of public sector blockchain use cases.

The index is not intended to be definitive and will be subject to refinement as the evolution of policy responses toward blockchain continues to unfold in response to new opportunities and challenges. Further, there are opportunities to refine the methodology of the index as adoption of blockchain matures and new

uses for this technology are discovered. In addition to developing indexes incorporating a larger cohort of countries, it is possible to extend the current index methodology to incorporate policies pursued by sub-national governments. Future research into the refinement of crypto-friendly indexes may embrace methodological alterations including subjective evaluations of taxation and regulatory climates by blockchain analysts and participants.

As indicated in this paper observable differences can be identified in terms of the policy treatment of blockchain technology and its applications within the APEC region, as of October 2018. This study indicates that countries such as the United States, Japan, Singapore, Australia and Canada have invoked relatively crypto-friendly policies comparable to best-practice standards found in jurisdictions such as Estonia, Switzerland and the United Arab Emirates. APEC member-countries which diverge from the crypto-friendly cohort have tended to do so either on the basis of a lack of formal policy position (at the time of writing this report) or, in some limited cases, adverse or hostile responses to certain aspects of blockchain activity such as ICO issuance or the operation of crypto exchanges. The findings of this crypto-friendly index provide diagnostics for relatively crypto-unfriendly countries to improve their relative ranking thorough the introduction of blockchain-accommodative policy reforms.

It is envisaged that the crypto-friendly index would serve as a platform for further academic and applied policy research into the nature of distributed ledger technologies and their impacts upon economies. Contingent upon the provision of a sufficiently minimal data sample size, it is possible to use this crypto-friendly index for empirical research. Some potential research opportunities include: is there a relationship between the degree of crypto-friendliness and the spatial distribution of blockchain-related activity? Are there any links between crypto-friendliness and background economic institutions, such as adherence to the rule of law and protection of property rights? How do assessments of crypto-friendliness relate to the structure of national innovation systems, and the possibility to undertake permission less innovation [18]? Is crypto-friendliness related to variables such as country size, labour market skills or general aptitudes towards technology and material progress?

The APEC region consists of a diverse cohort of countries, from developing to developed economies with a heterogeneous set of economic, cultural, social and political conditions. Technological advances

Table I: Crypto-friendly index results for APEC member-states (information as at October 2018)

Country	Total score	ICO restrictiveness		Crypto exchange restrictiveness		Taxation treatment		General policy interest	
		Regulatory stance[a]	Regulatory treatment by nature/purpose of ICO[b]	Regulatory stance[c]	AML/CTF/KYC regulation[d]	Cryptocurrency tax treatment[e]	Capital gains tax rate[f]	Public sector use cases[g]	Sandboxing trials / arrangements[h]
Hong Kong, SAR China	13	3	1	3	1	1	2	1	1
Singapore	13	3	1	3	1	1	2	1	1
Australia	12	3	1	3	1	1	1	1	1
United States	12	3	1	3	1	1	1	1	1
Canada	11	3	1	3	1	1	0	1	1
Japan	11	3	1	3	1	1	0	1	1
New Zealand	11	3	1	3	1	1	1	1	0
Malaysia	10	3	1	3	1	0	0	1	1
Philippines	10	3	1	3	1	0	0	1	1
Chinese Taipei	9	3	0	3	1	0	0	1	1
Mexico	8	2	0	3	1	0	0	1	1
Korea, Republic of	7	0	0	1	1	1	2	1	1
Thailand	7	1	1	1	1	1	1	0	1
Papua New Guinea	6	2	0	2	0	0	0	1	1
Russian Federation	6	2	0	2	1	0	0	1	1
Brunei Darussalam	5	2	0	2	0	0	0	0	1
Chile	5	2	0	2	0	0	0	1	0
Indonesia	5	2	0	1	0	0	0	1	1
Peru	4	2	0	2	0	0	0	0	0
China	2	0	0	0	0	0	0	1	1
Vietnam	2	1	0	1	0	0	0	0	0

Notes: (a) Allowed (score=3), neutral/no regulation (2), restricted (1), disallowed (0). (b) Yes (1), no/n.a. (0). (c) Allowed (3), neutral/no regulation (2), restricted (1), disallowed (0). (d) Yes (1), no/n.a. (0). (e) Asset/commodity/money/property/other (1), none (0). (f) Low 0-20% (2), medium 20-40% (1), high 40%+ (0). (g) Yes (1), no (0). (h) Yes (1), no (0). For country information and sources informing the indicator scores, see Supplemental Material.

such as blockchain provide the potential for closer trade, financial and economic integration amongst APEC economies, as well as lucrative opportunities for citizens residing in this region to enhance their social capabilities and harness economic development potential. Ultimately, blockchain is a governance technology and this fact suggests the need for coherent, whole-of-government responses within jurisdictions as well as cross-country collaborations amongst APEC members as a whole.

Whilst there remains an expectation that the extent of crypto-friendliness will continue to vary amongst APEC member-states for some time, the ability of governments to develop creative and flexible policy responses to the opportunities potentially posed by blockchain will be a critical determinant of the long-term economic success for the region.

References

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

[2] C. Berg, S. Davidson and J. Potts, "The blockchain economy: what should the government do?" Medium, November 11, 2017. [Online]. Available: https://medium.com/cryptoeconomics-australia/the-blockchain-economy-what-should-the-government-do-c69cbdab7c3c. [Accessed 30 September 2018].

[3] M. Finck, "Blockchains: Regulating the Unknown," German Law Journal, vol. 19, no. 4, pp. 665-692, 2018.

[4] P. De Filippi and A. Wright, Blockchain and the Law: The Rule of Code, Cambridge: Cambridge University Press, 2018.

[5] M. Novak, "Crypto-friendliness: Understanding blockchain public policy," [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3215629. [Accessed 26 October 2018].

[6] M. Van Rijmenam and P. Ryan, Blockchain: Transforming Your Business and Our World, London: Routledge, 2018.

[7] "ICOData – database of presale and active ICO dates with rating," [Online]. Available: https://www.icodata.io/. [Accessed 30 September 2018].

[8] W. Kaal, "Initial Coin Offerings: The Top 25 Jurisdictions and their Comparative Regulatory Responses (as of May 2018)," Stanford Journal of Blockchain Law & Policy. [Online]. Available: https://stanford-jblp.pubpub.org/pub/ico-comparative-reg. [Accessed 26 October 2018].

[9] Netherlands Authority for the Financial Markets (Autoriteit Financiële Markten). "Initial Coin Offerings (ICO's): serious risks," [Online]. Available: https://www.afm.nl/en/professionals/onderwerpen/ico. [Accessed 20 September 2018].

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

[11] "Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats," [Online]. Available at: https://bitinfocharts.com/. [Accessed 28 September 2018].

[12] "Mt. Gox – Wikipedia," [Online]. Available at: https://en.wikipedia.org/wiki/Mt._Gox. [Accessed 20 September 2018].

[13] S. Jagati, "Binance Offers a $250K Bounty to Find Failed Hackers," Cryptoslate, March 11, 2018. [Online]. Available: https://cryptoslate.com/binance-offers-250k-bounty-find-failed-hackers/. [Accessed 20 September 2018].

[14] Organisation for Economic Co-operation and Development (OECD), Revenue Statistics 1965-2016, Paris: OECD Publishing, 2017.

[15] A. B. Atkinson and J. E. Stiglitz, "The Design of Tax Structure: Direct versus Indirect Taxation," Journal of Public Economics, vol. 6, pp. 55-75, 1976.

[16] K. L. Judd, "Optimal taxation and spending in general competitive growth models," Journal of Public Economics, vol. 71, pp. 1-26, 1999.

[17] C. Lammam and J. Clemens, Capital Gains Tax Reform in Canada: Lessons from Abroad, Vancouver: Fraser Institute, 2014.

[18] A. Thierer, Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, Revised and Expanded Edition, Arlington: Mercatus Center, 2016.

[i] The APEC member countries are: Australia; Brunei Darussalam; Canada; Chile; China; Chinese Taipei; Hong Kong, SAR China; Indonesia; Japan; Korea, Republic of; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; Philippines; Russian Federation; Singapore; Thailand; United States; Vietnam.

Photo by Dmitry Moraine on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-1-(5)2019

Cryptocurrencies & Initial Coin Offerings: Are they Scams? An Empirical Study

Daniel Liebau[1], Patrick Schueffel[2]
[1]IE Business School, IE University, Spain
[2]HEG Fribourg School of Management, Switzerland
Correspondence: dliebau@faculty.ie.edu
Received: 15 January 2019 **Accepted:** 20 March 2019 **Published:** 2 April 2019

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
The authors would like to thank Bobby Ong and the Coingecko team for their proactive support.

Abstract
The volume of Initial Coin Offerings (ICOs) had risen steeply with an all-time high market capitalisation of close to 1 trillion USD in December 2017. Since then the digital asset market has slumped, retreating to approximately 200 billion USD by mid-2018. Stakeholders of the crypto industry have pondered the reasons for this retrenchment and are increasingly focusing on the notion that many ICOs could be scams. A recent industry study even went as far to claim that 80% of all ICOs are indeed scams. In this paper, we investigate the question whether these scams are as common as claimed. We do so by first defining what a scam is and secondly, by drawing on empirical data to assess the number of cases fitting such a definition. Building on Principal Agent Theory and based on the statistical analysis of our empirical data set we attempt to establish the current state of affairs with regards to scams in the crypto-currency world. The results of our study divert from salient beliefs.
Keywords: *blockchain, scam, ICO, digital assets, ethics, crypto-currency, token*
JEL Classifications: *D01, D21, D26, D53, D84, K24*

1. Introduction

An Initial Coin Offering (ICO) is an unregulated process for capital-raising typically used by firms in the cryptocurrency field as a substitute for the controlled funding methods applied by other financial intermediaries [1]. The volume of ICOs had risen sharply with an all-time high market capitalisation of close to 1 trillion USD in December 2017. Since then the digital asset market has retreated to approximately 200 billion USD by mid-2018. Stakeholders of the cryptocurrency industry have since contemplated the causes for this retrenchment. While this "increasingly popular way to raise capital for Blockchain technology start-ups" [2, p.2] has become the method of choice for many crypto firms in order to raise capital, its performance increasingly often lacks behind expectations [3]. Consequently, numerous exponents of the cryptocurrency industry are increasingly focusing on the notion that many ICOs could be scams. A recent industry study went as far as to maintain that 80% of all ICOs are indeed scams.[4] However, it is generally acknowledged that poor economic performance cannot automatically be equated with a scam. Moreover, it is highly questionable that high failure rates are idiosyncratic to the novel phenomenon of the ICO. We, therefore, argue that a more differentiated view on ICOs and potential scams is necessary. Hence, with this study, we intend to investigate the question of whether and when ICOs can justifiably be called a scam. We believe that investigating this problem is of importance because scholars and practitioners alike have recently made rather coarse statements on this subject matter which were further amplified by the broader media. Economist Nouriel Roubini's testimony to the US Senate Hearing on "Exploring the Cryptocurrency and Blockchain Ecosystem", for instance, was subtitled "Crypto is the Mother of All Scams" [5] and Economics scholar Saifedean Ammous recently portrayed the Ethereum project as "a worthless scam" [6]. As ICOs nevertheless receive increasing attention not only by the media but also by investors, we deem it a worthwhile endeavour to investigate the magnitude of true scams in this area.

This article is organised in the following manner. First, we lay out the theoretical foundation of our research along with definitions of the terminology used. Secondly, the research methodology is explained sideways with the sample and data collection method.

In a third step, we present the results, before discussing them in a fourth phase. The article concludes with highlighting its contributions as well as its limitations and specifically the many possible future research directions with regards to the subject of scams in the Blockchain ecosystem.

2. Theoretical Foundation

Investigating scams is a multifaceted undertaking, and the term scam is not being used identically by all scholars, practitioners and the broader media. On the contrary, we believe that investors frequently mistake a poor economic performance for a scam and that this misjudgement is then further conveyed and amplified by the broader media. Over the next paragraphs we, therefore, provide a brief overview of the theory we ground our research on as well as the terms "scam" and "economic performance".

2.1 Principal-Agent Theory (PAT)

Agency Theory is a framework explaining how objectives are reached by separate players interacting with each other. As such it elucidates self-goals and other-goals and how distinct actors, so-called Principals and Agents, deal with difficulties in their coexistence. These challenges mostly arise from conflicts of interest between the Agent and the Principal [7]. Examples of such relationships include investor and broker, teacher and student, physician and patient as well as lawyer and client.

The conclusion that "agency, or acting for another, is pervasive" [8, p.1] holds in many aspects of life, and the cryptocurrency industry is no exception to this. Drawing on the findings of Mitnick [8] we employ the following four assumptions: first, actors are rational and sensibly weigh returns against investments. Second, actors will always seek for increasing returns. Third, the underlying model is a static one, that is there is no change in the actors' behaviour and learning. Lastly, acting on behalf of a third party may lead to fundamentally "different behaviour than acting for oneself." [8, p.4].

We deem PAT to be highly suitable to analyse the ICO phenomenon as the business entities' can be delineated as follows: The Principal is the investor/token buyer and agent is the software developer /token issuer, depicted in Figure 1.

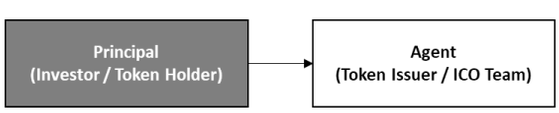


Figure 1. Principal and Agent in the context of for-business ICOs

The ICO team typically outlines the purpose, benefits and roadmap of their project in a whitepaper. The Principal, for ideological, economic or other reasons entrusts the Agent with funds to progress the project in question. The ICO team becomes the Agent acting on behalf of the Principal. The following parts of PAT are specifically appealing to consider in the context of ICOs and the Blockchain ecosystem: ICO projects typically exert considerable discretionary power over capital and resource allocation upon completion of the ICO. This corresponds with the assertion that "[t]he agent's problem is basically that of a choice of acts to best satisfy his preference for self and other goals" while being endowed with "considerable discretion with respect to the agent's goals" [8, p.34]. Such a constellation leaves the agent with the task to resolve a trade-off between self-goals and the agent's goals. We, therefore, pose that it is tempting for ICO teams to engage in fraudulent activities, especially in the absence of incentive systems that usually "include negative mechanisms like sanctions, threat of force, or reduction of agent return".[8, p.35] These incentive systems which typically reduce the likelihood of conflicts between the Principal and the Agent hardly exist in the crypto industry, increasing the risk for the Principal.

Then again this leads our thoughts to the subject of policing. "The cheapest method of policing the agent with respect to policing the principal's goals is to have the agent do it himself." [8, p.39]). Some, not all, ICOs work against a timeline with milestones. If a project does not hit the milestones, the community of Principals will publicly (mostly through social media) complain. Since many ICOs list their token on exchanges very swiftly after the ICO is complete, these complaints can impact the token price adversely. In summary, we consider the policing mechanisms available in the token world relatively weak and therefore conflicts of interest for the Agent are foreseeable.

3. Scam

The Oxford Dictionary defines a scam as "[a] dishonest scheme; a fraud." [9]. In a similar vein, Merriam-Webster states that a scam is "a fraudulent or deceptive act or operation" [10]. In turn, a fraud is an unlawful, respectively criminal act as it "consists of some deceitful practice or wilful device, resorted to with intent to deprive another of his right, or in some manner to do him an injury"[11][i]. In the context of business, scams are therefore regularly seen as acts throughout which the scammer purposefully deprives the trustful investor of his or her funds to advantage to the scammer. Consequently, the investment will not perform to the extent initially suggested by the scammer and believed by the investor. By comparison, the above-mentioned study by Dowlat, delineates scams in the following way: "Identified Scam (pre-trading): Any project that expressed availability of ICO investment (through a website publishing, ANN

thread, or social media posting with a contribution address), did not have/had no intention of fulfilling project development duties with the funds, and/or was deemed by the community (message boards, website or other online information) to be a scam." [4, p.23].

4. Economic Performance

Economic performance is the evaluation of a firm's success measured in monetary terms. It comprises its assets as well as liabilities and its ability to generate profits. Ultimately economic performance will determine the likelihood of organisational mortality.

Timmons Jeffry and Spinelli [12] estimated that the survival rate of new ventures is approximately 60% after the first year and 10% over ten years. Conducting research specifically on "new, adolescent, young, emerging and high-tech, technology, technology-intensive, and technology-based» ventures Song, Podoynitsyna, Van Der Bij and Halman [13, p.9] reported more fine-grained results. After analysing a longitudinal data set of 11,259 New technology ventures (NTVs) established between 1991 and 2000 in the United States, the authors conclude that the survival rate of NTVs with five or more full-time employees is only 36 per cent after four years and that this survival rate drops further to 21.9% after five years [13]. As Blockchain technology is a rather young phenomenon and technology is at the core of any crypto project, start-ups and NTVs and NTVs can provide interesting benchmarks.

5. Research Methodology

5.1 Sample

As we strive to establish the extent of scams among ICOs worldwide, the level of our analysis was set to a macro level. Accordingly, we collected global data from relevant international ICO Web sites, such as ICO Data [14], Token Market [15], ICO Bench [16], Coin Index [17], ICO Watch List [18], and CoinGecko [19]. While those sources did mention the ICO of the Decentralized Autonomous Organization (DAO), we decided to exclude this ICO from our sample as it would overly skew the data analysis with its emission volume of more than USD 150 million.

The decision to use the 2016 cohort was based on the rationale of providing a long enough time frame required for potential plaintiffs to file legal proceedings against fraudulent ICOs. Furthermore, 2016 was chosen as the number of ICOs throughout that year was already a multiple of the previous years, hence yielding a more solid base for a quantitative analysis than the cohorts of 2014 and 2015. To be included in the sample an ICO had to meet the following two criteria: first, it must be a public offering, i.e. advertised through the pertinent outlets of the crypto community and second it must have completed its ICO during the year 2016. Based on the defined sampling criteria a sample size of 45 was obtained.

5.2 Method

In our attempt to elicit the true ICOs scams we conducted a descriptive multi-level analysis on our sample. First, we scanned the Lexis Nexis Database for any news related to the sample ICOs. Lexis Nexis is considered to be among the most comprehensive news databases globally, providing interfaces to 36'000 international sources [20]. Search delimiters were set to cover only news items as of 2016 or younger. Each ICO was checked along with the keyword "scam" as well as the synonyms *fraud", "sham" "deceit", "con", and "hoax". Second, whenever any of these search terms in conjunction with an ICO yielded a result, we furthermore conducted a more in-depth search for any resulting legal proceedings or court cases that may have emerged subsequently. Third, if court cases were initiated, we investigated whether a verdict was delivered yet, if so, what the ruling was. The cut-off date for our data sampling process was the 8th of January 2019.

6. Results

Table 1 reports the ICOs of 2016 along with the findings from our descriptive multi-level analysis. Next to selected demographics of the ICOs such as token name, funds raised, ICO end, the table indicates whether the ICO was mentioned in the news as a scam, fraud, sham, deceit, con or hoax. We also counted these words in case they were used as verbs or adjectives. The dataset furthermore provides information on whether a lawsuit was initiated against any ICO of the 2016 cohort and if so, what the court's verdict was. Next, to this information, we gather a set of control variables, such as the issuing price of the token as well as its current price and performance in the market. The total number of subjects in the sample was 45. Of those 45 projects, three (6.7%) were referred to in the context of a scam in the news at least one time: DinarDirham, E-dinar, and Bitconnect. Bitconnect was furthermore named a fraud, deceit, and con. Lawsuits were initiated against two projects (4.4%): E-dinar and Bitconnect. In the case of one project (2.2%), Bitconnect, the court ruled that it was a fraudulent scheme whereas the court ruling for E-dinar stated that it was a legitimate token.

Looking at the control variables further points are noteworthy: For 22 of the 45 objects, respectively for 49% of the cases, no data could be obtained for the issuing price or the current price or both. Cases of missing data were labelled as, "n.a.". Consequently, no performance figures could be calculated for those projects. For those ICOs, however, for which financial

Table 1: Analysis of Initial Coin Offerings (ICOs), cohort of 2016.

No	Name	Token	USD Raised	End of ICO	Issuing Price	Current Price (8.1.2019)	Delta	Initial investment	Total Return	% with n.a.	Scam	Fraud	Sham	Deceit	Con	Hoax	Law Suit Initiated	Verdict: fraudulent
1	DigixDAO	DGD	5,500,000	3/1/2016	3.23529	21.15885	554%	1000	5540									
2	Lisk	LSK	6,500,000	3/21/2016	0.07647	1.40638	1739%	1000	17391									
3	Waves	WAVES	16,010,008	5/31/2016	0.18835	2.93855	1460%	1000	14602									
4	Newbium	n.a.	38,180	5/31/2016	n.a.	n.a.		1000	0									
5	Pluton	PLU	1,000,000	6/24/2016	1.17647	0.54633	-54%	1000	-536									
6	Rise	n.a.	1,188,823	6/24/2016	n.a.	n.a.		1000	0									
7	ICO OpenLedger	ICOO	1,388,427	6/30/2016	2.93754	0.11189	-96%	1000	-962									
8	Stratis	STRAT	600,945	7/26/2016	0.00715	1.11835	15541%	1000	155413									
9	Incent	INCNT	1,000,000	9/1/2016	0.04346	0.04472	3%	1000	29									
10	DinarDirham	DNC	n.a.	9/3/2016	n.a.	n.a.		1000	0		Y							
11	BlockPay	BLOCKPAY	675,000	9/5/2016	0.12435	0.04775	-62%	1000	-616									
12	NEO	NEO	3,758,871	9/7/2016	0.18794	8.39597	4367%	1000	43674									
13	Bitpark Coin	BITPARK	291,956	9/15/2016	0.10400	n.a.		1000	0									
14	FirstBlood	1ST	5,500,000	9/25/2016	0.06428	0.03230	-50%	1000	-497									
15	Iconomi	ICN	10,682,516	9/26/2016	0.10500	0.21120	101%	1000	1011									
16	DeClouds	DC	288,426	10/5/2016	n.a.	n.a.		1000	0									
17	Lykke	LKK	2,800,000	10/9/2016	0.05600	0.02202	-61%	1000	-607									
18	Synereo	AMP	4,700,000	########	0.1597	0.02	-87%	1000	-875									
19	eBoost	EBST	140,000	########	0.20000	0.02322	-88%	1000	-884									
20	SingularDTV	SNGLS	7,500,000	########	0.01500	0.01104	-26%	1000	-264									
21	Bitgirls	TOREKABU	n.a.	########	n.a.	n.a.		1000	0									
22	DECENT	DCT	4,126,300	11/6/2016	0.10715	0.12314	15%	1000	149									
23	Kibo Lotto	KBT	3,039,813	########	0.00000	n.a.		1000	0									
24	Golem	GNT	8,596,000	########	0.01048	0.07064	574%	1000	5740									
25	Komodo	KMD	1,983,781	########	0.02204	0.76213	3358%	1000	33580									
26	ETCWin	n.a.	1,309,000	########	0.00000	n.a.		1000	0									
27	Arcade City	ARC	699,187	########	n.a.	n.a.		1000	0									
28	Nexium	NXC	115,500	########	0.00400	0.00621	55%	1000	553									
29	Decentralized Capit	n.a.	n.a.	########	n.a.	n.a.		1000	0									
30	Mass coin	MASS	252,432	12/1/2016	0.00000	n.a.		1000	0									
31	Nodio	NOD	81,487	12/1/2016	n.a.	n.a.		1000	0									
32	Golos	GOLOS	462,000	12/4/2016	0.10000	0.00956	-90%	1000	-904									
33	Ark	ARK	942,593	########	0.00995	0.44753	4398%	1000	43978									
34	E-dinar	DER	n.a.	########	n.a.	0.00858		1000	0		Y						Y	N
35	vSlice	VSL	1,800,000	########	n.a.	0.00289		1000	0									
36	eGaaS	EGS	64,000	########	n.a.	n.a.		1000	0									
37	Roundcoin	ROUND	96,338	########	n.a.	n.a.		1000	0									
38	Bankcoin	BANKCOIN	1,000,000	########	0.25000	0.00476	-98%	1000	-981									
39	Hacker Gold	HKG	645,000	########	0.04004	n.a.		1000	0									
40	PRCOIN	PRCOIN	823,940	########	n.a.	0.00012		1000	0									
41	BlockCDN	BCDN	303,000	########	n.a.	n.a.		1000	0									
42	Darcrus	DAR	297,426	########	0.02000	0.01774	-11%	1000	-113									
43	ebitz	EBZ	285,035	########	0.00000	n.a.		1000	0									
44	Bitconnect	BITbitconnectNEC	450,289	########	n.a.	n.a.		1000	0		Y	Y		Y	Y		Y	Y
45	Branche	BLT	n.a.	########	n.a.	n.a.		1000	0									
	TOTAL	TOTAL	**96,936,274**					**45,000.00**	**314,420.80**	**18**	**3**	**1**		**1**	**1**		**2**	**1**
	in percentage							100%	698.7%	40.0%	6.7%	2.2%		2.2%	2.2%		4.4%	2.2%
		Sum of n.a's:	9,032,967					Total ROI	598.71%									
		% of total raised:	9.3%					Annualized ROI	164.33%									

performance figures could be calculated they varyfrom near total losses of the investment (-98%) to a significant multiplication in value (+15.541%). As we demonstrate in Table 1 an evenly distributed portfolio of these ICO tokens (we assumed 1000 USD allocation to each project) would have yielded a hypothetical return of approximately 598.71% over the two years and eight days period analysed.

7. Discussion

Drawing data from a global sample of international ICOs, this study shows that far less than the alleged 80% of ICOs are scams in the legal sense of the word. On the contrary, we could only identify one case (2.2%) where an ICO would match the definition of a scam as provided above. Even if we assumed that this figure is underestimated due to a large number of unreported cases, an adjusted estimate increasing this number previously reported 80%. What is more, even if we assume the worst-case scenario that the 22 projects for which we cannot obtain data on the issuing price or the current price or both turn all out to be scams we would see fundamentally different results by several hundred percent, it would not get close to the than established previously: These 22 cases would account for 49% of the ICOs observed and not for 80% as reported formerly [4].

7.1 Survival

At the same time, the worst-case failure rate of 49% may not be idiosyncratic to the field of ICOs. 51% survivors is relatively close to the above mentioned 60% survival rate for NTVs. Literature provides abundant evidence that other factors may also contribute to such high failure rates in similar settings. A plethora of factors can influence an organisation's performance and thus ultimately its survival. The number of potential antecedents to a firm's performance is large, especially if the company is not only of young age but especially if it ventures into international markets. This is typically the case with organisations conducting an ICO. Research has shown that companies of a young age are subject to higher failure rates than older ones. A substantial number of small firms typically fail early on after their inception [21, 22] because they suffer from what scholars call “liability of newness” [23]. At the same time, it was established that companies which enter a foreign institutional environment suffer from "liability of foreignness" [24]. Consequently, ICOs typically suffer from those two disadvantages at the same time. Previous research has shown that companies of a young age are subject to higher failure rates than older ones. A substantial number of small firms typically fail early on after their inception [21, 22] because they suffer from what scholars call “liability of

newness" [23]. This concept suggests that young firms are particularly vulnerable to mortality because they still have to generate the necessary routines, relationships, and reputations that are required to efficiently operate in their respective surroundings [23]. Drawing on the findings of Lumpkin et al. [25] Sapienza, Autio, George and Zahra [26] allege that young firms are more likely to exhibit an entrepreneurial orientation to internationalization, which results in a higher risk-taking proclivity, greater propensity to innovation and a more proactive stance, yet they point out that these firms have a very limited stash of reserves which makes them extremely vulnerable in case of organizational mistakes. Anand and Delios [27] and Hamel et al. [28] contend that over time firms will increasingly be able to utilise their reputation, brand, marketing channels, social capital, company culture and customer loyalty to ease disruptions caused by the business environment or by internal mistakes.

Companies that enter the international domain are typically confronted with a range of costs associated with their expansion. Typically, such costs include learning costs, but more specifically also adjustment costs for adapting to the foreign environment [24]. Foreign entrants typically display a lack of familiarity with legal, social, and economic conventions, as well as consumer preferences and cultural features of the targeted foreign markets. In addition, firms that enter foreign markets are typically obliged to modify their routines and processes to properly operate within these markets. Whilst these companies typically do benefit from the experience they had previously made with marker entries when further entering subsequent markets [29], these companies are nonetheless faced with the task of adapting some of their existing processes and creating some new ones in order to optimally serve this foreign market. Creating those routines and adapting others will consume additional resources [30]. These costs can be significant and enduring and in the worst case fatal to the venture [31]. Besides, companies regularly incur yet additional costs associated with their internationalization. These costs stem from an increased organizational and environmental complexity which leads to additional costs for governance, coordination, and transaction that may outweighing the benefits gained from internationalization [32].Lastly, internationalization increases ventures' exposure to financial and political risks resulting from currency fluctuations, governmental directives, and trade regulation [33, 34].

Taken together liability of newness and liability of foreignness can pose severe obstacles to new ventures conducting business internationally. Sleuwaegen and Onkelinx [35] established that 29% of their surveyed international new ventures had to withdraw from the international market place and, as a consequence, failed to survive altogether.

7.2 Financial performance

The results pertaining to the financial performance of the ICO also yielded some interesting insights. As mentioned before, assuming a worst-case scenario an investor investing in all tokens throughout the 2016 ICO vintage would have suffered a total loss for many of them. However, those tokens which survived would have handsomely compensated for those losses. As mentioned above, an evenly distributed portfolio of ICO tokens would have yielded an interest of approximately 164% p.a. or 598.71% total return over the ca. two-year period. Despite all controversy, it may even occur justifiable to the rational investor to be scammed in individual cases as long as other portfolio components display the growth in value leading to the above returns. Of course, caveat emptor remains true and historical performance was seldom a good predictor of future performance. Other recent ICO research focusing on historical returns during the same period could be an indication of bubbles [36] which explain these abnormally high returns after such a short period, even in the start-up space.

8. Limitations and future research directions

This study is not exempt from limitations which in turn enable other researchers to contribute. We encourage further studies on scams in the crypto sphere considering variations in the methodological as well as empirical setup. Moreover, as our study is solely an ex-post observation which is only of limited utility to crypto investors, we issue a call to put a larger emphasis on investigating the antecedents of scams.

8.1 Methodology

Mitnick [8, p.9] maintains that so-called "collapsed relations" where Agent and Principal are identical are not in the scope of the PAT. Consequently, one could argue that differences may exist between a more community-based, more decentralised ecosystem, such as Bitcoin and pure for-business entities that use the ICO mechanism as a means of funding their proprietary business. In the context of Blockchain, such relationships are best depicted as "interwoven decentralisation" where ICO teams, ecosystem users, and token holders can be both Principals and Agents at the same time. Borders may not be as clearly defined as initially assumed, leaving the subject interlocked as depicted in Figure 2.

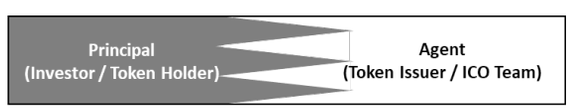


Figure 2: Principal and Agent in the context of cryptocurrencies & interwoven decentralization

Building on the findings of Mitnick [8] further aspects of PAT offer additional research directions in the context

of ICOs. We consider the following four topics as particularly noteworthy. First, as Mitnick [8, p.17] puts it "[a] rational party would not enter into a contract if he/she did not expect it to be fully and perfectly operative, i.e. all parties will abide by it (Alternatively, of course, the party may expect the contractual arrangement to malfunction to his benefit)". Henceforth, the research questions arise whether ICO teams understand that a SAFT[ii] contract - which virtually does not contain any investor rights - will indeed malfunction? Moreover, does this understanding of the extremely skewed risk-taking by the Principal, turn ICO teams into scammers? Secondly Mitnick [8, p.17] points out that "[t]he rational contracting party with preference characterised by some measure of risk aversion, i.e. security rather than adventure, will demand that some guarantees or assurances accompany the contract.". Here, the following research questions emerge: Does this suggest that most ICO investors are indeed not rational since "assurances and guarantees" are most commonly missing in current SAFT agreements? How can this be aligned with current research on asset-bubbles such as Zetzsche, Buckley, Arner and Föhr [37]? Thirdly, Mitnick [8, p.18] argues that valid agreements should be kept. Validity requires an absence of … fraud or deceptions". Building on the previous research questions we therefore ask whether a SAFT without investor rights be considered a "valid" contract? Furthermore, we suggest considering the consequences if it was not a valid one. Fourth, throughout this study we have focused on the Principal as the investor and token holder and the Agent representing the token issuer and ICO teams. Consequently, there is the opportunity to expand ICO scam research to other actors in the ecosystem such as centralised exchanges, market makers and actors on social media aiming to deceive potential investors through misleading statements and false offerings. Fraudulent market practices in today's securities markets such as "Pump and Dump" as observed by Li, Shin and Wang [38] in the crypto-currency markets may be considered a scam.

8.2 Empirical Setup

As outlined above the basis of our empirical research was the 2016 cohort of ICOs. The subsequent years, 2017 and 2018 displayed a vast increase in ICOs. Hence, the most obvious opportunity to build on our research is to replicate our study with data comprising those two vintages. While the total amount of ICO projects increased drastically, it remains to be seen if the percentage of scams changed as well.

8.3 Antecedents to scams - The Crypto Scam Probability Index (CSPI)

In order to warn investors of scams ex-ante, we would welcome any research contributing to a Crypto Scam Probability Index (CSPI) in order to potentially spot dubious projects before investors put their money into them. The underlying notion is to create a mechanism that can be used to protect investors from bad actors. A comprehensive set of meaningful factors for such an index would need to be established. Yet, first indicators have already been raised by journalists [39], being 1) plagiarism, 2) identity theft and 3) advertising of improbably returns. Clearly, we foresee that this set is extensible for numerous factors such as whether SAFTs had been used, how much have been raised, whether developers are actively working on the project etc. Applying hierarchical regression analysis [40] and / or necessary condition analysis [41] to the 2017 cohort of ICOs researchers could empirically identify relevant factors predicting ICO scams.

For illustration purposes we suggest designing the CSPI along the following lines:

$$\Pi_{SCAM} = \sum \frac{1}{a}SU + \frac{1}{b}AR + \frac{1}{c}DA + \frac{1}{d}KD + \frac{1}{e}VE + \frac{1}{f}SO + \cdots + \frac{1}{z}XY$$

For each factor coding and weighting according to its importance in the context of ICO scams is required, where $\sum a,b,c,d,e,f,\ldots,z \equiv 100$ and where the variables capture the following facts (not comprehensive!)

SU: SAFT was used (no = 0; yes =1)

AR: amount of funds raised (USD 0-15m = 0; >USD 15m =1)

DA: developers are active (no = 0; yes =1)

KD: KYC on clients is done (no = 0; yes =1)

VE: vesting is required (no = 0; yes =1)

SO: code is open source (no = 0; yes =1)

XY: other factors

Conclusion

So far, literature yields only limited insights on scams in the context of ICOs. This paper enhances our knowledge about this phenomenon, contributing to existing cryptocurrency research. Using a global sample, this study has revealed that the magnitude of ICO scams is much smaller than initially anticipated. The article offers alternative explanation for the allegedly poor performance of ICOs by relating them to studies from entrepreneurship literature. Moreover, this paper sketches a possibility of how scams could be more easily identified ex ante in the future.

References

[1] P. Schueffel, The Conscise Fintech Compendium, Fribourg: School of Management Fribourg, 2017.

[2] A. de Jong, P. Roosenboom, and T. van der Kolk, "What Determines Success in Initial Coin Offerings?," Available at SSRN 3250035, 2018.

[3] ICO Rating, ICO Market Research Q3 2018, ICO Rating, Saint Petersburg, 2018.

[4] S. Dowlat, Cryptoasset Market Coverage Initiation: Network Creation, 2018.

[5] K. Rooney. "Bitcoin is the 'mother of all scams' and blockchain is most hyped tech ever, Roubini tells Congress," 11 January 2019; https://www.cnbc.com/2018/10/11/roubini-bitcoin-is-mother-of-all-scams.html.

[6] F. Gheorghe. "A Bitcoin Maximalist Just Compared Proof Of Stake To The Fed (And Why This Isn't The Case)," 11 January 2019; https://beincrypto.com/a-bitcoin-maximalist-just-compared-proof-of-stake-to-the-fed-and-why-this-isnt-the-case/.

[7] J.-J. Laffont, and D. Martimort, The theory of incentives: the principal-agent model: Princeton university press, 2009.

[8] B. Mitnick, "The theory of agency: A framework," 1975.

[9] Oxford English Dictionary, "scam, n.," Oxford English Dictionary Online, 27. November, Oxford University Press, 2018.

[10] Merriam-Webster, "scam, n.," Merriam-Webster Inc., 2018.

[11] Black's Law Dictionary, "What is FRAUD?," The Law Dictionary, Sureswift Capital, 2018.

[12] A. Timmons Jeffry, and S. Spinelli, "New Venture Creation," Irwin, Homewood III, 1990.

[13] M. Song, K. Podoynitsyna, H. Van Der Bij, and J. I. M. Halman, "Success Factors in New Ventures: A Meta-analysis*," Journal of Product Innovation Management, vol. 25, no. 1, pp. 7-27, 2008.

[14] ICODATA.io, "ICO Status," 2018.

[15] TokenMarket, "Past ICOs," TokenMarket Ltd., 2018.

[16] ICO Bench, "Browse ICOs," 2018.

[17] Coin Index, "Browse Initial Coin Offerings," ICOindex.com, 2018.

[18] ICO Watch List, "Welcome to the ICO Watch List!," 2018.

[19] Coingecko. "ICO," 10 December, 2018; https://www.coingecko.com/en/ico.

[20] LexisNexis, "LexisNexis, the world's leading provider of news, business and legal information," RELX Group, 2018.

[21] J. E. Everett, and J. Watson, "Do small businesses have high failure rates? Evidence from Australian retailers," Journal of Small Business Management, vol. 34, no. 4, pp. 45-62, 1996.

[22] W. M. Ladzani, and J. J. van Vuuren, "Entrepreneurship training for emerging SMEs in South Africa," Journal of Small Business Management, vol. 40, no. 2, pp. 154–161, 2002.

[23] A. L. Stinchcombe, "Social Structure and Organizations," Handbook of Organizations, J. G. March, ed., pp. 142-193, Chicago: Rand-McNally, 1965.

[24] S. Zaheer, "Overcoming the liability of foreignness," Academy of Management Journal, vol. 38, no. 2, pp. 341-363, 1995.

[25] G. T. Lumpkin, and G. G. Dess, "Clarifying the entrepreneurial orientation construct and linking it to performance," Academy of Management Review, vol. 21, no. 1, pp. 135-172, 1996.

[26] H. J. Sapienza, E. Autio, G. George, and S. A. Zahra, "A capabilites perspective on the effects of early internationalization on firm survival and growth," Academy of Management Review, vol. 31, no. 4, pp. 914-933, 2006.

[27] J. Anand, and A. Delios, "Absolute and relative resources as determinants of international acquisitions," Strategic Management Journal, vol. 23, no. 2, pp. 119-134, 2002.

[28] G. Hamel, and C. K. Prahalad, "Strategy as stretch and leverage," Harvard Business Review, vol. 71, no. 2, pp. 75-84, 1993.

[29] F. Vermeulen, and H. G. Barkema, "Learning through acquisitions," Academy of Management Journal, vol. 44, no. 3, pp. 457-476, 2001.

[30] W. Mitchell, J. M. Shaver, and B. Yeung, "Foreign entrant survival and foreign market share: Canadian companies' experience in United States medical sector markets," Strategic Management Journal, vol. 15, no. 7, pp. 555-567, 1994.

[31] J. V. Singh, R. J. House, and D. J. Tucker, "Organizational change and organizational mortality " Administrative Science Quarterly, vol. 31, no. 4, pp. 587-611, 1986.

[32] S. Zaheer, and E. Mosakowski, "The dynamics of the liability of foreignness: A global study of survival in financial services," Strategic Management Journal, vol. 18, no. 6, pp. 439-663, 1997.

[33] A. K. Sundaram, and J. S. Black, "The environment and

internal organization of multinational enterprises," Academy of Management Review, vol. 17, no. 4, pp. 729–757, 1992.

[34] D. M. Reeb, C. C. Y. Kwok, and H. Y. Baek, "Systematic Risk of the Multinational Corporation," Journal of International Business Studies, vol. 29, pp. 263-279, 1998.

[35] L. Sleuwaegen, and J. Onkelinx, "International commitment, post-entry growth and survival of international new ventures," Journal of Business Venturing, vol. 29, no. 1, pp. 106-120, 2014/01/01/, 2014.

[36] H. Benedetti, and L. Kostovetsky, "Digital tulips? Returns to investors in initial coin offerings," Returns to Investors in Initial Coin Offerings (May 20, 2018), 2018.

[37] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators," University of Luxembourg Law Working Paper, no. 11, pp. 17-83, 2017.

[38] T. Li, D. Shin, and B. Wang, "Cryptocurrency pump-and-dump schemes," Available at SSRN, 2018.

[39] The Wall Street Journal. "A Flood of Questionable Cryptocurrency Offerings - Search for hundreds of projects showing signs of plagiarism, identity theft and promises of *improbable returns," 09 January, 2019; https://www.wsj.com/graphics/whitepapers/.*

[40] J. F. Hair, R. L. Tatham, R. E. Anderson, and W. Black, Multivariate Data Analysis, 5th Edition ed.: Prentice Hall, 1998.

[41] J. Dul, "Necessary Condition Analysis (NCA)," Organizational Research Methods, vol. 19, no. 1, pp. 10-52, 2015.

[i] We accounted for any fraud case, independent of its regulatory status, i.e. whether it is an unregulated utility token or a regulated security token.

[ii] The Simple Agreement for Future Tokens (SAFT) is a contract offered by ICO teams to investors. It conveys the rights in tokens prior to the development of the tokens' functionality.

Photo by chuttersnap on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-1-(3)2019

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

Darcy W.E Allen, Alastair Berg, Brendan Markey-Towler
Blockchain Innovation Hub, RMIT University, Australia
Correspondence: alastair.berg@rmit.edu.au
Received: 23 January 2019 **Accepted:** 14 February 2019 **Published:** 24 February 2019

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
DA, AB & BM-T designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

We apply institutional cryptoeconomics to the information problems in global trade, model the incentives under which blockchain-based supply chain infrastructure will be built, and make predictions about the future of supply chains. We argue blockchain will change the patterns and dynamics of how, where and what we trade by: (1) facilitating new forms of economic organisation governing supply chain coordination (such as the V-form organisation); (2) decreasing information asymmetries and shifting economic power towards the ends of supply chains (e.g. primary producers); (3) changing the dimensions along which we can reliably differentiate goods and therefore de-commoditising goods and disaggregating price signals; and (4) decreasing consumer reliance on quality proxies (e.g. production within national borders).

Keywords: *Institutional Cryptoeconomics, Institutional Economics, Supply Chain Management, Blockchain Supply Chains*

1. Introduction

Blockchain and other distributed ledger technologies are poised to act as new economic infrastructure for global trade networks [1]. As a technology for creating distributed ledgers of information, blockchain may act as the infrastructure on which information about goods are validated, stored and accessed. Blockchain might not simply make our existing supply chain structures more efficient, but transform how, where and what we trade. When the standardised shipping container was invented in the 1950s it didn't just made goods cheaper; it also altered trading patterns, opened up new trade networks, and made some traditional port infrastructure redundant [2]. In this paper we draw on the existing literature of blockchain-based supply chains [1, 3] together with the emerging field of institutional cryptoeconomics [4-6] to ask the question: how might blockchain-based supply chain infrastructure change our global trade networks? We first model the incentives necessary for supply chain actors to implement and build this infrastructure, before making four predictions:

- Blockchain will drive creation of new forms of economic organisation to coordinate the information problems along global supply chains, such as the V-form organisation [7, 8];
- Blockchain will help reduce information asymmetries (e.g. information about markets, prices and the structure of the supply chain itself) and therefore shift economic power towards the ends of the supply chain (e.g. primary producers and consumers);
- Blockchain will drive de-commoditisation of goods by offering deeper information for consumers to make more subjective value perceptions; and
- Blockchain will facilitate new proxies of quality—as distinct to that derived simply from production within national borders—and therefore a closer match between comparative advantages and production.

Blockchain as an institutional technology for supply chain infrastructure

When described simply as a new type of ledger, blockchain might seem to be little more than accounting technology. Such innovations, however, can have a profound impact on an economy's institutional structure. The ledger-centric view of the economy argues the importance of ledgers in mapping property ownership and relationships, along with other rights and responsibilities which underpin economic and political exchange [see 9]. Tracking inventories and ownership rights throughout complex organisational

structures requires robust ledgers which can be reconciled and audited with relative ease. Changes to the nature of ledgers have long been associated with changes in institutions. The emergence of literacy in the ancient Near East enabled detailed records of taxation and expenditure [6, 10], while double entry bookkeeping contributed to the emergence of capitalism by facilitating distributed ownership of enterprise, the spread of risk, and the emergence of multinational corporations [11]. The propensity to exchange is closely correlated with the ready verification of property rights, along with a system of courts and law to enforce those rights [12].

Transaction costs have been used to account for organisational variety [13]. Coase [14] and Williamson [15] sought to explain why some transactions occur within a firm rather than a market.[i] The logic is that different institutions create alternate organisational structures to transact, and the choice of institution depends on several behavioural factors which give rise to transaction costs. For instance, people exhibit cognitive limitations (e.g. bounded rationality) and do not always act benevolently (i.e. people can be opportunistic).[ii] Transaction cost economics gains predictive logic by recognising that transactions exhibit different types and degrees of asset specificity, uncertainty and frequency of exchange which interact with these behavioural factors to give rise to transaction costs [16, 20, 21].[iii] From this perspective blockchains 'industrialise trust' by reducing the transaction costs which economic actors might otherwise face, thereby shifting the mix of transaction cost minimising institutions [23]. Institutional cryptoeconomics uses the transaction cost economics framework to explain how blockchain technology shifts the comparative efficacy of firms, markets, governments and civil society to solve economic problems [24-26].

There are three main types of trade costs that create frictions in supply chains: transportation, political and information costs [27]. Transportation costs have been lowered through transportation technologies including the shipping container [2, 28]. Political and regulatory barriers such as tariffs have been reduced through global coordination bodies such as the World Trade Organization (WTO) [29]. However, when goods move along supply chains, trusted information about those goods must also move with them. That information must be produced and maintained through economic organisation. Consumers demand information in terms of the legitimacy, quality and provenance of a product. That information enables consumers to differentiate products and to subjectively value them. Governments demand information about goods to comply with domestic regulations, such as biosecurity restrictions, minimum labour or ethical standards and sanctions compliance. Producers demand information about goods after they have sold them, including information about their consumers as well as the rents and actions of others along the supply chain (e.g. fraudulent activity in transit).

Information costs increase as organisational distance increases [30]. Goods have characteristics that are the product of production, financing, delivery, warehousing, regulatory procedures and a myriad of other processes in a supply chain. Except for in the context of a supply chain located wholly within a vertically integrated organisation, these processes might occur across tens, hundreds, or even thousands of discrete organisations. Apple, for instance, has 785 suppliers, across 31 countries [31]; their products are (officially) available for sale in most countries, apart from those subject to US sanctions such as North Korea and Syria, or where there is little demand, like in Afghanistan and Yemen [32]. As supply chains become longer and more complex, information changes hands more often and across more relationships [33], potentially leading to information loss or fraud.

Producing and maintaining trusted information about goods is costly. Private organisations produce some of this information, ensure its integrity, and communicate that information with others. Some supply chain information is produced through brand reputation, "repeat transactions … and social norms that are embedded in particular geographic locations or social groups" [34]. Siloed companies communicate information through paper-based bills of lading and ship manifests to maintain and update ledgers of information. When there is a lack of incentives for private companies to provide the information, they may be required to through legislation. Estimates of the administrative cost of this paperwork varies from 15 per cent of the value of goods shipped [35] to being equal to the cost of physically moving those goods [36]. The complexity of global supply chains also means that shipping goods involves a multitude of organisational interactions; Maersk found that a single shipment of refrigerated goods in 2014 from Africa to Europe involved 30 different individuals and organisations, with 200 separate interactions [37]. This process is not only costly, but due to the complexity and multiple interactions it is error-prone and open to fraud [38, 39].

Available technologies constrain what institutional solutions can be implemented to lower transaction costs [40]. Blockchain and other distributed ledger technologies create new potential for emergent governance solutions by storing transparent and tamper-resistant information about goods. This information could include ownership, location, environmental impact, and time stamping data [41]. The technology could be used, for instance, in the context of food safety and traceability, where provenance information can be consulted in real-time by consumers and regulators [see

3, 42]. Blockchain-based supply chains thus compete with other institutional governance systems (firms, markets and governments) to overcome information costs.

There is substantial interest from the private sector and from governments to develop blockchain-based economic infrastructure for global supply chains. This includes validating the legitimate ownership of goods traded [43], identifying counterfeit medicines [44, 45], tracking the trade of protected species [46] and managing food safety incidents [42]. Distributed ledger technologies are being adopted by firms including IBM, Maersk and Walmart as the economic infrastructure to achieve greater levels of assurance over the nature and provenance of goods as they move along supply chains [3]. For instance, in 2017 IBM and Danish shipping company Maersk announced their TradeLens blockchain solution [37]. Walmart has since announced their intention to use the IBM Food Trust platform to facilitate the sharing of provenance information by their leafy green suppliers in the wake of an E. coli outbreak [47].

Blockchain-based supply chains are likely to emerge in concert with other technologies, such as a permissioned network of actors who hold a QR code scanning technology that updates information on a private distributed ledger. This approach, however, raises questions of human involvement and the legitimacy of the data entered in the distributed ledger—the 'garbage in-garbage out' problem. Blockchains are unable to autonomously interact with real-world individuals or events and hence rely on 'oracles' to transmit data about temperature, contractual performance and so on [48]. Another approach will leverage more complex technologies in an attempt to input information via sensors [49], such as 'smart containers' where sensors upload information (e.g. temperature) to a blockchain-based distributed ledger. This represents a shift away from human-centred data input towards technology-centred data input, and might even see the dynamic adjustment of shipping routes and prioritisation based on the attributes of the goods shipped [50].

The precise nature of how blockchains will be applied within supply chain governance is uncertain. Adoption will likely require significant infrastructure upgrades or investments. In the following section we model the incentives for actors in a supply chain to adopt blockchain-based smart contracting supply chain infrastructure to get a sense of the factors from which that process will emerge.

Incentives to develop blockchain-based supply chain infrastructure

In this section we examine the necessary conditions that incentives for supply chain participants must meet for a blockchain-based supply chain to be built. The central institutional innovation for understanding blockchain-based supply chains is the smart contract. Proposed by Szabo [51], the smart contract is an algorithm which executes the provisions of a contract automatically upon the realisation of some state of the world. We could conceptualise a smart contract as follows. Upon the provision of some good or service x_{ij} by j to i, a smart contract executes automatic payment of some medium of exchange $p_{ij}(x_{ij})$, such as a cryptocurrency which is conditional on that good or service

$$p_{ij}(x_{ij}) = \begin{cases} p_{ij}^{N} & if\ x_{ij} = \{t_1 \dots t_N\} \\ \vdots & \vdots \\ p_{ij}^{1} & if\ x_{ij} = \{t_1\} \\ p_{ij}^{0} & if\ x_{ij} = \emptyset \end{cases}$$

with the property that $p^{N}_{ij} \geq \cdots \geq p^{1}_{ij} \geq p^{0}_{ij}$.

We define goods and/or services x_ij to be delivered as bundles of attributes $\{t_1 \dots t_N\}$ in the style of New Consumer Theory [52, 53], although defined more broadly than physical attributes to include information about the goods and/or services such as time and location of provision as well as state of provision. Once a smart contract is struck in a blockchain-based supply chain system, it is broadcast to the network of nodes holding the blockchain and validated once it is included in a block on which consensus is achieved by the network. When the conditions for its execution (the provision of x_{ij}) are broadcast to the network by whatever means, the contract is then executed. The blockchain on which a supply chain is implemented thus takes the form of a 'smart ledger', not only of static entries, but of smart contracts ready to be executed upon the realisation of various states of the world.

From a network of such contracts between i and j, we observe the emergence of the "decentralised autonomous organisation"—a network of economic interaction which emerges from the striking of smart contracts, and operates through their execution [4]. Obviously, such decentralised autonomous organisations can take the form of supply chains where they are organised around the provision of goods and services to meet some consumption end.

Under what conditions is there an incentive for i and j to implement their portion of a supply chain with smart contracts recorded and validated within a blockchain? The question, of course, comes down to the value that smart contract provides to those parties compared to other institutions. Smart contracts are costly to write and require specialised technical knowledge, so we would expect the emergence of organisations, such as consulting technology companies with specialties in cryptolaw. Obviously an incentive has to be provided

to the consulting firm to do so, which we denote as $c_{ik}[p_{ij}(x_{ij})]$ and $c_{jk}[p_{ij}(x_{ij})]$, the price i and j respectively pay to k to write the smart contract containing the protocol $p_{ij}(x_{ij})$ for them. Supposing that $c_k[p_{ij}(x_{ij})]$ is the opportunity cost of writing this contract, the consulting firm has an incentive to provide the smart contract as long as

$$c_{ik}[p_{ij}(x_{ij})] + c_{jk}[p_{ij}(x_{ij})] \geq c_k[p_{ij}(x_{ij})]$$

Let us suppose that the value that would be realised by i were j to provide them with the goods and/or services x_{ij} can be represented by a number $v_i(x_{ij})$ (for instance, marginal profit). In that case, given a distribution of beliefs $\beta_i(x_{ij} \mid p_{ij}\ \delta_j^b) \in [0,1]$ about the provision of x_{ij} by j conditional on the provisions p_{ij} of the smart contract and an information set δ_j^b about j contained within the blockchain (such as satisfaction metrics and so on), and assuming a von-Neumann-Morgenstern incentive structure, the expected value obtained by striking the smart contract on a blockchain is

$$\sum_{x_{ij}} \beta_i(x_{ij}|p_{ij}\ \ \delta_j^b)[v_i(x_{ij}) - p_{ij}(x_{ij})] - c_{ik}\left(p_{ij}(x_{ij})\right)$$

Were we to imagine that the cost to j of providing x_{ij} to i to be $c_j(x_{ij})$, and assuming a perfect correspondence between cost incurred and outcome in terms of provision of x_{ij} we could say that the value to j of striking the smart contract and providing x_{ij} to i is

$$p_{ij}(x_{ij}) - \left[c_j(x_{ij}) + c_{jk}\left(p_{ij}(x_{ij})\right)\right]$$

Now suppose that the same provisions $p_{ij}(x_{ij})$ would apply in an off-blockchain contract, that the same values $v_i(x_{ij})$ would obtain for i upon receipt of x_{ij}, and that the same costs $c_j(x_{ij})$ would be incurred for j to provide it. Suppose further that a distribution of beliefs $\beta_i(x_{ij} \mid p_{ij}\ \delta_j^b) \in [0,1]$ exists for i about the provision of x_{ij} by j conditional on the provisions p_{ij} and an information set δ_j^i available to i about j. To execute the contract, i and j have to incur a cost of verifying that x_{ij} has been provided which we call $c_i^T(x_{ij})$ and $c_j^T(x_{ij})$, and we assume that there is a perfect correspondence between the incurring of this cost and verification. This cost is variously the cost of compensating management hierarchies for providing third-party verification in firms, or the cost of verification by third parties in markets [54]. In markets we would imagine that these costs fall on j most heavily as they concern brand building and guarantees of various kinds to convince i that x_{ij} has been provided such that they ought to execute payment $p_{ij}(x_{ij})$ within the contract.

We will therefore find that there is an incentive to adopt blockchain-based supply systems if three conditions are simultaneously met:

$$\sum_{x_{ij}} \beta(x_{ij}|p_{ij}\ \ \delta_j^b)[v_i(x_{ij}) - p_{ij}(x_{ij})] - c_{ik}\left(p_{ij}(x_{ij})\right) \geq \sum_{x_{ij}} \beta(x_{ij}|p_{ij}\ \ \delta_j^i)[v_i(x_{ij}) - p_{ij}(x_{ij})] - c_i^T(x_{ij})$$

$$p_{ij}(x_{ij}) - \left[c_j(x_{ij}) + c_{jk}\left(p_{ij}(x_{ij})\right)\right] \geq p_{ij}(x_{ij}) - \left[c_j(x_{ij}) + c_j^T(x_{ij})\right]$$

$$c_{ik}\left(p_{ij}(x_{ij})\right) + c_{jk}\left(p_{ij}(x_{ij})\right) \geq c_k\left(p_{ij}(x_{ij})\right)$$

The third condition suggests that we will observe incentives for consulting companies to adopt blockchain technology and begin writing smart contracts if their opportunity costs are adequately compensated. However, the first two conditions require a little more interpretation. If we rearrange them we find that i has an incentive to adopt blockchain-based supply systems if

$$\sum_{x_{ij}} [\beta(x_{ij}|p_{ij}\ \ \delta_j^b) - \beta(x_{ij}|p_{ij}\ \ \delta_j^i)][v_i(x_{ij}) - p_{ij}(x_{ij})] \geq c_{ik}\left(p_{ij}(x_{ij})\right) - c_i^T(x_{ij})$$

while j has an incentive to adopt blockchain-based supply systems if

$$c_j^T(x_{ij}) \geq c_{jk}\left(p_{ij}(x_{ij})\right)$$

The second—the conditions under which j will be incentivised to adopt blockchain-based supply systems—is a very simple condition. If they are going to achieve similar compensation relative to costs for supplying x_{ij} in either blockchain-based or firms/market supply chains, the question of their incentivisation to adopt blockchain-based systems comes down to the differential costs of verification in the two systems—by smart contract or third party. If verification costs that x_{ij} has been provided are lower in blockchain-based supply chains, there is an incentive to adopt them.

The first condition—the conditions under which i will be incentivised to adopt blockchain-based supply systems—is a little more involved as it involves, in particular, the differential beliefs $\beta(x_{ij} \mid p_{ij}\ \delta_j^b) - \beta(x_{ij} \mid p_{ij}\delta_1^i)$ held about the delivery of x_{ij} in its various forms. Any increase in the transaction costs $c_{ik}[p_{ij}(x_{ij})] - c_i^T(x_{ij})$ caused by the expense of writing a smart contract must be compensated for by an increase in the expected value to be brought about by this contract. If the provisions of the contract itself do not change, then that increase in the value expected to arise from the contract comes from the increased *beliefs* about the net positive values $v_i(x_{ij}) - p_{ij}(x_{ij}) > 0$) and the decreased *beliefs* about the net negative values $v_i(x_{ij}) - p_{ij}(x_{ij}) < 0$) that may be realised by a supply chain based on a blockchain. That, naturally, is brought about by the range of information δ_j^b that is available within a blockchain about j upon which beliefs can be formed relative to the range of information δii that is available to i within a market/firm context.

We have good reason to believe that these two

conditions for incentivising the adoption of blockchain-based supply systems will become increasingly easy to satisfy over time, especially with respect to *i*, the "buyer" in this supply chain. In particular, we can expect that the cost of writing smart contracts will decrease markedly as consulting firms move down the learning curve and develop base templates. Moreover, such costs only need be incurred once when the smart contract needs to be written in the first place or altered, whereas verification costs must be incurred for each transaction in a market/firm setting. But it is in the wealth of information that is stored in a blockchain upon which to form expectations about the likelihood x_{ij} will be provided that we really see that incentives will emerge to adopt blockchain-based supply systems. Blockchain is *designed* to store information and validate it, which means we are very likely to see a better basis for more accurate beliefs to form about the provision of x_{ij} in various states by j within blockchain-based supply chain systems.

Predictions for the future of supply chain governance

New forms of economic organisation

Even if supply chain actors are incentivised to adopt blockchain-based infrastructure, this adoption process is likely to require significant coordination and cooperation across multiple actors. The evolutionary change from the current, and often paper-based, system towards a more digitised blockchain-based system requires technical and economic coordination between supply chain actors. On one hand there could be forced adoption along a supply chain due to some market power. We saw a recent example of this with Walmart. Alternatively, as suggested by our model of the incentives at play in blockchain-based supply chains, third parties, such as consulting firms, might be required to coordinate and supply the technology necessary. If this is so, as our model would suggest, we will observe a new form of organisation to facilitate supply chain coordination: the V-form organisation [8].

Berg, Davidson and Potts recently introduced the V-form organisation as an "outsourced, vertically integrated organisation tied together not by management and corporate hierarchy but by a shared, distributed and decentralised ledger – a blockchain" [8]. Rather than a multidivisional (M-form) company where operations are divided into self-contained business units and overarching corporate hierarchy [21, 55], a V-form organisation is a decentralised organisation of fully independent companies both coordinating and auditing their activities through a decentralised blockchain ledger, and having a common coordinating third party, such as a consulting firm or technology company, who brokers that collaboration [see also 7]. In terms of our model above, we will observe *i* and *j* striking smart contracts written by *k* within a blockchain based ledger rather than within an organisation where verification occurs in a command-and-control hierarchy.

The institutional possibility of a V-form organisation represents a qualitative change in supply chain governance. Consensus over facts along a supply chain—including information about the attributes of goods—can now be achieved through outsourcing to a decentralised blockchain ledger, rather than relying on vertical integration. Previously supply chain trust has been provided by hierarchy in the form of the M-form organisation. Existing supply chain organisations now essentially face a wider range of institutional possibilities: making trust (through vertical integration), outsourcing trust (through market exchange), or now achieving trust though outsourcing to a network (through a common distributed ledger). Over time we anticipate a move towards the outsourcing of trust to a distributed ledger.

Shifts in economic power through reductions in information asymmetries

Information asymmetries exist along supply chains in both directions: producers lack information about where their goods are eventually sold, and consumers lack information about the provenance of the goods they buy. A reduction in information asymmetries shifts economic power towards the polar ends of supply chains.

Producers lack information over who the final market consumers are, the price(s) at which those goods are sold, the behaviour of actors along the chain, and how rents are distributed across the various actors. A coffee farmer in a remote area, for instance, might lack information other than the price at which they sell the coffee to an intermediary, including information about their consumers and final prices. This lack of information about goods as they move generates information asymmetries. We expect information asymmetries to increase as the distance between actors increases, including for consumers (e.g. insufficient or reliable information regarding the provenance of the product). Reducing these uncertainties and information asymmetries may dramatically alter the value they place on those products.

Information asymmetries persist in supply chains for several reasons. Supply chain participants might lack incentives to produce and maintain information about goods as they move. Notwithstanding issues of fraud or error there are a range of coordination problems that prevent supply chain information from being produced. Transaction costs might make producing the information economically unviable. Blockchain might better economise on these transaction costs while overcoming the incentive problems that cause

information asymmetries to persist. In terms of our model above, the information δ_j^i that *i* has about *j* upon which beliefs $\beta(\cdot)$ are based is stored in a blockchain which is designed to accumulate such information, and therefore is potentially of greater quantity and quality than the information δ_j^i that would be otherwise available to *i*.

If blockchain-based supply chains reduced information asymmetries we would expect shifts in economic power to the polar ends of the supply chain. Primary producers might gain bargaining power because they can identify final market customers (potentially enabling them to develop new patterns of trade and lower the rent of intermediaries). They therefore might be able to find more direct paths to market by better economising on the structure of a supply chain. Consumers, including those who are buying products as inputs into production, gain greater power along several dimensions. For instance, consumers might more easily restructure supply chains by dynamically switching between suppliers, and they might rely less on third-parties, such as restaurants, to provide verification of the characteristics of goods. The information produced through blockchain trade infrastructure might lead to greater competition between suppliers of similar goods regardless of existing trade relationships.

De-commoditising and disaggregating prices

Many goods in a modern economy are commoditised because of a lack of information to differentiate them from other goods. The prices consumers attach to those goods might not be fully reflective of their underlying (potential) value. One way to define a good is by its vector of attributes $x_{ij}=\{t_1 \ldots t_N\}$. Consumers observe those attributes to make subjective perceptions of the value of goods $v_i(x_{ij})$. For instance, a fresher perishable good might be worth more to consumers. Alternatively, a good that is simply located in a different physical location has a different value to a consumer. Keeping all else constant, the higher perceived value of a fresher good would translate to a higher market price. Furthermore, the vector of attributes defining a good changes through time (e.g. the good is damaged in transit). Information about attributes is shrouded in uncertainty and must be produced and maintained through different forms of economic organisation. The uncertainty about the good is particularly high when the information is not easily verifiable through third party observation of the good before or even after it is consumed (e.g. credence goods).

It is unnecessary for a consumer to have the theoretically complete set of vector characteristics that define a good because some of those characteristics will be unrelated to the formation of subjective value. Nevertheless, blockchain-based supply chain infrastructure means consumers might not only be able to access cheaper and more trustworthy information about the goods that they buy, but also more granulated and detailed information on previously unobservable characteristics. That is, information about the vectors of goods that were either not previously produced or not previously observable due to transaction costs might become possible.

There are several implications of blockchain-based supply chain infrastructure on the operation of market prices. First, we anticipate a *de-commoditisation of goods*. Two products that were previously considered identical because of a lack of information about their differing vectors of characteristics might now be reliably differentiated. Those products might fall into two different markets. The second order effect of this is potentially more granulated prices that are more closely reflective of the underlying physical good. That is, a *disaggregation of prices*, perhaps splitting existing markets into new markets of premium and non-premium segments. The precise margins at which additional trustworthy information will shift the price of goods will emerge over time, and will be directly related both to the subjective perceptions of consumers buying those goods, and the entrepreneurial efforts of people seeking to create the blockchain-based infrastructure that will produce and govern that information. Finally, to the extent that market prices represent the aggregation of distributed and contextual information of market participants [56], we would expect over the longer term more *effective market coordination*.

Fewer quality proxies

Consumers regularly rely on quality proxies. These proxies range from production within national borders to brand association and reputation. As blockchain supply chain infrastructure is built, however, we would expect that consumers rely more on the underlying characteristics of the specific good they are buying—because of the fall in transaction costs of producing that information—rather than proxies. A smart contract $p_{ij}(x_{ij})$ of the form we have considered above naturally lends itself to being made contingent upon the vector $x_{ij}=\{t_1 \ldots t_N\}$ of attributes that the good is verified to have, and can be designed to incentivise the provision of particular characteristics, rather than the consumer having to rely on proxies to inform choice between a range of simple contracts for goods.

A consumer seeking some minimum level of health and safety regulations, labour practices and food safety measures, may buy goods that are produced within national borders that have strict laws relating to those matters. The information that those proxies represent do not necessarily correlate directly with the characteristics of the product underlying it. This is not to say that either: (1) goods produced within those jurisdictions could possibly not meet those minimum

standards; or that (2) producers in jurisdictions without those standards might decide to voluntarily take sufficient health and safety or other measures. This observation also applies to other proxies and desired attributes, such as brand reputation. One function of brands is to signal to consumers that an organisation has ensured the quality of that product—effectively confirming information about its vector of characteristics. These examples of national borders and brand reputation are examples of governance solutions to the problem of producing trusted information about the characteristics of goods.

While proxies might be economically efficient given some level of transaction costs—that is, where it is too costly to produce more detailed information about specific goods—blockchain-based supply chains might enable consumers to better contract for the supply of the underlying attributes of goods such as in the way we have modelled above. As proxies are replaced by more specific information about goods, then consumers will shift their consumption patterns—purchasing goods that more closely fit the criteria they are seeking. In the longer run this may change the goods that are produced in certain nations. Producers within economies who were previously held back by reputational problems—for instance, in developing economies which are beset by poor food safety reputations—might be better able to market their products to consumers using more detailed information. Furthermore, we would expect this to shift the production patterns of goods to more closely match the comparative advantages of economies.

Conclusion

We have made several contributions. First, we have outlined the potential of blockchain as economic infrastructure for the production and governance of information along supply chains. Second, we have modelled the necessary conditions for there to be incentives for such infrastructure to be built. Third, we propose that the building of this blockchain infrastructure might lead to new forms of economic organisation such as the V-form organisation, a shifting of economic power to the polar end of supply chains due to reductions in information asymmetries, the de-commoditisation of goods and the disaggregation of prices that assist market coordination, and reductions in the use of proxies used by consumers to value goods. In this way blockchain-based supply chain infrastructure won't just make existing supply chains cheaper and more efficient, but might fundamentally change the way that globalisation takes place.

References

[1] D. W. E. Allen, C. Berg, S. Davidson, M. Novak, and J. Potts, "Blockchain TradeTech," presented at the APEC Study Centres Consortium Conference (ASCCC), Port Moresby, Papua New Guinea 14-15 May 2018, 2018.

[2] M. Levinson, The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger - Second Edition with a new chapter by the author. Princeton University Press, 2016.

[3] R. Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," The JBBA, vol. 1, no. 1, p. 3712, 2018.

[4] S. R. Davidson, P. De Filippi, and J. Potts, "Blockchains and the Economic Institutions of Capitalism," Journal of Institutional Economics, pp. 1-20, 2018.

[5] T. J. MacDonald, D. W. E. Allen, and J. Potts, "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking," in Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century, P. Tasca, T. Aste, L. Pelizzon, and N. Perony, Eds. Cham: Springer International Publishing, 2016, pp. 279-296.

[6] C. Berg, "What Diplomacy in the Ancient Near East Can Tell us About Blockchain Technology," Ledger, vol. 2, pp. 55-64, 2017.

[7] C. Berg, S. Davidson, and J. Potts, "Outsourcing vertical integration: introducing the V-form network," Medium, 2018.

[8] C. Berg, S. Davidson, and J. Potts, "Outsourcing Vertical Integration: Distributed Ledgers and the V-form Organisation," ed. RMIT University Working Paper, 2018, pp. 1-10.

[9] C. Berg, S. Davidson, and J. Potts, "Ledgers," SSRN, 2018.

[10] J. C. Scott, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. Yale University Press, 1998.

[11] W. Sombart, Der moderne Kapitalismus. Duncker & Humblot, 1902.

[12] J. R. Commons, The Legal Foundations of Capitalism. New York: Macmillan, 1924.

[13] J. R. Commons, "The problem of correlating law economics and ethics," Wis. L. Rev., vol. 8, p. 3, 1932.

[14] R. H. Coase, "The nature of the firm," economica, vol. 4, no. 16, pp. 386-405, 1937.

[15] O. E. Williamson, Markets and hierarchies, analysis and antitrust implications: a study in the economics of internal organization. Free Press, 1975.

[16] O. E. Williamson, The economic intstitutions of capitalism.

NY: Free Press, 1985.

[17] K. J. Arrow, "The organization of economic activity: issues pertinent to the choice of market versus nonmarket allocation," The analysis and evaluation of public expenditure: the PPB system, vol. 1, pp. 59-73, 1969.

[18] H. A. Simon, Models of Man. New York: Wiley, 1957.

[19] H. A. Simon, Administrative Behavior, 2nd ed. New York: Macmillan, 1961.

[20] O. E. Williamson, "Comparative economic organization: The analysis of discrete structural alternatives," Administrative science quarterly, pp. 269-296, 1991.

[21] O. E. Williamson, The Mechanisms of Governance. Oxford University Press, 1996.

[22] S. P. Kulkarni and K. C. Heriot, "Transaction costs and information costs as determinants of the organizational form: A conceptual synthesis," American Business Review, vol. 17, no. 2, p. 43, 1999.

[23] C. Berg, S. Davidson, and J. Potts, "Blockchains industrialise trust," SSRN, 2017.

[24] C. Berg, S. Davidson, and J. Potts, "The Blockchain Economy: a beginner's guide to institutional cryptoeconomics," in Medium, ed, 2017.

[25] A. Berg, C. Berg, S. Davidson, and J. Potts, "The institutional economics of identity," SSRN, 2017.

[26] D. W. E. Allen, C. Berg, A. M. Lane, and J. Potts, "Cryptodemocracy and its institutional possibilities," The Review of Austrian Economics, pp. 1-12, 2018.

[27] D. Petropoulou, "Information costs and networks in international trade," London, CEPR, 2005.

[28] D. Hummels, "Transportation Costs and International Trade in the Second Era of Globalization," Journal of Economic Perspectives, vol. 21, no. 3, pp. 131-154, 2007.

[29] J. Goldstein, "International institutions and domestic politics: GATT, WTO, and the liberalization of international trade," in The WTO as an international organization, A. O. Krueger, Ed., 1998, pp. 133-152.

[30] A. Banet, "Organizational Distance: A Concept for the Analysis and Design of Organizations," Group & Organization Studies, vol. 1, no. 4, pp. 496-497, 1976.

[31] T. Clarke and M. Boersma, "The governance of global value chains: Unresolved human rights, environmental and ethical dilemmas in the apple supply chain," Journal of Business Ethics, vol. 143, no. 1, pp. 111-131, 2017.

[32] J. Linshi, "Why U.S. Sanctions Mean Some Countries Don't Get Any iPhones," in Time.com, ed, 2014.

[33] A. Awaysheh and R. D. Klassen, "The impact of supply chain structure on the use of supplier socially responsible practices," International Journal of Operations & Production Management, vol. 30, no. 12, pp. 1246-1268, 2010.

[34] G. Gereffi, J. Humphrey, and T. Sturgeon, "The governance of global value chains," Review of international political economy, vol. 12, no. 1, pp. 78-104, 2005.

[35] T. Groenfeldt, "IBM And Maersk Apply Blockchain To Container Shipping," in Forbes, ed, 2017.

[36] N. Popper and S. Lohr, "Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?," in The New York Times, ed, 2017.

[37] IBM, "Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain," ed, 2017.

[38] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?," in Hamburg International Conference of Logistics (HICL), Hamburg, 2017, pp. 2-18.

[39] V. Grover and M. Malhotra, "Transaction cost framework in operations and supply chain management research: theory and measurement," Journal of Operations Management, vol. 21, no. 4, pp. 457-473, 2003.

[40] D. C. North, Institutions, institutional change and economic performance. Cambridge University Press, 1990.

[41] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," International Journal of Research in Engineering and Technology, vol. 5, no. 9, pp. 1-10, 2016.

[42] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in Service Systems and Service Management (ICSSSM), 2016 13th International Conference on, 2016, pp. 1-6: IEEE.

[43] S. Underwood, "Blockchain beyond bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15-17, 2016.

[44] S. Apte and N. Petrovsky, "Will blockchain technology revolutionize excipient supply chain management?," Journal of Excipients and Food Chemicals, vol. 7, no. 3, p. 910, 2016.

[45] T. K. Mackey and G. Nayyar, "A review of existing and emerging digital technologies to combat the global trade in fake medicines," Expert opinion on drug safety, vol. 16, no. 5, pp. 587-602, 2017.

[46] W. J. Sutherland et al., "A 2017 horizon scan of emerging issues for global conservation and biological diversity," Trends in

Ecology & Evolution, vol. 32, no. 1, pp. 31-40, 2017.

[47] Walmart, "In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens," ed, 2018.

[48] P. De Filippi and A. Wright, Blockchain and the Law: The Rule of Code. Harvard University Press, 2018.

[49] H. M. Kim and M. Laskowski, "Toward an Ontology-driven Blockchain Design for Supply-chain Provenance," Intelligent Systems in Accounting, Finance and Management, vol. 25, no. 1, pp. 18-27, 2018.

[50] R. Mohan, P. Patil, and I. Rajesh, "PRIORITY ROUTING OF SHIPMENT USING IOT SENSOR DATA FROM SHIPMENT PACKAGES," 2018.

[51] N. Szabo, "The idea of smart contracts," Nick Szabo's Papers and Concise Tutorials, 1997.

[52] K. J. Lancaster, "A new approach to consumer theory," Journal of political economy, vol. 74, no. 2, pp. 132-157, 1966.

[53] D. S. Ironmonger, New commodities and consumer behaviour. Cambridge: Cambridge University Press, 1972.

[54] O. E. Williamson, The Economic Institutions of Capitalism. NY: Free Press, 1985.

[55] A. D. Chandler, Strategy and Structure: Chapters in the History of the Industrial Enterprise. M.I.T. Press, 1962.

[56] F. A. Hayek, "The Use of Knowledge in Society," The American Economic Review, vol. 35, no. 4, pp. 519-530, 1945.

[i] Transactions costs in general refer to the 'friction' inherent in exchange [16] and are the "costs of running the economic system" [17].

[ii] Bounded rationality was first proposed by Simon [18] and refers to the cognitive and language based limits of rationality; economic actors are "intendedly rational, but only limitedly so" [19]. Opportunism in contrast refers to the way in which economic actors are generally guided by self-interest, and may act to selectively reveal, obfuscate, or otherwise manipulate information to their advantage; opportunism is what Williamson [16] refers to as "self-interest seeking with guile".

[iii] For instance, asset specificity ranges from uniquely idiosyncratic investments where those investments would be lost if the relationship was to be severed, to more general purpose investments that are more easily redeployed to other uses. Frequent and similar transactions are "often associated with internalization of economic activities" [22] in a hierarchical governance structure like a firm such that establishment costs can be amortised.

Photo by Renan Kamikoga on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-1-(6)2019

Parameters for building sustainable Blockchain Application Initiatives

Lewis Laidin, Kassandra A. Papadopoulou, Nathan A. Dane
Blockchainers CIC and The University of Manchester, UK
Correspondence: lewislaidin@gmail.com
Received: 15 January 2019 **Accepted:** 6 February 2019 **Published:** 8 April 2019

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
LL, KP and ND designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
The authors acknowledge Dr. Christos-Efthymios Kotselidis, SupplyBlockchain, Inc., Dr. Jane Thomason, Dr. Naseem Naqvi, The British Blockchain Association, Anton Hristoff, Cornell University, Deloitte, KPMG, IBM, PricewaterhouseCoopers, Grant Thornton, Nicholas Joan Vermeulen, Sebastian Cochinescu, Matthew Lucas, Oraclize, Thomas Bertani, ConsenSys, Loubna Hadid, Bruce Silcoff, Adam Chidgey, Sara Simeone, Cygnetise, Steve Pomfret, Simon Herko, IBISA, Medici Ventures and others who chose to be anonymous for their participations towards the study for this paper and Manchester Enterprise Centre, Dr. Martin Henery for the continuous support that makes this paper possible.

Abstract

Despite the demand and interest for the blockchain technology, there are still major challenges for blockchain application initiatives (projects and ventures) to be sustainable and reliable. While starting a non-blockchain initiative already comes with its own sets of challenges and has around 50% failure rate, starting a blockchain initiative rises the rate to 90% due to additional variables and confusion on top of this. Such a situation deters innovators and eventually dampens innovation, requiring priority for actions. This paper attempts to contribute by compiling and outlining the various key variables to be considered, as a set of parameters for blockchain initiators. Through secondary data collection: literature reviews, report studies and primary data collection: interventional and observational case study, interviews with blockchain researchers, businesses and entrepreneurs, this paper categorises variables into blockchain-related and business-related categories, outlining consideration points for each of the variables. By summarizing and integrating the variables and referring to theories of innovation and adoption, it is concluded that concept validation entailing both initiative feasibility and user-demand, is of key importance for blockchain innovations.

Keywords: *blockchain, business, initiatives, challenges, barriers, parameters, feasibility, concept*
JEL Classifications: *D04, D07, D08, I07, O03, Y04*

1. Interest Vs Progress

Blockchain is a type of distributed ledger technology (DLT) which has garnered a lot of attention in the past few years from researchers to business and governments. According to the Deloitte 2018 Global Survey [1], more than 80% of companies in Canada, China, France, Germany, Mexico, UK either have blockchain projects in production or have production plans for 2019. Looking beyond companies, government are exploring this technology, the UAE Government is leading the wold's first blockchain powered government initiative, including the 'smart Dubai' initiative, and launched the 'Emirates Blockchain Strategy 2021', where they aim to exploit the technology and to transform 50% of government transactions into the blockchain platform in the next three years [2]. It should be noted that there are no International Standards in place presently for the standardisation of blockchain and distributed ledger technologies, however there is a process for that in place [3]. In the UK, the Financial Conduct Authority (FCA) for example has accepted 29 blockchain businesses for their fourth sandbox cohort, accounting for more than 40% of the total numbers with the attempt to explore suitable regulatory approaches [4].

Contrary to the amount of interest from various stakeholders, according to Gartner Hype Cycle, developed by the Gartner information technology research company, blockchain has gone down from the Peak of Inflated Expectations to the Trough of Disillusionment [5]. This can also be seen from the Deloitte's report where 39% respondents say that blockchain is overhyped and the drop in global cryptocurrency market taking place at the time of writing. There are various explanations for the contrast of interest versus progress including the availability of required resources, technological capability and limitation, ecosystem support and even lack of compelling applications. Although discussing & determining the root causes are not in the scope of this paper, all the points above lead to possibilities of failed blockchain initiatives or in other words, lack of practical use-cases which can add doubts about the technology and therefore can be seen in the hype cycle.

The next phase in the Gartner Hype Cycle is called Slope of Enlightenment which is described as "More instances of how the technology can benefit the enterprise start to crystallize and become more widely understood. Second and third generation products

appear from technology providers." [6]. With the level of interest remaining, blockchain technology is well placed to make progress from the current downwards phase towards the next upwards phase by understanding how to get to the next phase and what is blocking the progress. By making it a priority to compile and understanding some barriers that impede the success of blockchain initiatives, not only efforts can be better directed so that challenges can be gradually overcome, but they also help innovators to invent by being aware of the possible challenges and consideration points, so time and investment risks can be strategically planned. With less amount of wasted resources from innovators, it can also prevent creating more doubts from the society, allowing interests to continue growing.

2. Methodology

This paper, which draws contents from a postgraduate research project, summarises critical barrier points that will be useful for blockchain initiatives to consider early on. As blockchain initiatives can be businesses or projects, consideration points for venture-related variables are briefly pointed out while focusing on blockchain-related variables. Through literature review, challenging points for blockchain initiatives are initially gathered and categorised into a set of 38 hypotheses. The points were then selected further via primary data collection through interviews with researchers, businesses and entrepreneurs in the blockchain industry with 1-6 years of experience, totalling 12 participants. Individual interviews were chosen to allow constructivism approach to gather and interpret various views and opinions from participants. Participants chose their areas of expertise to comment on and were asked in the format of open-ended questions to allow commentaries, if in their opinion, the relevant hypotheses are challenges for blockchain initiatives. Their answers and commentaries were analysed to validate the hypotheses. The results of this small-scale qualitative study are written in this paper but due to the scope and space limitation, the set of hypotheses, participant information, result and analysis as well as participation information sheet, consent form and interview questions are not included. However, for ease, the resulting set of consideration points are put together as a checklist and is included in the Appendix of this paper.

3. Consideration parameters for blockchain initiatives

3.1 Blockchain parameters

This section includes barrier points that blockchain initiatives might face in relevance to their usages of blockchain technology. The points gathered in the literature review were first categorised together which were then used in the individual interviews as described in the methodology brief above. This includes data audit, scalability, societal, regulation, governance, operational, security and privacy.

3.1.1 Blockchain data audit

This section includes barrier points that blockchain initiatives might face in relevance to their usages of blockchain technology. The points gathered in the literature review were first categorised together which were then used in the individual interviews as described in the methodology brief above. This includes data audit, scalability, societal, regulation, governance, operational, security and privacy. Even if transactions are validated through blockchain itself, there is still a possibility for data tampering especially in private and consortium blockchains where the quantities of nodes responsible for verifying are limited in general if compared to public blockchain. This means that there is a need for auditing to make sure that the blockchain is functioning as intended. It is important to consider if the project requires real-time transaction analysis and if system auditing is required. Data read from blockchain might have latency and not be 100% real-time [7]. According to Interactive Advertising Bureau (IAB) guidelines for example, data timeliness for real-time auctions must be less than 100 milliseconds [8]. There are two reasons for latency, first being that at any given time, a node might only get the version of the data that is given to it while other nodes might yet receive the most recent version of the data. The second reason is that there is a possibility for every transaction that the network of nodes agrees on different sets of data, creating a fork [9]. Whereas if auditing the system is required so that it is running as intended, including for example if participants are behaving as they should, or if data is managed and transacted appropriately, the auditor's technical capability needs to be taken in consideration.

3.1.2 Scalability

Blockchain scalability issues can be related with two main metrics which are transaction throughput and latency. The first one refers to transaction per second while the latter one refers to transaction confirmation and propagation time [10]. Trade□offs between different approaches are made towards scalability, security or decentralisation. For example, to improve security, there is a possibility of pegging into the Bitcoin network, but with the result of having lower scalability, and improvement of security is debatable. Some opt to forgo decentralisation in improving security and scalability by choosing permissioned ledgers with closed participants [10]. It is therefore important to consider beforehand if the public decentralisation is required as well as if immediate high throughput is required for the initiatives. Further, as different consensus mechanisms make different assumptions, it is important to consider

one that suits the initiatives.

3.1.3 Societal elements

Points worth consideration relevant to this subsection include technology awareness, skills, control and accessibility. For any blockchain initiatives, it is important to consider if the target users or audiences have the required technical awareness and capability [11]. Blockchain initiatives also should plan so that target users or audiences have the necessary level of accessibility required, whether it is technical such as internet access or non-technical such as government authorisations [12]. Different and rare skill-sets might also be needed including cryptographers, lawyers or even social experts depending on the blockchain architecture. It is also important to consider the viability in terms of willingness to cooperate from industry partners as blockchain is a technology that also shifts control power in general [11].

3.1.4 Regulation

Some countries have regulation first, business second approach while others such as in East-Asia have approach the other way around therefore complying with regulatory approaches can vary. In general, however, it is important to analyse the relevant regulatory approaches particularly if digital currencies or Initial Coin Offerings (ICOs) are involved, or if traditional securities are involved. Even though the UK regulatory approach towards blockchain technology seems to be non-prohibiting as for example, the FCA remains open to the process and technology if the result is protected and risk is mitigated [4], digital currencies face regulatory questions in terms of their security status, and which activities are legally allowed as well as the imposes on various jurisdictions. As regulatory landscape is constantly changing and can be uncertain, preparing steps to have sufficient legal assurances can be crucial.

3.1.5 Governance

Blockchain provides and requires possibilities of new governance structure and different governance models are still being tested and developed [13]. Success rate can be increased if blockchain initiatives consider ahead how to make sure future upgrades as well as how future governance model changes can be introduced. This is because governance involves the decision-making processes related to the management of the system protocol, in this case, blockchain protocol, including creation, update or abandoning of rules pertaining smart contracts, fees, conflict resolutions, roles of participants [14]. Making plans so that future upgrades and changes can be done efficiently will prevent network issues and therefore maintain system operations which involves various and numerous participants. Relevant to this, it is also important to consider how to sufficiently incentivise network participants for the sustainability of the network [7]. If disputes among participants happen, it is also worth considering how such issues can be settled in a timely and efficient manner. For consortium governance, on top of the internal blockchain governance, it is important to also manage governance among participants. This is because a consortium is normally business-related, and counterparties will have different priorities due to the possibility of relation to profit and loss of their businesses. Further, as a starting consortium, it is worth keeping the number of parties manageable as too few can be unappealing while too many can be challenging to govern.

3.1.6 Operational

Interoperability can be a major challenge which can be solved through early planning. For blockchain initiatives that require interoperability with existing IT systems such as an Enterprise Resource Planning (ERP) or Customer Relationship Management (CRM), it needs to be considered how these systems can exist and be interoperable from the beginning. This can be further complicated when different businesses and organisations are required to interoperate if they are using different and complex systems. It is also important to consider if interoperability with other blockchain systems, including reliance of information between one to another, is required for the initiatives as different blockchain systems might have vastly different architectures and functionality. As blockchain is not currently the most efficient way to store data [15], it is worth considering if the system initiatives require a high volume of storage in the future. While some systems allow running on top of existing infrastructure, most will require additional infrastructure, potentially including specialised hardware devices. It is therefore important to also consider if additional infrastructure is required for the blockchain system to operate as intended.

3.1.7 Security

As with most technology, security is a constantly improving matter. For blockchain technology, it helps to know beforehand if private keys are going to be stored in mobile and computer devices as they provide entry points where security breaches can happen. As third-party integrations increase the number of security variables to account for, requiring plenty of them can create challenges and is worth considering early in the design process [16]. Blockchain initiatives should also determine if their system will be written in a Turing-Complete language, as it allows for more functionality but at the same time opening more possibility for vulnerabilities. Penetration tests, especially for blockchain systems, are crucial in terms of security as

they allow attack vectors to be discovered. Further, with options available for using the services of freelancers, contractors or agencies to develop the system, it helps to determine if the code will be written and maintained by a trustworthy party.

3.1.8 Privacy

Privacy issues are a major barrier towards the public acceptance and mass adoption of blockchain applications [17]. There are situations where elements of transparency in blockchain can have negative impacts and this is especially true if the information involved is sensitive or personally identifiable data such as medical, financial or governmental [18]. It is therefore important to consider beforehand if the initiatives are dealing with sensitive data and if it is required to share personal data with other third parties. It is important to note that personal data might include hashes, transactions and or other personally identifiable information [19]. On top of the matter of user preferences, privacy is also affected by the regulatory policies such as General Data Protection Regulation (GDPR). According to GDPR, it is important in general for blockchain initiatives to consider how to implement and allow a 'right for erasure' policy for personal data.

3.2 Business parameters

This section briefly points out the barriers that blockchain initiatives might face. These points were gathered and categorised from the commentaries from blockchain businesses and entrepreneurs in the individual interviews described in the methodology brief above on what some challenges for their blockchain initiatives are. This includes funding, market needs, team, marketing, feasibility and implementation, legal and regulatory. This section contains lesser focus than the previous section as the parameters pointed out below were gathered from participant commentaries rather than initialised by literature review but were included in this paper due to its relevance. Also, the focus of this paper is on blockchain parameters leaving business parameters to be explored in more details in further work.

3.2.1 Funding

With options to choose from token offerings, venture capital firms, angel investors and other funding routes, it is important to create a plan detailing the steps towards how necessary funding can be obtained for the venture.

3.2.2 Market needs

While the general approach caused by the inflated hype for blockchain technology is to offer solutions to a problem, it is important for blockchain initiatives that want to be sustainable to find and ensure market needs.

3.2.3 Team

As an emerging technology, talent with the necessary skillsets can be a challenge to find, therefore it helps to consider how to find the right team for the business venture.

3.2.4 Marketing

Marketing strategy and its message, audience and timing are crucial, especially for blockchain initiatives that are targeting end-users as their audiences. This can be relevant to how the technology might be seen as a hype and requires communication and presentation that appeals to target audiences.

3.2.5 Feasibility and Implementations

It is important to consider how feasible a blockchain initiative is, which the parameters in this paper should help determine by providing an initial gauge, and how to implement, including mitigations for future challenges and risks.

3.2.6 Legal and regulatory

With the legal and regulatory landscape constantly changing, it is important to closely refer to the relevant approaches and consider how to be compliant.

4. Conclusion

Observations and analysis process are not included in this paper due to space limitation, hence their summaries are reflected in the paper in the form of the written parameters above. The parameters aim to help blockchain projects that are still in the initial stages, to promote early considerations so that unnecessary resources can be avoided but at the same time directed efforts can be put in. Ongoing projects, however, might still be able to benefit from the parameters when for example re-prioritising. Journal and article sources are used as much as possible, but as some blockchain research and development are done mostly by individual developers, researchers and companies, it is to be noted that company reports and, in some cases, blogs are also used. Due to time-limitation and the lack of established standardisation in the blockchain industry, only a small sample size of participants was collected. This means that the findings in this study are partly-limited by views and opinions of the participants and by the literature review conducted. As the interest and demand for blockchain technology improves however, there will be more opportunities to work with established researchers and industry leaders to further validate the barrier points written in this paper. Future work that attempts to further validate the points in larger sample

size and in different stages of the technology maturity, as well as work that covers business variables above in more details will allow this paper to serve better in supporting blockchain initiatives.

By consulting the Diffusion of Innovation (DOI) theory by E.M. Rogers [20], [21] which explained how an innovation gains adoption through a specific population spread, it can be said that adoption must start with the individual making choices to accept a certain innovation, before spreading to market level, creating diffusions. This means that offering working blockchain solutions for problems of individuals is useful to give blockchain technology an adoption momentum. It can then be concluded that among the parameters listed in the paper, individual or market needs as well as feasibility should be the main considerations for blockchain initiatives and the technology.

Appendix

BLOCKCHAIN IMPLEMENTATION REQUIREMENT CHECKLIST

C (C1,C2,C3, etc) refers to the term 'Checklist'
C1: Is real-time transaction analysis required?
C2: Is system auditing required?
C3: Are control variables to be audited and analysed determined from the beginning?
C4: Is it required to be publicly decentralised?
C5: Is high throughput required in the immediate future?
C6: Is fitting consensus-mechanism chosen and used?
C7: Does the target audience require technological capacity?
C8: Are specialised skill-sets required?
C9: Will institutions and organisations be required to fully give up control?
C10: Do the target audiences have the necessary relevant level of accessibility?
C11: Are there any digital currencies or ICO involved?
C12: Are there any traditional securities involved?
C13: Is it under supportive jurisdicitons?
C14: Is there sufficient legal assurances?
C15: Can future system upgrade be done efficiently?
C16: Can future governance model be improved and changed efficiently?
C17: Are participants incentivised sufficiently?
C18: Can issues and disputes be settled in a timely and efficient manner?
C19: For consortium, is consortium governance model put in place?
C20: For consortium, is the starting participant numbers more than 5 and less than 50?
C21: Is interoperability with existing IT system required?
C22: Are there plenty of cooperations with other businesses required?
C23: Is interoperability with other blockchain systems required?
C24: Is high storage required in the near future?
C25: Is additional infrastructure required?
C26: Is it required for private keys to be stored in mobile and computer devices?
C27: Are plenty of third party integrations required?
C28: Will it be written in Turing-Complete language?
C29: Is penetration test done and passed?
C30: Is the codebase written by trustworthy party?
C31: Does the case deal with sensitive data?
C32: Is it required to share personal data with other third parties?
C33: Does it comply with Data Protection Act for personal data?
C34: Does it comply with GDPR?

Disclaimer

Please remember that this list produces nothing more than an evaluation, and serves not more than a guide or framework. The framework relates to implementation, but does not include business feasibility which covers business-case related variables such as market needs, funding, management team among others.

It is out of the scope of this framework to suggest potential directions. The framework can be used in collaboration with relevant consultant or specialist to create lists of potential directions.

This framework may be updated in the future as the area develops. You should not rely on this framework as legal advice.

References

[1] Deloitte, "Deloitte's 2018 global blockchain survey", 2018. [Online] Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf. Accessed on: Jan. 3, 2019.

[2] United Arab Emirates Government, Emirates Blockchain Strategy 2021, 2018. [Online]. Available: https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021. Accessed on: Jan. 10, 2019.

[3] International Organization for Standardization, ISO/TC 307 Blockchain and distributed ledger technologies, 2019. [Online]. Available: https://www.iso.org/committee/6266604.html. Accessed on: Jan. 10, 2019.

[4] Financial Conduct Authority, "Regulatory sandbox - cohort 4", 2018. [Online]. Available: https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-4-businesses. Accessed on: Jan. 5, 2019.

[5] Gartner, "Gartner Identifies Five Emerging Technology Trends That Will Blur the Lines Between Human and Machine", 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-08-20-gartner-identifies-five-emerging-technology-trends-that-will-blur-the-lines-between-human-and-machine Accessed on: Jan. 5, 2019.

[6] Gartner, "Hype Cycle Research Methodology", 2018. [Online]. Available: https://www.gartner.com/en/research/methodologies/gartner-hype-cycle. Accessed on: Jan. 3, 2019.

[7] I. Aldridge and S. Krawciw, "Real-time risk: What Investors Should Know About FinTech, High-Frequency Trading, and Flash Crashes", 1st ed. John Wiley & Sons, 2017, p. 30-40.

[8] Interactive Advertising Bureau, "Programmatic Trading: An IAB Europe White Paper", 2014. [Online]. Available: https://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf. Accessed on: Jan. 10, 2019.

[9] E. Ben, K. Brousmiche, H. Levard and E. Thea, "Blockchain for Enterprise: Overview, Opportunities and Challenges", 2017. [Online]. Available: https://www.researchgate.net/publication/322078519_Blockchain_for_Enterprise_Overview_Opportunities_and_Challenges. Accessed on: Jan. 10, 2019.

[10] S. Bano, M. Al-Bassam and G. Danezis, "The Road to Scalable Blockchain Designs", Shehar Bano, 2017. [Online]. Available: https://sheharbano.com/assets/publications/usenix_login_2017.pdf. Accessed on: Jan. 5, 2019.

[11] Deloitte, "Blockchain Enigma. Paradox. Opportunity", 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf. Accessed on: Jan. 3, 2019.

[12] W. Al-Saqaf and N. Seidler, "Blockchain technology for social impact: opportunities and challenges ahead", Journal of Cyber Policy, vol. 2, no. 3, pp. 338-354, 2017. Available: 10.1080/23738871.2017.1400084. Accessed on: Jan. 10, 2019.

[13] F. Niederman, R. Clarke, L. Applegate, J. L. King, R. Beck, and A. Majchrzak, "IS Research and Policy: Notes From the 2015 ICIS Senior Scholar's Forum", Communications of the Association for Information Systems: Vol. 40, Article 5, 2017. [Online]. Available: http://aisel.aisnet.org/cais/vol40/iss1/5. Accessed on: Jan. 10, 2019.

[14] L. Bosankic, "Blockchain governance: takeaways from nine projects", Medium, 2018. [Online]. Available: https://medium.com/@leo_pold_b/blockchain-governance-takeaways-from-nine-pr ojects-8a80ad214d15. Accessed on: Jan. 10, 2019.

[15] D. Treat, L. McGraw, C. Helbing and C. Brodersen, "Blockchain Technology: Preparing for Change", Accenture, 2015. [Online]. Available: https://www.accenture.com/t20160608T052656__w__/us-en/_acnmedia/PDF-5/Accenture-2016-Top-10-Challenges-04-Blockchain-Technology.pdf. Accessed on: Jan. 10, 2019.

[16] M. Orcutt, "Blockchain could be the key to revolutionizing our energy grid", MIT Technology Review, 2017. [Online]. Available: https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid. Accessed on: Jan. 5, 2019.

[17] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", 2016 IEEE Symposium on Security and Privacy (SP), 2016. Available: 10.1109/sp.2016.55. Accessed on: Jan. 5, 2019.

[18] S. Goldfeder, H. Kalodner, D. Reisman and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies", Proceedings on Privacy Enhancing Technologies, vol. 2018, no. 4, pp. 179-199, 2018. Available: 10.1515/popets-2018-0038. Accessed on: Jan. 10, 2019.

[19] W. Maxwell and J. Salmon, "A guide to blockchain and data protection", Hogan Lovells, 2017. [Online]. Available: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf. Accessed on: Jan. 3, 2019.

[20] E. Straub, "Understanding Technology Adoption: Theory and Future Directions for Informal Learning", Review of Educational Research, vol. 79, no. 2, pp. 625-649, 2009. Available: 10.3102/0034654308325896. Accessed on: Jan. 10, 2019.

[21] W. W. LaMorte, "Diffusion of Innovation Theory", School of Public Health - Boston University, 2018. [Online]. Available: http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories4.html. Accessed on: Jan. 10, 2019.

Photo by Jorge Vasconez on Unsplash

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-1-(7)2019

The Application of Behavioural Heuristics to Initial Coin Offerings Valuation and Investment

Maxwell Stanley
University of Essex, UK
Correspondence: maxamus.stanley@gmail.com
Received: 20 March 2019 **Accepted:** 29 March 2019 **Published:** 12 April 2019

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgements:
MS would like to thank Dr. Ahrash Dianat - MSc Supervisor University of Essex, Navroop Sahdev – MIT and Halla Al-Razouq

Abstract

Blockchain projects have seen a rush of investment in the form of Initial Coin Offerings (ICOs) in 2016 and 2017, yet little is understood about how to valuate these projects. This research explored the application of behavioural heuristics to ICO valuation and investing. Identified were six variables that may impact investment decision making due to key behavioural biases. These variables - coin value, market capitalisation, ease of understanding, market sentiment, maximum ICO bonus level, and pre ICO social media levels - were analysed using Pearson's Correlation against return on investment (ROI). The data was collected from numerous ICO websites and Twitter. Fundamental analysis was taken from Coincheckup due to it being a major source of information for many retail investors and using a well-defined methodology. Sentiment data was collected from Twitter and assessed using Crimson Hexagon's social sentiment analysis tool. Ease of understanding was evaluated using AWS Blockchain business canvas. All information was compiled into a single dataset and the top 47 projects in terms of ROI were utilised for this research. Ease of understanding was found to be significantly correlated with ROI. Ease of understanding was then combined with fundamental analysis to develop a hybrid model of evaluation for cryptocurrency projects. This model substantially outperformed fundamental analysis alone, with a 33.6% improvement on ROI. In conclusion, current methods of fundamental analysis for blockchain projects are an inadequate method for capturing their full potential future value. Investors lacking appropriate tools and with limited knowledge and experience - along with the relatively recent advent of cryptocurrencies - are being influenced by behavioural factors such as ease of understanding. It is therefore important that investors and entrepreneurs alike take such factors into consideration.

Keywords: *blockchain, behavioural economics, behavioural heuristics, ICO, cryptoeconomics, tokenomics*
JEL Classifications: *D02, D71, H11, P16, P48, P50*

1. Introduction

Before any business launches an ICO, they have two economic concerns: their cryptoeconomics and their tokenomics. Any factor that is likely to affect these economic concerns needs to be considered during the development phase. This research will argue that behavioural heuristics, rules of thumb that investors may utilise will impact price action in secondary markets. Where applicable, evidence from stock investing, venture capital investing and crowdfunding will be provided. It will clearly state why these heuristics may be particularly powerful in the cryptocurrency market, how these behaviours manifest, and how investors can take advantage of this information to improve their returns.

1.1 Cryptoeconomics & Tokenomics

The success of a blockchain comes down to its ability to incentivise the users of that network. To incentivise users, Blockchain projects use a randomised reward mechanism secured via cryptography. This is Cryptoeconomics.

Tokenomics is directly related to the liquidity of the system. Its function is to find the optimum point at which the short-term financial utility of a token intersects with the long-term utility of a token. This will directly impact the number of tokens there should

be in the system. In the short-term, when there is a very limited application for the tokens, there needs to be a financial incentive incentive for an individual to invest. However, if the price were to continually increase, there would be limited incentive for an individual to use that token on the network rather than speculate on it as an investment. If behavioural heuristics play a role in the formation of token price, then they need to be incorporated into your tokenomics to ensure the long-term success of a blockchain project.

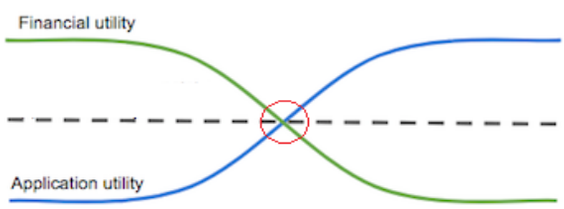


Figure 1. A graphical depiction of the intersection of application utility and financial utility as time progresses

2. Literature Review

2.1. Heuristics

Tversky and Kahneman [1], leaning on decades of psychological research, suggested that in complex decision-making situations individuals will use heuristics to ease the cognitive complexity of the task. Whilst these heuristics are a necessity in order to navigate the complexities of life, they are inherently prone to errors and biases.

There are four key general heuristics:

2.1.1. Affect, as argued and tested by Finucane et al [2]:

This is a reliance on the initial feeling experienced, or our intuitive judgement. As the decision we are presented with increases in complexity, our reliance on this initial intuitive judgement increases. Our reliance on it is also increased when presented with time constraints.

2.1.2. Representativeness

This is our tendency to assume individual characteristics to be representative of the whole regardless of whether those characteristics actually relate to the whole.

2.1.3. Availability

This is our tendency to make a decision based on the most salient information. This results in an overweighting of more recent information and the most extreme factors

2.1.4. Anchoring and Adjustment

When making a judgement, decision-makers often use an initial value and adjust away from it accordingly. Often this initial value - the Anchor - can lead to a biased judgement.

Each of these heuristics can lead to a number of systematic biases which can impact investment decisions within the cryptocurrency market.

2.2. Affect

Affect [3] is the reliance on a positive or negative feeling toward a stimulus. Lemmon and Portniaguina [4] found that forecasts of consumer confidence in "affect" predicted returns for the 25 years post-1977. They concluded that this was due to the increase in household investors, suggesting that when the expertise of the investor is low, behavioural biases played a larger role in an investor's ROI.

This is not dissimilar to the cryptocurrency market, which has a high percentage of household investors. Bollen [5] showed how social media data, namely Twitter, can be used to elicit sentiment. He found it can be accurately used to predict changes in the Dow Jones Industrial Average. Slovic et al. [6] refer to an "affect pool," or a collection of all the positive and negatively tagged associations. A similar approach is taken here with the ratio of positive to negative Twitter postings.

2.3. Herding

Some of the most salient information for investors is the most recent price action. A stock could be in demand and have seen its price rise in the previous period or investors could be selling that stock, resulting in a price drop. Researchers have found that market demand, rather than the expectations of fundamental value, influence demand [7]. Banerjee [8] was one of the first to look at herding behaviour. Using a simple model, he showed how using other peoples' information rather than one's own leads to an inefficient equilibrium. Further seminal work performed by Lakonishok, Shleifer, and Vishney [9] found correlated trading across subgroups of investors. Both of these studies focused on "Smart Money" institutional investors. These are investors who shouldn't be easily swayed by the actions of others. The cryptocurrency market has a large portion of individual investors. These are investors who are more likely to deviate from rational trading practices. Barber, Odean, and Zhu [10] showed that bias in individual investors is stronger and more persistent. This was supported by Merli & Roger [11], who built on LSVs model and included the measurement of individual herding on the trading records of over 87,000 investors from 1999-2006. According to Merli & Roger, the examination of an individual's heterogeneity, they could use poor past performance to predict the increased likelihood of herding in the next quarter.

In the cryptocurrency market, with its high percentage of individual investors (those most prone to biases), we would expect to see high levels of herding resulting in huge price swings due to overreaction. This is something that is very common in the market, so commonplace it even has its own term: "mooning." Kraft, Penna & Pentland [12] found strong evidence for a peer effect on the buying behaviour of cryptocurrency investors. They proposed one of three behavioural mechanisms for such an effect:

1. Traders explicitly copying buying trades – Herding
2. Buying due to momentum – Representativeness
3. Buying salient coins with recent price action – Attention

Using data from crowdfunding campaigns (a capital raising mechanism not unlike ICOs) Lu et al [13] found that early social media engagement and promotional activity correlated with the success rate of the project. Additionally, a number of studies have looked at Twitter volume and trading volumes and found positive correlations [14]. A similar correlation is likely between ICO success and ROI.

Another aspect of ICOs that may affect ROI is bonus levels. Adhami et al. [15] found that ICO bonuses were marginally correlated with ICO success. Behavioural economics suggests that ICOs with a particularly high bonus will dissuade later adopters and lead to a reduced ROI for investors.

2.4. Representativeness

This is the assumption that a sample is representative of the population. Two of the most common examples of this are the Gambler's Fallacy and Hot Hands Fallacy. These two fallacies are related to a belief in momentum. The same bias can be seen in trading behaviour. Barber, Odean, and Zhu concluded that "investors tend to buy stocks with strong past returns." Moment trading is a well-documented characteristic of the cryptocurrency market. Liu and Tsyvinski [16] found strong evidence of this, finding that "a one standard deviation increases in today's return leads to increases in daily returns by 0.33%." During a weekly timeframe, a one standard deviation increases leads to a 3.16% increase at week t+1. In real terms, this is a 5.55% ROI at the daily level and a 16.64% ROI at the weekly level. The particular significance of their finding is that traditional technical analysis methods of analysis were not significant, or they had no discernable pattern. They concluded that cryptocurrencies did not behave like a traditional asset, a store of value such as precious metals, or as a currency; instead, they had their own characteristics and market-specific factors. Whilst their paper focused on the top three cryptocurrencies - Bitcoin, Ripple and Ethereum - and looked at trading rather than ICOs, it is reasonable to believe that these market-specific factors will be present in ICOs as well. Tversky & Kahneman [17] noted that these reasoning errors are most severe as uncertainty increases, which could explain the large deviations in price. Whilst this research will not examine momentum directly, it will explore a few factors that could lead to increased demand and subsequent momentum. Chief among those will be the Size Effect.

The Size Effect is the assumption that smaller firms outperform larger firms. Initially observed by Banz [18], the literature on whether this is actually evident is mixed. Some suggest that over time, the effect disappears [19] Others show seasonal variation [20]. What is apparent is that the effect is not linear [21]. The effect could be due to investors erroneously believing that smaller capitalisation firms have more room to grow. By looking at the market capitalisation of ICOs, we can see whether a size effect is present in the cryptocurrency market. The ICOs in the lower percentile would therefore be correlated with larger ROIs.

2.5. Availability

The availability heuristic states that the most recent or salient information has a stronger influence on our decision-making. One aspect that affects the salience of information is familiarity. The familiarity bias is most clearly demonstrated by the Home Bias. This is an investor's preference to invest in their own country [22]. Very simply, investors tend to stick to what is familiar and therefore easier to understand. This is also evident in investors' decisions towards industries of expertise.

Zacharakis & Meyer [23] determined that one of the key markers for venture capital (VC) investment is market familiarity and competition. They note that this could lead to the behavioural bias of only investing in a company or product the VC can immediately understand. In the cryptocurrency market, the traditional method of evaluating an ICO is very similar to that of a VC evaluating a startup. Traditionally this would involve looking at the team, the potential market they are entering, competition, quality of the product, and the business plan. For a blockchain startup, this would be their whitepaper and timeline. Coincheckup, a highly popular website for cryptocurrency platforms, uses a similar VC-style model to evaluate and weight the quality of blockchain startups. It looks at the team, potential market, competition, and quality of the product. Additional factors that determine VC involvement include a preference for smaller emerging markets [24] and a preference for niche markets [25]. These factors could explain the rapid expansion of

capital into the blockchain space.

Brennan & Cao [26] point out that when investors have limited information, researchers tend to see return-chasing behaviour, i.e., only buying when risk-adjusted returns are high. This behaviour is extremely prevalent in the cryptocurrency market. This behaviour would suggest a lack of expertise in the market. This is likely to lead to stronger effects from biases such as familiarity. In the cryptocurrency market, ICOs that have a product that is easy to understand, or one that is similar to a product an investor may already know, can take advantage of this bias. By analysing the whitepaper, researchers can ascertain the complexity of the product and the degree to which it is easy to understand, or its similarity to a well-known product. Shehhi et al [27] found that ease of understanding played a role in an investor's choice of which cryptocurrencies to mine.

2.6. Research Questions

Considering the research from behavioural economics and the work that has already been done on the cryptocurrency market, I propose the following research questions to be explored:
Q1) Will ICOs with large bonus levels dissuade later investors because of a fear they have already missed out?
Q2) Will higher ratios of positive sentiment, or pre-ICO social media levels, or coin size, or market capitalisation, be correlated with higher ROI in ICO investing due to behavioural factors such as Affect, Herding, and the Size Effect?
Q3) Will the ease of understanding of a blockchain project be correlated with higher ROI due to familiarity?
Q4) Would a hybrid Behavioural and Technical Model of ICO rating be correlated with higher ROI than a Technical Model alone?

3. Methodology

The cryptocurrency market is relatively new. Whilst Bitcoin has been around since 2008, it was only with the launch of Ethereum in 2014 and the subsequent "altcoins" that began using the ERC20 Ethereum platform that a market began to form. 2016 saw a boom and the formation of a true marketplace, with a huge increase in ICOs - from 39 total until 2016 to 256 in 2016 alone. As such, getting reliable data is extremely difficult; no single repository for the industry currently exists. The data in this research was collated from several sources. The data was taken from tokendata.io and cross-referenced with data from icostats, icobench, and icodata, along with the websites for the respective ICOs.

Data regarding the top ICOs sorted by their respective ROIs was collected and categorized using the business/ICO name, ICO date, ICO price in USD, current price in USD (as of June 2nd 2018) and ROI in USD. ROI was given as a multiple of initial investment. The top 51 ICOs by ROI were kept with the exception of Aeternity (phase 2) - this data was an extension of the phase 1 ICO. Later in the process, three more ICOs were removed: Ethereum, Nxt, and Metal. This was because it was discovered that they did not meet the requirement of a fully public ICO. This final cull left us with a dataset of 47 ICOs.

3.1 Fundamental Analysis Data

Coincheckup was used to collect data on the team, advisors, brand/hype, product, coin, social engagement, communication ability, business transparency, and/or Github data. These are key variables used as industry standards for evaluating the fundamentals of an ICO project. Coincheckup uses this data to create an overall weighted score for that business. Coincheckup was used because it is currently an industry favourite. This research used the same information with a few changes. The approach was to look at information only available at the time of the ICO, so the below criteria under Coin Strength was not included in the analysis:

- Average trading volume in past 3 months against other assets' average volume.
- Average market cap in the last 3 months against other assets' average market cap.
- Value growth since trade start date against total market growth.

This reduced the weighting for coin strength to 6.9% for semi and centralised structures, and 8.1% for decentralised structures. The left-over weighting from this reduction was redistributed evenly across all categories to keep the ratios intact. The revised weighting was used to give an overall score for that business/ICO. This was a given as a percentage and used to represent the overall strength of that business/ICO. Using Pearson Correlation, the ROI for the ICOs was compared to their weighted score. This gave us the correlation for a solely fundamental model. This was used later to compare against a hybrid model.

Behavioural Variables

The key general heuristics were used to categorise several key biases. These biases were explored to see how they may manifest in the cryptocurrency market. The following were identified as potential triggers for a behavioural response:

- ICO bonus levels – Loss Aversion
- The ratio of positive to negative information from Twitter data – Affect
- Pre-ICO social media levels (Twitter) – Herding
- Ease of understanding the whitepaper/product/similarity to a well-known product

– Familiarity Bias
- Small market cap – Size Effect

3.3 Behavioural Variable Data Collection

1) Max ICO bonus levels were taken from the whitepapers of the respective ICO along with the ICO rating website. Building upon Adhami, Giddici & Martinazzi's [15] work, the research will explore whether a large maximum ICO bonus discourages potential investors.

2 & 3) Affect and pre-ICO social media levels were found using Twitter data using a similar approach to that of Bollen [5]. Affect was found using Crimson Hexagon's Sentiment Analysis tool for keywords in the crypto space. This was used to elicit market sentiment at the time of an ICO. Pre-ICO social media levels were found using the "$" tag for the respective ICO for the two months prior to the launch, along with a number of keywords for the industry. Sentiment data was binned into three-month periods from January 2016 to June 2018.

4) The ease of understanding was evaluated using Amazon's web service template for evaluating the applicability of a blockchain project. The score was given based on the ease of completing the various sections. The scores for each section were averaged to give an overall 'ease of understanding' score for that project. The score was given out of five.

5) Coin value and market cap were taken from the token data source.

Behavioural Data Analysis

Pearson's Correlation was used to identify whether any of these biases were present and whether they correlated with the ROI of the top 50 performers. For significance levels, one-way ANOVAs were used. Once the correlating variables were identified, they were combined with the data from the fundamental analysis and used to create a new Weighted Behavioural Algorithmic score. This score was then compared against the ROI of the top 50 performers to see whether it has a stronger correlation, and therefore whether we could use the algorithm to better predict potential high performers.

3.5 Review

The main issue faced during this research was the difficulty of getting high-level data. There is no single repository for cryptocurrency data, so the data provided was taken from multiple sources. Due to this necessity, the research was restricted to a severely limited number of ICOs. A further limitation was the use of Twitter data alone as an indication of pre-ICO social media levels. Additional social media channels such as Telegram, Discourse, and Reddit are heavily used by blockchain projects. Whilst this paper will not be evaluating the causality of the behavioural mechanism, only its correlation to an investor's ROI, any follow-up work should include a causal link. For example, further work could build on the work of Frey, Herbst, and Walter [28], who found that as the number of active traders decreases, so does the level of Herding. By examining the number of active traders on the various crypto-trading platforms over time, researchers could seek to elicit Herding levels.

4. Research Findings

This research sought to explore which behavioural factors may play a role in the decision-making process of investors in the cryptocurrency market. Identified were six variables that may play a role due to key behavioural biases. This section shows the results of a Pearson's Correlation test along with a regression analysis of those variables.

Table 1. Pearson's Correlation

	ROI (x)
ROI (x)	1
FA Score	0.159142633
Coin Value	-0.106236506
MarketCap	-0.168776981
Ease	0.3375918
Sentiment	-0.113042187
ICO Bonus	0.157188773
Pre-ICO SM	-0.08048759

Table 1 shows the Pearson's Correlation of the six behavioural variables - Coin Value, MarketCap, Ease of Understanding, Sentiment, ICO Bonus Level, and Pre-ICO Social Media Levels - along with Traditional Fundamental analysis. The Correlation showed no strong correlations amongst any of our variables. Interestingly, the fundamental analysis score, showed next to no correlation. This would suggest that the current methods of fundamental analysis for blockchain projects are inadequate. This finding supports that of Liu and Tsyvinski [16], who also found no correlation of traditional technical analysis factors in cryptocurrency markets.

The maximum level of correlation was ease of understanding with 0.3375918. A one-way ANOVA was conducted and found to be statistically significant $F(1,45)= 5.788$, ($P = .0203$), shown in Table 2.

Table 2. One-way ANOVA results

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	18400.81	18400.81	5.788246	0.020304*
Residual	45	143054.8	3178.995		
Total	46	161455.6			

Table 3 shows a low R Squared for the ANOVA; however, that is expected with the limited observations

and the nature of the data.

Table 3: Regression statistics for ease of understanding

Regression Statistics	
Multiple R	0.337592
R Square	0.113968
Adjusted R Square	0.094279
Standard Error	56.38258
Observations	47

Main Findings

The data shows that fundamental analysis of blockchain projects is not correlated with ROI. Additionally, the data shows that behavioural factors do play a role - in particular, the ease of understanding of the project. The previous literature suggested six hypotheses to explore. Below are the detailed findings from the analysis of each of those questions.

Q1 regarding bonus levels showed no correlation with ROI. Previous research by Adhami, Giddici & Martinazzi [15] did find a marginal correlation with the success of ICOs. From this finding, it was suggested that larger bonus levels may dissuade investors. Further analysis showed that the highest average return for bonus levels was between 10% & 20% (Figure 2). Projects with higher bonus levels saw a rapid drop-off in average ROI. There was no difference between instances when projects that had a maximum bonus of 5% were included, and when the analysis was limited to those projects with a bonus of 10% & 20% alone. Due to the benefits of offering a slightly higher bonus level, the recommended maximum bonus level is between 10% and 20% for any ICO.

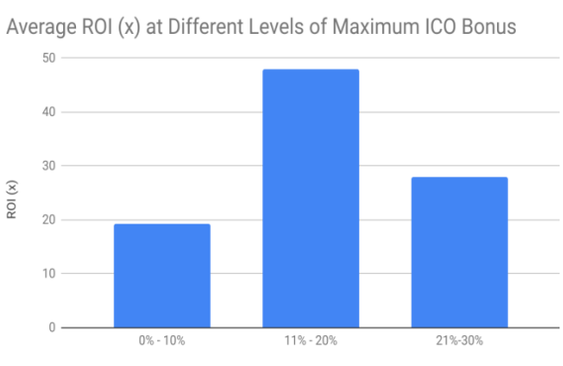


Figure 2. Average ROI per ICO Bonus level

Q2 was regarding the market sentiment at the time of the ICO. The results did not show any correlation. The approach taken here was to explore overall market sentiment. A finer analysis of the sentiment for a particular project in the months leading to its ICO may shed further light.

Q3 regarding pre-ICO social media levels was insignificant and did not correlate with ROI.

Q4, examining ease of understanding, proved significant. This suggests that the investor's decision to invest in a blockchain project is influenced by the ease of understanding the pertinent whitepaper. This is consistent with the assumption that in the absence of appropriate methods of fundamental analysis for blockchain projects, investors are relying on personal assumptions and feelings toward a particular project. As noted by Shehhi et al. [27], ease has been found to play a part in the decision of which cryptocurrencies to mine.

Q5 regarding market cap: The amount the ICO raised was not correlated with ROI. This suggests that investors are not concerned with coin value and market cap at the time of ICO. This is contrary to what we see in trading behaviour in cryptocurrency markets, where there is a clear preference for smaller-valued coins and medium sized market caps.

Q6 sought to answer whether a hybrid model of fundamental analysis and behavioural analysis could outperform fundamental analysis alone. Looking at the top 15 in terms of ROI based on fundamental analysis, the average return was 52.63x. Based on ease of understanding, the average ROI was 64.53x. The fundamental analysis approach of investing in projects above a certain threshold, 77%, saw an average ROI 62.56. A hybrid model looking at traditional analysis scores of 77% or above and an ease of understanding score of above 3.0 gained an average ROI of 83.64x. This is a 33.6% improvement. In terms of ROI, this is a 3360% gain. This would support the hypothesis that a hybrid model outperforms fundamental analysis alone.

Table 4. Average ROI results

Regression Statistics	
Multiple R	0.337592
R Square	0.113968
Adjusted R Square	0.094279
Standard Error	56.38258
Observations	47

5. Discussion

The analysis showed that of the six behavioural variables identified, ease of understanding was the only significant variable. When this variable was included in a hybrid model of analysis (inclusive of fundamental analysis), it outperformed the fundamental analysis alone by 33.6%. Investors taking this approach could see a massive increase in their returns. The next step would be to apply this model to another, larger dataset and see how it performs against new data. Machine learning techniques could hone in on the optimum levels to maximise ROI. This also highlights the importance of taking extra time when writing a whitepaper to ensure that it is easy to follow and understand. Whilst this can be difficult due to the technical nature of many

blockchain projects, it is clearly important to investors and should not be over looked. A valuable approach could be to split the contents of a whitepaper into a high-level overview and a separate technical whitepaper. That way, investors can read the appropriate paper based on their level of technical sophistication.

Whilst the analysis showed a significant result, there were a number of limitations of the approach that must be addressed, the largest being the use of USD as our currency reference. Most of the ICOs presented in this study did not allow for USD investment. The investment was either in Ethereum or bitcoin. In some cases, it could have been that whilst there was a positive return in USD in terms of bitcoin or Ethereum, the returns could have been much less or even negative due to the substantial growth of both of these coins during the period of analysis. For example, Waves was included in our analysis with an ROI of 17x; however, in terms of bitcoin, this was a loss. Another limitation was how this research evaluated ease of understanding. Whilst the study used the AWS Blockchain Business Canvas as a template, the assessment of ease was subjective. Further studies could be improved by providing a more structured analysis. For example, points could be awarded for particular keywords, executive summary, or particular sections.

6. Conclusion

Cryptocurrencies do not fit typical fundamental analysis. These "coins" have no underlying assets; instead, their value comes from network values. It is a speculative market. The characteristics of such a market include short-term "narrow frame" investors, noise traders, and momentum chasing. We, therefore, cannot exclude behavioural factors when looking at price action. For startups that are planning to use an ICO as their funding vehicle, it is important that they take these factors into consideration when they are looking at their tokenomics - these will have a direct impact on the longevity of the project. For investors, it is important to understand the behavioural factors that may bias their investment decision. These findings are supported by the work from Hargrave, Sadhev & Feldmeier [29]. A key variable to consider is the ease of understanding of the whitepaper. Investors with limited knowledge and experience in blockchain find comfort and confidence in products that they can more readily understand. It is important for entrepreneurs not to underestimate the importance of their whitepaper to the success of their project. Additionally, investors can seek to maximise their returns by including this in their analysis. A final note is for entrepreneurs to limit the size of the bonuses offered for early involvement in an ICO. The recommendation from these findings is between 10% and 20%. Likewise, investors should be wary of projects offering particularly large bonuses. Further analysis is needed as to the extent of behavioural factors at play in the cryptocurrency market. Further research should seek to rectify the limitations of this research and build upon its findings. It is evident that this is a fledgling field; as the market becomes more sophisticated, the expectation is that better-educated investors will lead to behavioural factors playing less of a role. For now, however, investors and entrepreneurs alike cannot afford to ignore the significance of behavioural factors.

References

[1] A. Tversky, D. Kahneman, "Judgment under Uncertainty: Heuristics and Biases," Science, vol. 185, no. 4157, pp.1124-1131, 1974.

[2] M. L. Finucane, A. Alhakami, P. Slovic and S. M. Johnson, "The affect heuristic in judgments of risks and benefits," Journal of Behavioural Decision Making, Vol.13, pp.1-17, 2000. Available: doi:10.1002/(SICI)1099-0771(200001/03)13:1<1::AID-BDM333>3.0.CO;2-S

[3] G. W. Brown and M. T. Cliff, "Investor sentiment and asset valuation," Journal of Business, vol. 78, pp. 405–440, 2005.

[4] M. Lemmon and E. Portniaguina, "Consumer confidence and asset prices: some empirical evidence," Review of Financial Studies, vol. 19, pp. 1499–1529, 2006.

[5] J. Bollen, H. Mao and X. Zeng, "Twitter mood predicts the stock market," Journal of Computational Science, vol. 2, no. 1, pp. 1-8, 2010.

[6] P. Slovic, M. L. Finucane, E. Peters and D. G. MacGregor, "The affect heuristic," European Journal of Operational Research, vol. 117, pp. 1333-1352, 2007.

[7] D. Hirshleifer and S. Teoh, "Herd Behaviour and Cascading in Capital Markets: A Review and Synthesis," European Financial Management, vol. 9, no. 1, pp. 25–66, 2003.

[8] A. Banerjee, "A Simple Model of Herd Behavior," The Quarterly Journal of Economics, vol. 107, no. 3, pp. 797–817, 1992. Available: doi:10.2307/2118364

[9] J. Lakonishok, A. Shleifer and R. W. Vishny, "The Impact of Institutional Trading on Stock Prices," Journal of Financial Economics, vol. 32, pp. 23-43, 1992.

[10] B. M. Barber and T. Odean, "All that Glitters: The Effect of Attention and News on the Buying Behavior of Individual and Institutional Investors," The Review of Financial Studies, vol. 21, no. 2, 2008. Available: doi:10.1093/rfs/hhm079

[11] M. Merli and T. Roger, "What drives the herding behaviour of individual investors?" Finance, vol. 34, no. 3, pp. 67-104, 2013.

[12] P. Krafft, N. Penna and A. Pentland, "An Experimental Study of Cryptocurrency Market Dynamics," presented at the ACM CHI Conference on Human Factors in Computing Systems, Montreal, Canada, 2018. Available: doi:10.1145/3173574.3174179

[13] C. Lu, S. Xie, X. Kong and P. Yu, "Inferring the impacts of social media on crowdfunding," Proceedings of the 7th ACM international conference on Web search and data mining, New York, New York, USA, 2014. Available: doi: 10.1145/2556195.2556251

[14] D. Tsui, "Predicting Stock Price Movement Using Social Media Analysis," Stanford University Technical Report, 2017.

[15] S. Adhami, G. Giudici and S. Martinazzi, "Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings," Journal of Economics and Business, 2018. Available: http://dx.doi.org/10.2139/ssrn.3046209

[16] Y. Liu and A. Tsyvinski, "Risks and Returns of Cryptocurrencies," NBER working paper, 2018. Available:https://economics.yale.edu/sites/default/files/files/Faculty/Tsyvinski/cryptoreturns%208-7-2018.pdf

[17] A. Tversky and D. Kahneman, "Extensional vs. Intuitive Reasoning: The Conjunction Fallacy in Probability Judgment," Psychological Review, vol. 90, no. 4, pp. 293-315, 1983.

[18] R. W. Banz, "The relationship between return and market value of common stocks," Journal of Financial Economics, vol. 9, no. 1, pp. 3–18, 1981.

[19] E. F. Fama and K. R. French, "Size, value, and momentum in international stock returns," Journal of Financial Economics, vol. 105, no. 3, pp. 457-472, 2012.

[20] K. E. Easterday, P. K. Sen and J. A. Stephan, "The persistence of the small firm/January effect: Is it consistent with investors' learning and arbitrage efforts?" The Quarterly Review of Economics and Finance, vol. 49, no. 3, pp. 1172–1193, 2009.

[21] E. F. Fama and K. R. French, "Dissecting anomalies," Journal of Finance, vol. 63, no. 4, pp. 1653–1678, 2008.

[22] K. R. French and J. M. Poterba, "Investor Diversification and International Equity Markets," American Economic Review, vol. 81, no. 2, pp. 222-226, 1991.

[23] A. Zacharakis and D. G. Meyer, "A lack of insight: Do Venture Capitalists really understand their own decision process?" Journal of Business Venturing, vol. 13, pp. 57-76, 1998.

[24] D. Fichera, "The Insider's Guide to Venture Capital: Who the Key Players Are, what They're Looking For, and how to Reach Them," Published by Prima Venture, California, USA, 2001.

[25] J. J. Camp, "Venture Capital Due Diligence: A Guide to Making Smart Investment Choices and Increasing Your Portfolio Returns," Published by John Wiley and Sons, New York, New York, USA, 2002.

[26] M. J. Brennan and H. H. Cao, "International portfolio investment flows," Journal of Finance, vol. 52, pp. 1851-1880, 1997.

[27] A. A. Shehhi, M. Oudah and Z. Aung, "Investigating factors behind choosing a cryptocurrency," IEEE International Conference on Industrial Engineering and Engineering Management, pp. 1443-1447, 2014. Available: doi: 10.1109/IEEM.2014.7058877

[28] S. Frey, P. Herbst and A. Walter, "Measuring mutual fund herding - A structural approach," Journal of International Financial Markets, Institutions and Money, vol. 32, pp. 219-239, 2014.

[29] J. Hargrave, N. Sahdev, and O. Feldmeier, "How Value is Created in Tokenized Assets," SSRN, 2018. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3146191

Photo by Haziqah Noor-ul-Islam at 1st Blockchain International Scientific Conference, in London. 12 March 2019

CONFERENCE PROCEEDINGS

1st Blockchain International Scientific Conference 12 March 2019, London

1. Blockchain investigations – Beyond Money

Simon Dyson
Edinburgh Napier University, UK
Category: Oral Presentation

Abstract
Cryptocurrency investigations have centred 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 Silk Road market place 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 paper examines the hosting of stolen data (P.I.I) personal identifiable information on a distributed blockchain host where the data is also stored. 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 tool box. 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*

2. Cryptocurrencies & Initial Coin Offerings: Are they Scams? An Empirical Study

Daniel Liebau[1], Patrick Schueffel[2]
[1]*IE Business School*
[2]*HEG Fribourg School of Management*
Category: Oral Presentation

Abstract
The volume of Initial Coin Offerings (ICOs) had risen steeply with an all-time high market capitalisation of close to 1 Trillion USD in December 2017. Since then, the digital asset market has slumped, retreating to approximately 200 Billion USD by mid-2018. Stakeholders of the crypto industry have pondered the reasons for this retrenchment and are increasingly focusing on the notion that many ICOs could be scams. A recent industry study even went as far to claim that 80% of all ICOs are indeed scams. In this paper, we investigate the question whether these scams are as common as claimed. We do so by first defining what a scam is and secondly, by drawing on empirical data to assess the number of cases fitting such a definition. Building on Principal Agent Theory and based on the statistical analysis of our empirical data set we attempt to establish the current state of affairs with regards to scams in the cryptocurrency world. The results of our study divert from salient beliefs.
Keywords: *blockchain, scam, ICO, digital assets, ethics, crypto-currency, token*
JEL Classifications: *D01, D21, D26, D53, D84, K24*

3. The Application of Behavioural Heuristics to ICO Valuation and Investment

Maxwell Stanley
University of Essex, UK
Category: Oral Presentation

Abstract
Blockchain projects have seen a rush of investment in the form of Initial Coin Offerings (ICOs) over the past eighteen months, yet little is understood about how to valuate these projects. This research looked at the application of behavioural heuristics to ICO valuation and investing. Identified were six variables that may play a role due to key behavioural biases. These variables, coin value, market capitalisation, ease of understanding, market sentiment, maximum ICO bonus level, and pre ICO social media levels were analysed using Pearson's correlates for their correlation with return on investment. The data was collected from numerous ICO websites along with Twitter data. Fundamental analysis was taken from Coincheckup due to this being a major source of information for many retail investors and uses a well-defined methodology. Sentiment data was collected from Twitter and assessed using crimson hexagons Sentiment tool. Ease of understanding was evaluated using AWS Blockchain business canvas. All information was compiled into a single dataset and the top 47 projects in terms of ROI were utilised. Ease of understanding was found to be significantly correlated ROI. Ease of understanding was then combined with fundamental analysis to develop a hybrid model of evaluation for Cryptocurrency projects. This model substantially outperformed fundamental analysis alone with a 33.6% improvement on ROI. In conclusion, current methods of fundamental analysis for Blockchain projects are inadequate to capture their potential future value. Investors, devoid of appropriate tools, limited knowledge and experience due to the relative novelty, are being influenced by behavioural factors such as ease of understanding. It is therefore impertinent that investors and entrepreneurs alike take such factors into consideration.
Keywords: *blockchain, behavioural economics, behavioural heuristics, ICO, cryptoeconomics, tokenomics*
JEL Classifications: *D02, D71, H11, P16, P48, P50*

4. Assigning Residual Rights to Smart Contracts

Lucas Leger
Conservatoire des Arts et métiers
Category: Oral Presentation

Abstract
One of the promises of smart contracts is to remove third parties to structure trading relationships in the digital world, from market platforms to organizations themselves. The conditions under which trade will take place is enforced through self-executing programs that run on blockchains. In this theoretical paper, we investigate how can we assign optimal residual rights within smart contracts? Indeed, in traditional organizations like firms, ownership rights are well established. As shown by Grossman and Hart (1986) in their seminal work an optimal distribution of residual rights, i.e. control over the use of assets, protect stakeholders and owners "from future holdups by other trading partners." In blockchain-based networks this setup does not exist, because i) assets are especially human capital, ii) funds are stored on the blockchain where residual rights lay in the hand of a third party: miners and the so-called whales who basically control the consensus protocol. Using The DAO hack as a use case, we demonstrate that most smart contracts lack governance mechanisms to protect and incentivize both owners and investors, especially when things do not go according to plan. Then, we apply the formal framework of incomplete contract theory to design a smart contract that would automatically assign optimal residual rights.
Keywords: *Smart contracts, Incomplete contracts, residual rights, governance, DAO*

5. Parameters for building sustainable blockchain application initiatives

Lewis Laidin, Kassandra A. Papadopoulou
The University of Manchester, UK
Category: Oral Presentation

Abstract
Despite the demand and interest for the technology, there are still major challenges for blockchain application initiatives (projects and ventures) to be sustainable and reliable. While starting a non-blockchain initiative already comes with its own sets of challenges and has around 50% failure rate, starting a blockchain initiative rises the rate to 90% due to additional variables and confusions on top. Such a situation deters innovators and eventually dampens innovation, requiring priority for actions. This paper attempts to contribute by compiling and outlining the various key variables required to be considered, creating a set of parameters for blockchain initiators. Through secondary data collection: literature reviews, report studies and primary data collection: interventional and observational case study, interviews with blockchain researchers, businesses and entrepreneurs, this paper categorises variables into blockchain-related and venture-related categories, outlining consideration points for each variables. To summarise the variables and by consulting theories of innovation and adoption, it is then concluded in the paper that concept validation entailing both initiative feasibility and user-demand, is of key importance, both for blockchain innovation, for trust between ecosystem stakeholders and for the venture sustainability.
Keywords: *blockchain, business, initiatives, challenges, barriers, parameters, feasibility, concept*
JEL Classifications: *D04, D07, D08, I07, O03, Y04*

6. Blockchains and Financial Intermediation – An alternative approach to monitor the Monitors

Klara Sok
Conservatoire National des Arts et Métiers
Category: Oral Presentation

Abstract
The emergence of Bitcoin, blockchains and distributed ledger technologies led some commentators call for the end of banks, or at least for a profound change in financial intermediation (Antonopoulos, 2016): what if, indeed, there were an alternative solution to producing and distributing financial services to society, to the one we know today? What if organizing markets in a different way, with the use of information technology, could mechanically decrease uncertainty, just by design? Could the panopticon architecture of distributed autonomous organizations (DAOs) be a substitute to current financial intermediation? This research work proposes a theoretical framework aiming at supporting socio-economic analyses of blockchain-based innovations applied to financial intermediation, through the lens of institutional information transformation. Financial intermediation is considered as a solution to information asymmetries resulting in market inefficiencies (such as adverse selection and moral hazard) between demand for financing and financing offering. Financial institutions operate as informational "monitors" on behalf of funders (Diamond, 1984) and are themselves monitored ("monitoring the monitor") through financial regulation and institutional surveillance. This research aims at theoretically demonstrating how distributed ledgers and distributed consensus, applied to financial transactions, could impact the structure and efficiency of our financial system, depending on their organizational design and institutional embeddedness.
Keywords: *blockchain, Bitcoin, financial intermediation, cryptofinance, monitoring the monitor, fintech*
Themes: *blockchain, financial intermediation, monitoring the monitor, oracles, information asymmetry, adverse selection, moral hazard, fintech, regtech*

7. Capital mobility in light of emerging technologies: the case of crypto-asset investment

Alfio Puglisi
Kings College London, UK
Category: Oral Presentation

Abstract

The benefits of Blockchain technologies in finance are widely acknowledged but there are concerns on the risks associated with it. In this space, crypto-assets are new financial innovation and have only recently begun to attract the attention of financial regulators. What remains to be seen is how different jurisdictions approach regulations regarding Blockchain applications, not only in concept but also in actual practices.

This paper takes a cross-country comparative approach of the diverse types of governance strategies taken to date to address the risks posed by Blockchain technologies and their fit to current orthodoxies of regulatory governance. It examines the (in) adequacy of traditional approaches to regulating and governing Blockchain technologies and of the actions of government with new approaches.

For instance, in December 2017 the International organisation for securities (IOSCO) published on its website a non-binding statement on crypto-assets and initial coin offerings (ICOs), emphasizing crypto-assets as a form of security. Regulatory preferences at national and international level differ. Offshore jurisdictions respond to markets via a responsive regulatory framework, allowing players with more flexibility. On the other hand, most developed economies acknowledge the issues but yet have implemented any specific strategies. Thus, this regulatory uncertainty fuels self-regulatory frameworks administered by private enterprises. Self-regulatory frameworks can be explained in terms of a coordination game between actors in the crypto space. To do so, this paper employs a comparative politics approach to examine policy preferences.

Results shows that regulatory institutions allow jurisdictions to protect sector's competitiveness and lead the way to the race of the global FinTech hub. Self-regulation allows players to shape public debate in the area of crypto-finance

8. Blockchain and Distributed Ledger Cryptography Evaluation in Post-Quantum World

Rob Campbell
Capitol Technology University
Category: Oral Presentation

Abstract

This paper evaluates the current cybersecurity vulnerability of the prolific use of Elliptical Curve Digital Signature Algorithm (ECDSA) cryptography in use by the Bitcoin Core, Ethereum, Bitcoin Cash, and enterprise blockchains such as Multi-Chain and Hyperledger projects such as Fabric, and Sawtooth Lake. These blockchains are being used in Media, Health, Finance, Transportation and Government with little understanding, acknowledgment of the risk and no known plans for mitigation and migration to safer public-key cryptography. The second aim is to evaluate ECDSA against the threat of Quantum Computing and propose the most practical National Institute of Standards and Technology (NIST) Post-Quantum Cryptography candidate algorithm lattice-based cryptography countermeasure that can be implemented near-term and provide a basis for a coordinated industry-wide lattice-based public-key implementation. Commerical quantum computing research and development is rapid and unpredictable, and it is difficult to predict the arrival of fault-tolerant quantum computing. The current state of covert and classified quantum computing research and development progress is unknown and therefore, it would be a significant risk to blockchain and Internet technologies to delay or wait for the publication of draft standards. Since there are many hurdles Post-Quantum Cryptography (PQC) must overcome for standardization, it is the author's view that coordinated large-scale testing and evaluation must be now.

Keywords: *ECDSA, blockchain, post-quantum, lattice-based cryptography, cybersecurity*

9. Leveraging Blockchain Technology for the Social Determinants of Health

Marquesa Finch
Patientory Association
Category: Oral Presentation

Abstract

Although not a new technology, blockchain has increased in popularity since 2017 as a technology that may prove to have many benefits for the healthcare industry. With secure technology and encryption mechanisms, blockchain can give rise to a new era digital healthcare technologies with improved access to patient data.

For blockchain, 2018 has no doubt been a milestone year. At the time this paper was written, over $21 Billion had been raised in 2018 alone on tokens sales over 905 ICOs. And while cryptocurrency may be experiencing an adjustment, one thing is clear--blockchain's utility across industries is poised to disrupt many of our current systems for exchanging data, information, as well as money. Within healthcare, blockchain's immutable distributed ledger offers solutions for many pain points within our healthcare system including privacy, trusted record keeping, and data coordination/access. While the identified use cases in healthcare are numerous, one stands out in particular-- the coordination and access to trusted data in addressing the social determinants of health.

The barriers to data sharing among clinical entities are breaking down as technology solutions become evident and accepted. Blockchain technology provides the means to create a trust protocol verifying identity and transactions. The ability to trust the process, trust the security, trust the identity and intersect with clinical and public health imperatives will enhance data management, care coordination and improve the process and outcome of individual and community health.

10. Distributed Stateless Society: Liberty, Manorialism and State

Aleksei Gudkov
UCL Centre for Blockchain Technologies, UK
Category: Oral Presentation

Abstract

Decentralization, creativity and freedom are the key notions describing all major trends on blockchain. Common cultural identity allows forming a stateless society in virtual world. Stateless society exists without any sort of state attribute. Distributed stateless society is formed on the on-line network and blockchain technology. The Distributed stateless society has no territory, sovereignty and central authority with coercive power. The core values of stateless society are liberty and cooperation based on anonymity and voting. Speaking in favor of human right we should accept the right to be anonymous. Anonymity guaranties personal freedom through negative liberty on distributed network. The right to be anonymous is important not only for participants of distributed stateless societies but also for fighting with censorship and personal information collection. Economic development of the Distributed stateless society is based on smart contracts and cryptocurrency, which make available exclusion of intermediaries. Though, the adaptation to off-line word has some problems. The major problem of adaptation of blockchain technology is competition between math law, code and legal rules. The blockchain technology under traditional legal regulation has a good chance for implementation in a close system for data management but not for a creation of legal facts yet. I propose to support autonomy of blockchain technology and prohibit it from traditional operational model with human verification and old fashion regulation. We have all chances to create cooperative distributed society to achieve the balance between private and public needs. The Cooperative distributed society should be based on concept of private ordering, where all interested parties rely on self-regulation by creation of self-governance system recognized and legitimized by state authority. The critical element

of the self-governance structure is self-regulatory body. It is reasonable to build a community-driven self-regulatory body to find a compromise between stateless society and traditional regulation. We should speak for independent self regulatory layer for blockchain network. I call for discussion on freedom on blockchain network and invite you to take part in creation of a distributed cooperative society.
The present article aims analysis of stateless societies; reviews historical development of the concept; discuss the features of Distributed stateless society, variants of adaptation blockchain technology, threats of distributed manorialism; and helps to uncover conflicts and opportunities.

11. Data Transparency in Interbank Lending

Andrew Seski[1], John B. Zirnkilton[2]
[1] *University of Delaware, USA*
[2] *Broad Reach Management LLC*
Category: Oral Presentation

Abstract
Considerations and Limitations of Tracking Quality of Collateral with DLTs:
1. Goal: Call to attention the overlap in focus by multiple central banks and boards of financial stability: opacity in bilateral repo markets, defining high quality liquid assets, and oversaturation of short-term funding for long-term projects. DLTs: a distributed ledger across interbank lending networks for access to uniform market data, origination of collateral, and the number of market participants relying on that asset for liquidity would serve as a single portal into capturing hard-to-track market data that countries rely upon for systemic risk modeling.
Exploring limitations of ethereum-based smart contracts:
A. While incredibly fast to read from, blockchains are also incredible slow to read to.
B. Upper limits of chosen fields encoded into smart contracts are reached quickly when the associated logic is complex.

DLT Proposal and Call to Action

1. Market Issues:
A. No window into the complex repo markets, relying on ETF data to model liquidity provisions.
B. Slow and inefficient settlements, centralized trust, and asymmetric information.
C. No way to adequately regulate what is unknown.

2. Proposed Solutions:
A. A single distributed ledger to track the full lifecycle of both sides of transactions in interbanking networks including derivative exposures and further measuring the shadow banking network.
B. Encoded smart contracts that only settle with matching regulatory requirements.
C. Aim to negate a need to rely on Self-Regulatory Organizations, Central Clearing Houses, and Rating Agencies for uniform information.

3. Call to Action:
A. Review requirements of defining high quality liquid assets across borders and provide increased transparency in collateral management.
B. Continue to explore methods to merge and update multiple technological infrastructures into a single portal of access to uniform information.

Photo by Ciprian Boiciuc on Unsplash

FOR AUTHORS

We are now accepting manuscripts for Sep - Oct 2019 Edition (Volume 2, Issue 2).

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 **£585** (£485 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.

JBBA ACADEMIC PARTNERS
1ST EDITION, AUGUST 2018

BLOCKPASS IDENTITY LAB

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Edinburgh Napier UNIVERSITY

pl^g

ENTERPRISE ETHEREUM ALLIANCE

JBBA ACADEMIC PARTNERS
2ND EDITION, DECEMBER 2018

The Open University

r3.

Ulster University

Department for International Trade

ENTERPRISE ETHEREUM ALLIANCE

THE BRITISH BLOCKCHAIN ASSOCIATION IS WORKING IN COLLABORATION WITH

appg BLOCKCHAIN

BBC GLOBAL NEWS LTD

Department for International Trade

GCPSE Global Centre for Public Service Excellence

UNDP Empowered lives. Resilient nations.

Isle of Man Government
Reiltys Ellan Vannin

Portuguese Blockchain Alliance

British Embassy Lisbon

ENTERPRISE ETHEREUM ALLIANCE

FINTECH CIRCLE

OUR MEMBERS

patientory association

ARABIANCHAIN TECHNOLOGY

Web3 Labs

Baker McKenzie.

Gresham International

Abt ASSOCIATES
BOLD THINKERS DRIVING REAL-WORLD IMPACT

KAMBIO VENTURES

Lightbulb Capital

pillar.

BLOCKCHAIN DIGITAL
Distributed Application Studio

BLOCKCHAIN
Association of Belgium

FINTECH
WORLDWIDE LTD.

BLOCKCHAINLIVE

Jibrel Network

GRANDEO

pl^g

NORDIC BLOCKCHAIN ASSOCIATION

QADRE.
BRINGING TRUST TO THE DIGITAL AGE

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

razlin.

Volume 1 - Issue 1
Edition July 2018

Volume 1 - Issue 2
Edition December 2018

Follow us on:

Contact us at:

www.britishblockchainassociation.org

admin@britishblockchainassociation.org

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 (July and January).

Next Round of Fellowship Applications has been commenced (Applications submission Deadline: 30 June 2019)

For more information visit: **britishblockchainassociation.org/fellowship** or contact: **admin@britishblockchainassociation.org**

The British Blockchain Association

Collaboration. Innovation. Excellence

www.britishblockchainassociation.org

THE JBBA THE JOURNAL OF THE BRITISH BLOCKCHAIN ASSOCIATION