Geneva Reports on the World Economy 21

The Impact of Blockchain Technology on Finance: A Catalyst for Change

Michael Casey, Jonah Crane, Gary Gensler, Simon Johnson and Neha Narula

ICMB INTERNATIONAL CENTER FOR MONETARY AND BANKING STUDIES

CEPR

The Impact of Blockchain Technology on Finance: A Catalyst for Change

Geneva Reports on the World Economy 21

International Center for Monetary and Banking Studies (ICMB)

International Center for Monetary and Banking Studies
2, Chemin Eugène-Rigot
1202 Geneva
Switzerland

Tel: (41 22) 734 9548
Fax: (41 22) 733 3853
Web: www.icmb.ch

Centre for Economic Policy Research

Centre for Economic Policy Research
33 Great Sutton Street
London EC1V 0DX
UK

Tel: +44 (20) 7183 8801
Fax: +44 (20) 7183 8820
Email: cepr@cepr.org
Web: www.cepr.org

ISBN: 978-1-912179-15-2

The Impact of Blockchain Technology on Finance: A Catalyst for Change

Geneva Reports on the World Economy 21

Michael Casey
MIT Sloan and MIT Media Lab; Chair of Advisory Board, CoinDesk

Jonah Crane
FinTech Innovation Lab and RegTech Lab

Gary Gensler
MIT Sloan and MIT Media Lab; Chairman, Maryland Financial Consumer Protection Commission

Simon Johnson
MIT Sloan; Member of Advisory Board, CoinDesk (unpaid); Peterson Institute for International Economics; CEPR

Neha Narula
MIT Media Lab and MIT Sloan

None of the authors invests in cryptocurrencies or blockchain technology-related companies.

ICMB INTERNATIONAL CENTER FOR MONETARY AND BANKING STUDIES
CIMB CENTRE INTERNATIONAL D'ETUDES MONETAIRES ET BANCAIRES

CEPR PRESS

The International Center for Monetary and Banking Studies (ICMB)

The International Center for Monetary and Banking Studies (ICMB) was created in 1973 as an independent, non-profit foundation. It is associated with Geneva's Graduate Institute of International and Development Studies. Its aim is to foster exchanges of views between the financial sector, central banks and academics on issues of common interest. It is financed through grants from banks, financial institutions and central banks. The Center sponsors international conferences, public lectures, original research and publications. In association with CEPR, the Center has published the Geneva Reports on the World Economy since 1999. These reports attract considerable interest among practitioners, policymakers and scholars.

ICMB is non-partisan and does not take any view on policy. Its publications, including the present report, reflect the opinions of the authors, not of ICMB or any of its sponsoring institutions. The President of the Foundation Board is Thomas Jordan and the Director is Charles Wyplosz.

Centre for Economic Policy Research (CEPR)

The Centre for Economic Policy Research (CEPR) is a network of over 1,200 research economists based mostly in European universities. The Centre's goal is twofold: to promote world-class research, and to get the policy-relevant results into the hands of key decision-makers.

CEPR's guiding principle is 'Research excellence with policy relevance'.

A registered charity since it was founded in 1983, CEPR is independent of all public and private interest groups. It takes no institutional stand on economic policy matters and its core funding comes from its Institutional Members and sales of publications. Because it draws on such a large network of researchers, its output reflects a broad spectrum of individual viewpoints as well as perspectives drawn from civil society.

CEPR research may include views on policy, but the Trustees of the Centre do not give prior review to its publications. The opinions expressed in this report are those of the authors and not those of CEPR.

About the authors

Michael Casey is a senior advisor at MIT Media Lab's Digital Currency Initiative and a senior lecturer at MIT's Sloan School of Management. He also the Chairman of CoinDesk's Advisory Board. Before joining MIT, Michael spent 18 years at Dow Jones and *The Wall Street Journal*, where he last served as a columnist covering global economics. He is the author of five books, including the recently published *The Truth Machine: The Blockchain and the Future of Everything*, co-authored with Paul Vigna. Michael is a graduate of the University of Western Australia and has higher degrees from Curtin and Cornell universities.

Jonah Crane is an advisor to financial technology companies, Regulator in Residence at the FinTech Innovation Lab in New York, and Executive Director of RegTech Lab in Washington D.C. where he advises regulators and policymakers on facilitating innovation. Jonah previously served as a Senior Advisor and Deputy Assistant Secretary for the Financial Stability Oversight Council at the United States Treasury Department. Before joining Treasury, Jonah was a policy advisor to Senator Chuck Schumer and a corporate attorney at Milbank, Tweed, Hadley & McCloy LLP in New York. Jonah received a J.D. from New York University School of Law.

Gary Gensler is Senior Advisor to the Director, MIT Media Lab; Senior Lecturer, MIT Sloan School of Management; and Chairman, Maryland Financial Consumer Protection Commission. He formerly was Chairman of the U.S. Commodity Futures Trading Commission, leading the Obama Administration's reform of the $400 trillion swaps market. During the Clinton Administration, he was Under Secretary of the Treasury for Domestic Finance, and Assistant Secretary of the Treasury. Previously, Gensler was a partner at Goldman Sachs. He earned his MBA and BSE from the Wharton School, University of Pennsylvania. He is a recipient of the 2014 Tamar Frankel Fiduciary Prize.

Simon Johnson is the Ronald A. Kurtz (1954) Professor of Entrepreneurship at the MIT Sloan School of Management, where he is also head of the Global Economics and Management group and chair of the Sloan Fellows MBA Program Committee. Simon is a senior fellow at the Peterson Institute for International Economics in Washington, D.C. and a member since inception of the FDIC's Systemic Resolution Advisory Committee. In July 2014, Simon joined the Financial Research Advisory Committee of the U.S. Treasury's Office of Financial Research (OFR), and subsequently chaired the Global Vulnerabilities Working Group. He is a Research Fellow in CEPR's Development Economics programme. Simon has a Ph.D. in economics from MIT.

Neha Narula is the Director of the Digital Currency Initiative at the MIT Media Lab. She received her PhD in computer science from MIT in 2015, where she worked on concurrency control for scalable distributed systems and databases. Her current research interests are in cryptocurrencies and distributed systems. Neha is a member of the World Economic Forum's Global Futures Council on Blockchain and has given a TED talk on the future of money. In a previous life, she helped relaunch the news aggregator Digg and was a senior software engineer at Google.

List of abbreviations

AMF	Autorité des Marchés Financiers
AML	anti-money laundering
API	application programming interface
ASX	Australian Stock Exchange
ATS	alternative trading system
BRBC	Belt and Road Blockchain Consortium
CCP	counterparty clearing house
CFT	combatting the financing of terrorism
CFTC	US Commodity Futures Trading Commission
DAO	Decentralised Autonomous Organisation
dApp	distributed application
DCM	designated contract markets
DLT	distributed ledger technology
DTCC	Deposit Trust and Clearing Corporation
ESMA	European Securities and Markets Authority
FCM	futures commission merchant
FINMA	Swiss Financial Market Supervisory Authority
FSB	Financial Stability Board
FX	foreign exchange
HKMA	Hong Kong Monetary Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICE	Intercontinental Exchange
ICO	initial coin offering
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
ISDA	International Swaps and Derivatives Association
JFSA	Japanese Financial Services Agency
KYC	know your customer
MiFID II	Markets in Financial Instruments Directive II
RFED	retail foreign exchange dealer
RTGS	Bank of England Real Time Gross Settlement System
SAFTs	Simple Agreements for Future Tokens
SEC	U.S. Securities and Exchange Commission
SEF	swap execution facility
SRO	self-regulatory organisation

Contents

List of conference participants

Mirko Abbritti	Associate Professor Economic Department Universidad de Navarra
Ivan Adamovich	Chief Executive Officer Private Client Bank AG Zürich
Edmond Alphandery	Chairman Euro 50 Group Paris
Mourtaza Asad-Syed	CEO Yomoni Asset Management Paris
Katrin Assenmacher	Head of Division Monetary Policy Strategy Division European Central Bank Zürich
Simone Auer	Advisor to the Governor Swiss National Bank
Richard Baldwin	Professor of International Economics The Graduate Institute Geneva
Jeanne Barras-Zwahlen	Consultant Banque Julius Baer Geneva
Vít Bárta	Advisor to Governor Czech National Bank Prague
Geoffroy Bazin	Chief Executive Officer BNP Paribas Geneva
Charles R. Bean	Professor London School of Economics UK Office for Budget Responsibility London Chair, CEPR, London

David Begg	Professor Imperial College Business School London
Erik Berglof	Director Institute of Global Affairs London School of Economics
Jan Marc Berk	Director Economics & Research De Nederlandsche Bank
Claudio Borio	Head of the Monetary and Economic Department Bank for International Settlements Basel
Michael Burda	Prof. Dr. h.c., Ph. D School of Business and Economics Humboldt-University Berlin
Luigi Buttiglione	Managing Partner of Sempera Founder of LB-Macro London
Mark Carey	Co-President GARP Risk Institute Arlington, USA
Jaime Caruana	Former General Manager BIS
Francesca Caselli	Economist Research Department IMF
Stephen Cecchetti	Rosen Family Chair in International Finance Brandeis International Business School Waltham, USA
Stijn Claessens	Head of Financial Stability Policy Deputy Head of Monetary and Economic Department Bank for International Settlements Basel
Benoît Coeure	Member of the Executive Board European Central Bank Frankfurt

Jonah Crane	Regulator in Residence FinTech Innovation Lab
Jean-Pierre Danthine	President Paris School of Economics
Xavier Debrun	Division Chief Research Department IMF
Jose de Gregorio	Professor Department of Economics Universidad de Chile
Jacques Delpla	Associate Researcher Toulouse School of Economics
Renaud De Planta	Managing Partner Pictet Group Geneva
Virginia di Nino	Economist International Policy Analysis Division European Central Bank
Steve Donzé	Senior Macro Strategist Pictet Asset Management Geneva
Cédric Dupont	Professor of International Relations The Graduate Institute Geneva
Jean-Pierre Durante	Economist – Head of Applied Research Banque Pictet & Cie
Barry Eichengreen	Professor Department of Economics and Political Science University of California Berkeley
Emmanuel Ferry	Chief Investment Officer Banque Pâris Bertrand Sturdza Geneva
Alessandro Flamini	Professor Department of Economics University of Pavia

Andrea Fracasso	Professor School of International Studies University of Trento
Jeffry Frieden	Professor Department of Government Harvard University
Hans Genberg	Executive Director The SEACEN Centre Kuala Lumpur
Gary Gensler	Senior Advisor to the Director MIT Media Lab Senior Lecturer MIT Sloan School of Manageme
Petra Gerlach	Head of Monetary Policy Analysis Swiss National Bank
Stefan Gerlach	Chief Economist EFG Bank Zürich
Francesco Giavazzi	Professor of Economics Bocconi University Milan
Olivier Ginguene	CIO Asset Allocation and Quantitative Investment Pictet Asset Management SA Geneva
Michel Girardin	Lecturer University of Geneva
Pierre-Olivier Gourinchas	Professor of Economics University of California Berkeley
Clemens Grafe	Economist Goldman Sachs London
Laszlo Halpern	Senior Research Fellow Institute of Economics Centre for Economic and Regional Studies Hungarian Academy of Sciences Budapest

Philipp Hartmann	Deputy Director General Research European Central Bank Frankfurt
Harald Hau	Professor of Economics and Finance University of Geneva Geneva Finance Research Institute
Pablo Hernandez de Cos	Director General Economics, Statistics and Research Banco de España Madrid
Mathias Hoffmann	Professor of International Trade and Finance Department of Economics University of Zurich
Patrick Honohan	Professor of Economics Trinity College Dublin Peterson Institute for International Economics Trustee, CEPR, London
Yi Huang	Assistant Professor of Economics Pictet Chair in Finance and Development The Graduate Institute
Takatoshi Ito	Professor School of International and Public Affairs Columbia University New York
Nadezhda Ivanova	Advisor to the First Deputy Governor Bank of Russia Moscow
Simon Johnson	Professor Sloan School Massachusetts Institute of Technology (MIT) Cambridge, USA
Thomas Jordan	Chairman of the Governing Board Swiss National Bank
Vivek Joshi	Principal Secretary Monitoring and Co-ordination Government of Haryana I ndia
Jean Keller	Chief Executive Director Quaero Capital SA Geneva

Signe Krogstrup	Advisor Research Department IMF
Jean-Pierre Landau	Professor SciencesPo Paris
Jan Langlo	Director Association of Swiss Private Banks Geneva
Valérie Lemaigre	Chief Economist Asset Management BCGE Geneva
Carlos Lenz	Head of Economic Affairs Swiss National Bank
Andréa M. Maechler	Member of the Governing Board Department III Swiss National Bank
Antoine Magnier	General Inspector of Social Affairs French Ministry of Labor and Social Affairs Paris
Michaël Malquarti	Senior Portfolio Manager Quaero Capital Geneva
Nikolay Markov	Senior Economist Pictet Asset Management Geneva
Aurelie Martin	Economist Autonomy Capital London
Robert McCauley	Senior Adviser Monetary and Economic Department Bank for International Settlements Basel
Alessandro Missale	Professor of Economics University of Milan
Carlo Monticelli	Vice-Governor Financial Strategy Council of Europe Development Bank – CEB Paris

Neha Narula	Director MIT Digital Currency Initiative MIT Media Lab Cambridge, USA
Judith Nemenyi	Senior Advisor Financial Research Institute Budapest
Dirk Niepelt	Director Study Center Gerzensee
Patrick Odier	Senior Managing Partner Banque Lombard Odier & Co Ltd Geneva
Fabio Panetta	Deputy Governor Member of the Governing Board Banca d'Italia
Ugo Panizza	Professor of International Economics Pictet Chair in Finance and Development The Graduate Institute
Pierre Pâris	CEO Banque Pâris Bertrand Sturdza Geneva
Yung Chul Park	Professor of Economics Division of International Studies Korea University
Alonso Perez	Portfolio Manager Wellington Management London
Avinash Persaud	Professor and Chairman Intelligence Capital Limited Barbados
Marcel Peter	Deputy Director International Monetary Cooperation Swiss National Bank
Adrien Pichoud	Chief Economist SYZ Asset Management SA Geneva

Huw Pill	Chief European Economist Global Macro Research Goldman Sachs International
Jean Pisani-Ferry	Professor SciencesPo Paris
Richard Portes	Professor of Economics London Business School European Systemic Risk Board Honorary President and Founder, CEPR, London
Frédéric Potelle	Head of Research Bordier & Cie Geneva
Fabrizio Quirighetti	CIO Multi-Asset & Fixed Income SYZ Asset Management
Bertrand Rime	Director Financial Stability Swiss National Bank
Alain Robert	Executive Vice Chairman Global Wealth Management UBS Switzerland AG
Andrew Rose	Professor Haas School of Business University of California Berkley
Valerie Rouxel-Laxton	Senior Fellow The Atlantic Council Washington D.C
Hans-Joerg Rudloff	Chairman Marcuard Holding London
Philippe Rudloff	Founding and Managing Partner Atlantis Marcuard Geneva
Nabil Jean Sab	Chief Executive Officer Compagnie Privée de Conseils et d'Investissements SA Geneva

Pierre Sicsic	Invited Scholar Paris School of Economics and Banque de France
Anthony Smouha	CEO Atlanticomnium SA Geneva
Sergio Sola	Economist Middle East and Central Asia IMF
Nicolas Stoffels	Head of Financial Markets Analysis Swiss National Bank
Livio Stracca	Head of International Policy Analysis Division European Central Bank
Katsiaryna Svirydzenka	Economist Asia and Pacific Department IMF
Alexandre Swoboda	Professor of Economics Emeritus The Graduate Institute
Gianluca Tarolli	Market Economist Research Banque Bordier & Cie Geneva
Leslie Teo	Chief Economist Economics and Investment Strategy GIC Private Limited Singapore
Cédric Tille	Professor of Economics The Graduate Institute
Albi Tola	Senior Economist International Monetary Cooperation Swiss National Bank
Pascal Towbin	Senior Economist Financial Stability Swiss National Bank
Angel Ubide	Managing Director Goldman Sachs & Co
Sebastian Weber	Economist European Department IMF

Ghislaine Weder	Head Economics and International Relations Nestlé SA
Charles Wyplosz	Professor of International Economics The Graduate Institute Director ICMB, Geneva CEPR, London
Attilio Zanetti	Head of Economic Analysis Swiss National Bank
Jean Zwahlen	Former General Director Swiss National Bank
Patrick Zweifel	Chief Economist Pictet Asset Management Geneva

Foreword

The Geneva Reports on the World Economy are published annually by CEPR and ICMB and have been providing innovative analysis on important topical issues facing the global economy since 1999.

This 21st report assesses the role blockchain technology can play in the financial sector and beyond. Assessing its core mechanism and its applications – in particular, Initial Coin Offerings and crypto-exchanges – the authors discuss the potential costs and benefits both within the financial context and beyond, providing details of a host of relatively unknown experiments that are under way. They explain how the possibility of substantial savings might lead to the erosion of large existing rents. They also list the many challenges that must be solved before the technology is actually adopted. In particular, the decentralized process through which transactions of all sorts can be verified requires absolute trust. Crypto-currencies provide strong incentives by offering the crypto-currency itself, in effect buying in the 'miners'. Blockchains must find other ways. This is one reason why current experiments limit access to known users, occupying a mid-ground between centralized and fully decentralized exchanges.

Despite its infancy, blockchain technology presents an opportunity to fundamentally transform the way financial markets work. The challenge is to reduce the cost of trust, to protect against criminal interference – money laundering and terrorism, for instance – to ensure that that the technology is appropriately adopted, utilised and governed. When and if these problems are solved, blockchains could provide enormous economic, social, and political benefits to society.

This report was produced following the Geneva Conference on the World Economy held in May 2018. CEPR and ICMB are very grateful to the authors and several discussants for their efforts in preparing material for this report, as well as to the conference attendees for their insightful comments. We are also thankful to Laurence Procter for her continued efficient organisation of the Geneva conference series, to Hayley Pallan for recording and summarising the discussions, and to Anil Shamdasani for his unstinting and patient work in publishing the report.

CEPR, which takes no institutional positions on economic policy matters, is delighted to provide a platform for an exchange of views on this topic.

Tessa Ogden
Chief Executive Officer, CEPR

Charles Wyplosz
Director, ICMB

July 2018

Executive summary

Blockchain technology – though still young and facing technical, commercial and regulatory challenges – has the potential to change many aspects of the financial services sector and the broader economy. New ways to intermediate capital and risk are emerging, providing a catalyst for change to incumbent financial sector firms. These technologies could improve automation across organisations and widen financial access. However, the technical and social infrastructure underpinning the technology is still significantly underdeveloped. Numerous technical challenges must be overcome – including performance, scalability, privacy, security, interoperability and governance – if it is to live up to any of its promise.

Prior waves of internet innovation overcame similar constraints over time, aided by ongoing enhancements to software, increases in basic computing power and investment in communications networks. With thousands of developers worldwide working on open source projects that aim to improve blockchain protocols and applications, there is reason to be optimistic that the technical issues will be addressed over time.

Yet the challenges are not just technical. The transition from existing business models to new arrangements potentially enabled by this technology is also hindered by commercial obstacles. Many companies and financial market utilities are trying proofs of concept or pilots, but none (to date) has applied blockchain technology to core business processes. Given that this technology's strength depends in part on multiple organisations using the same network – a structure that requires coordination among many parties – the path to incremental adoption is not clear.

In addition, blockchain projects need to be brought more fully within existing public policy frameworks. Rules that establish fair, efficient markets – and that protect investors – are just as important for blockchain-based decentralised financial products as for more established dimensions of finance. Also important and highly relevant are the policy goals of ensuring financial stability and guarding against tax evasion, money laundering and terrorism finance.

There are social and economic benefits from encouraging sensible innovation in blockchain technology that is consistent with established public policy goals. Properly introduced, the technology can mitigate the 'cost of trust', which manifests itself in numerous ways within the financial system and the economy (Casey and Vigna, 2018a; 2018b). In so doing, it could lower overall costs, reduce economic rents and create a more secure and fairer financial system.

In this report, we first provide a summary review of the basics of blockchain technology and its challenges, costs and benefits. We then give an overview of blockchain technology and the potential direct impact on the financial sector,

including a discussion of tokens, initial coin offerings (ICOs), and crypto-exchanges – all critical issues today. Building on this, we offer thoughts on possible use cases beyond the world of finance.[1]

Given the salience of public policy issues presented by the rapidly expanding markets for what we call 'crypto-finance', we provide a detailed review of ICOs and crypto-exchanges. Crypto-finance and token or coin trading have become the first significant applications of blockchain technology.[2] With approximately $300 billion in crypto asset market capitalisation, over 3,000 ICOs launched to date and 200 crypto-exchanges, this is a moment of decision for public officials and leading market participants. These markets currently operate with little or no investor protection, and are frequently subject to fraud, scams, front-running and other manipulative behaviour.

Following a discussion of public policy considerations and a review of the global regulatory approach to date, we explore in greater depth the current debates within the US and the possible path forward. Though a detailed review of all jurisdictions is outside the scope of this report, we believe the ongoing debates within the US are relevant to policymakers in all other locales where similar challenges arise.

1 We do not herein deal with the potential impact of cryptocurrency and related innovations on central banks and the conduct of monetary policy.

2 "State of the dApps: 5 Observations From Usage Data (April 2018)," *Medium*, 11 April 2018.

1 Blockchain technology basics

A blockchain is a unique type of computerised ledger, one that relies on cryptographic techniques and new methods for consensus to capture and secure the data. It is designed to be read by a computer, rather than by the human eye. A blockchain is denoted by the following characteristics:

- The ledger is shared among and worked on by multiple, possibly distrusting, participants, none of which has a single point of control over it.
- An ever-growing chain of ledger entries links the entire history in such a way as to prevent tampering with or rewriting past records.
- Digitally signed transactions or instructions indicate intent to record or modify data, or to transfer digital assets.

A brief history of consensus

Blockchains are built upon a well-known problem in computer science called *distributed consensus*. Distributed consensus is the problem of how multiple, independently run computers can reliably agree on a set of common data in the presence of faults – i.e., where there is a risk that one or more computers are intentionally or unintentionally programmed to introduce false information. This problem arises in large distributed networks like the internet, and many software companies employ distributed consensus algorithms to protect access to critical data, including Google, Facebook and Yahoo.

Pease et al. (1980) first posed the problem of consensus in a paper titled "Reaching Agreement in the Presence of Faults". Since then, computer science researchers have developed numerous systems to address the problem under different assumptions about the involved computers and the underlying network.

Systems with the strongest safety properties assume that the actors in the system might be *Byzantine* – which means they might be malicious and try to actively subvert agreement and introduce false data into the system. Such systems assume no limits on how faulty actors might act. The term comes from the Byzantine Generals Problem, posed in another paper by the same authors in which they describe a group of generals, each in command of a division of the Byzantine army, encircling an enemy city (Lamport et al., 1982). The generals must decide whether to attack the city or retreat. To complicate matters, some of the generals are traitors who are trying to sow disagreement, and the loyal generals must all attack or retreat together to avoid losses. The generals communicate by messenger to try to reach agreement on a strategy, and these messengers might be delayed or disappear. This problem maps nicely onto the distributed consensus problem, where the generals are computers, the traitors are faulty computers, and the messengers are data being sent over an unreliable network.

In a blockchain network, potentially Byzantine computers use a system of distributed consensus to agree upon the history of transactions in a ledger. Its first use stems from a white paper released in 2008 in which Satoshi Nakamoto proposed Bitcoin, a system for electronic, peer-to-peer payments (Nakamoto, 2008). In Bitcoin, rational, self-interested participants are incentivised to select and validate transactions made in its native currency, bitcoin. Through that process, they can agree upon a continually updated history of those transactions. Users have control over their bitcoin via a digital signature system by which they indicate consent to transfer coins. These digital signatures are public, cannot be forged, and can be verified by anyone. It is important that there is only one version of the transaction ledger because in order to verify a payment, participants look at the ledger to validate that an amount of bitcoin has indeed been transferred. If there were different ledger histories, a malicious user might be able to 'double spend', i.e., transfer a single bitcoin more than once, as two payments.

The consensus algorithm used to agree on the ledger in Satoshi's Bitcoin is based on participants competing to win rewards denominated in bitcoin. Its breakthrough feature is a 'proof-of-work' function, which imposes computation costs on each participant in the competition. The participants who engage in this process are called 'miners'. In essence, each miner collects a set of outstanding transactions, referred to as a 'block', while simultaneously competing to find a randomly chosen string of numbers and letters. Once a miner finds the required string, they broadcast it, along with the block, to the rest of the network and claim their reward, comprising a combination of freshly issued bitcoins and any fees that users have attached to transactions in the block. The competition for the next block begins, building on the chain of blocks that have come before. This is why the transaction ledger is known as a 'blockchain'.

Another important feature is that the Bitcoin protocol includes an algorithm that automatically adjusts the difficulty of completing the next block as the overall processing power of the computing network changes. As more miners join the network, the difficulty of the cryptographic challenge rises, and as miners leave it becomes easier to solve. Miners incur costs in the form of specialised computer hardware to solve the puzzle quickly and electricity to run that hardware. They will mine as long as the price of bitcoin is high enough to reward them for these costs. A core idea is that if the currency is valuable, then miners will be incentivised to continue building a single ledger faithfully. Anyone attempting to take over a sufficiently large number of miners to subvert the system and create multiple versions of the ledger would face increasing capital and operational costs to pay for the electricity and computer infrastructure. To date, that cost has proven prohibitively large for anyone to carry out such an attack.

Bitcoin's price in dollar terms has increased from zero to as high as $20,000 and was trading at around $6,500 per coin in July 2018. Despite that impressive valuation – which stands as a kind of natural 'bounty' or enticement for would-be hackers to try to break the system and steal funds – in nearly a decade, no one has broken the integrity of Bitcoin's blockchain. There have been no known instances of tampered ledger entries or evidence of miners trying to create multiple versions of the blockchain in order to double-spend bitcoin.

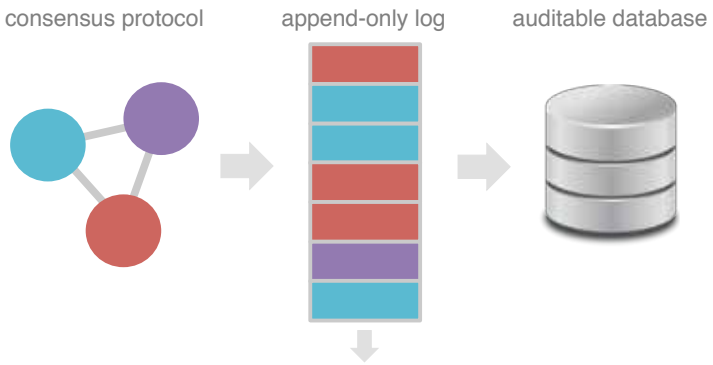
Another important feature of the network are the thousands of Bitcoin 'full nodes' in existence. Bitcoin full nodes are operating computers that observe and validate the Bitcoin blockchain, but do not generally mine new blocks. They serve as watchers over the blockchain. Full nodes do not receive any rewards in the protocol, but if a user is accepting a large payment in bitcoin, it is prudent for her to run a full node and validate that the blockchain includes the transaction correctly instead of relying on a third party or the miners.

The proof-of-work design used in Bitcoin – the competition to win bitcoin rewards – has become incredibly energy-intensive, raising concerns about its environmental impact, long-term sustainability and costly barriers to entry. In response, cryptocurrency developers are working on new consensus protocols, including a category called 'proof of stake', where participants vote on the true ledger weighted by how much stake, or currency, they hold in the system. The idea is that those holding the most currency have the greatest investment in the system proceeding securely. These designs have been launched in a few cryptocurrencies but are still experimental.

Blockchain technology and distributed databases

The essential features of a blockchain are that it is a consensus protocol used to create an append-only log (in the case of Bitcoin, a transaction ledger) that can then be used to form an auditable database (in Bitcoin, a record of who owns what coins).[3] This database is constructed by multiple, possibly distrusting participants and is secured using cryptography so that every entry can be audited and verified (Figure 1).

Figure 1 Elements of a Blockchain system



3 As recorded in the UTXO, or unspent transaction output, set.

Bitcoin's breakthrough contribution was to create a means of achieving consensus within an open, 'permissionless' environment – anyone can join the Bitcoin network and become a miner, compete for bitcoin currency rewards, and contribute to the ledger by engaging in proof of work. Today, however, many projects – especially in finance – are considering using blockchain technology in a more closed environment, and without the presence of an in-protocol currency (see Chapter 3).

These systems are known as 'permissioned' (or 'private') blockchains. There is a limited set of entities, or perhaps just a single organisation, allowed to write to the blockchain. This type of permissioned design is not necessarily new. It relies on distributed database technology and cryptographic techniques that are decades old, including distributed consensus algorithms, hashing and signatures. As permissioned blockchains raise questions about what should or shouldn't be called a 'blockchain', the term 'distributed ledger technology' (DLT) is often used to describe this field in broader, generic terms. It's clear, however, that the recent wave of DLT development and deployment was motivated by the success of Bitcoin and, subsequently, of other permissionless cryptocurrency systems.

Though the permissioned version of this technology is not new, many of the use cases are. Organisations for years have run their own individual databases, and continue to use costly reconciliation procedures to make sure their data are consistent across the ledgers of their counterparties. An expensive manifestation of this is the work done reconciling orders between different financial institutions. What is new with DLT is that multiple organisations are now further inspired to work together on a shared common, auditable database. Institutions are looking into blockchain technology, enabling users to maintain more control over their data while sharing them efficiently between organisations.

Smart contracts

In addition to keeping a ledger of ongoing currency transfers, blockchains can also reliably record other types of time-sequenced data, including processing the steps required to execute programs known as 'smart contracts'. Smart contracts digitally facilitate and enforce the transfer of digital assets according to software-defined contract conditions. For example, a company might execute a blockchain smart contract to pay a customer a digital asset if and only if a specific software clause is triggered by a mutually acknowledged change of state.

A key property of smart contracts is that they do not require a trusted third party such as a trustee or an escrow agent to intermediate between the contracting entities; the blockchain network enforces the execution of the contract on its own. This has the potential to reduce friction when transferring value between entities and opens the door to more automation of transactions.

Not all blockchains have the same capabilities with regards to smart contracts. Bitcoin supports a scripting language which facilitates only a small set of smart contracts. Other platforms, including Ethereum, NEO, EOS, LISK and Stratis,[4] support full-featured smart contracts and, by extension, enable the creation of distributed applications (known as dApps)

4 "Ethereum Competitors: Guide to the Alternative Smart Contract Platforms", Blockonomi, 28 February 2018.

Smart contracts and dApps allow new organisational arrangements between individuals and entities, creating pre-programmed transactions that potentially lessen the need for management or trustee decision making. These innovations have already raised technological, commercial and regulatory challenges.

For example, when an attacker exploited a smart contract flaw to siphon off over $50 million from The Decentralized Autonomous Organization (DAO) – a fundraising vehicle that raised $168 million when it was launched on Ethereum in 2016 – the Ethereum community questioned the principle of maintaining the ledger's immutability. The Ethereum Foundation decided to intervene on The DAO investors' behalf – in effect, bailing them out – by rewriting Ethereum's core code to delegitimise the attackers' transactions and recover the funds. To do so, the Foundation, influenced by the platform's heavily invested founders, convinced most users to go along with its decision. But this breach of immutability was a controversial move, and one that prompted a split in the Ethereum community – one splinter group decided to stick with the original, unamended code.

Adding to the controversy, the U.S. Securities and Exchange Commission (SEC) later issued a report that The DAO was a security issued in violation of securities laws. Though the SEC declined to take enforcement action, it was an important warning that ICOs and similar tokens (described below) are likely investment contracts and subject to US securities laws (see Chapter 4).

Tokens

Companies, foundations and open source projects have begun issuing their own tokens, intricately tied to the operation of their platforms. Some developers are doing so by creating their own token-backed blockchain platforms, following the Bitcoin model. Others have done so by issuing a new token managed by a smart contract 'on top' of an existing blockchain network. In the latter case, the underlying blockchain network's computers validate the token's transactions via the work they do processing and implementing the smart contract. (The most common example uses the ERC20 standard, by which tokens are issued on top of Ethereum).[5] Each token conforms to a set of rules, enforced by the smart contract, to which all users of the token implicitly agree.

What emerges is a 'token economy' in which a community, in theory, embeds incentives and disincentives into its medium of exchange. Potentially, this is a way to achieve internal governance of shared resources and coordination in the interests of a public good. Whether it is achievable is still an open question. The token market, discussed more fully in Chapters 3 and 4, is very volatile and experimental at the moment.

Currently, what is labelled a 'token' versus a 'cryptocurrency' remains unsettled. Cryptocurrencies are always generated by their own blockchains (as with Bitcoin or Litecoin) whereas tokens are usually issued within a smart contract managed by a blockchain network such as Ethereum. Most cryptocurrencies – including those based on copies, or forks, of existing cryptocurrencies – were brought into being through the mining process. Tokens may be sold to investors to pay for

5 See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

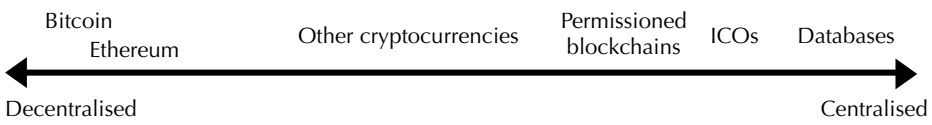
development of an application or blockchain platform. In some cases, however, both processes are used. Ethereum itself first had an initial coin offering of its native token, known as ether, and applied the funds to the Ethereum Foundation, but it has subsequently relied on mining to issue new coins.

A spectrum of decentralisation

Different blockchains, ledger-keeping systems, tokens and cryptocurrencies can be viewed on a spectrum of decentralisation, shown in Figure 2. On the decentralised end are systems like Bitcoin and Ethereum, which are permissionless, with no restrictions on who can join the system and participate in creating the ledger. But even within this category there are differences of degree. The Ethereum Foundation was able to intervene in order to organise a response to The DAO, while there has never been any such action in Bitcoin, making Ethereum slightly less decentralised than Bitcoin from a governance standpoint.

On the other end of this continuum is a traditional centralised database. In between are other tokens and various kinds of permissioned blockchains. Some tokens are relatively decentralised, while others have built-in governing organisations that ensure a higher degree of centralisation. It could be argued that any tokens that are initially issued or sold to fund development of a network are by definition centralised at that moment, because there is an organisation collecting funds to create the network. On the other hand, the smart contracts that track the subsequent secondary market trading in those tokens can be audited by computers operating within a more decentralised blockchain platform such as Ethereum.

Figure 2 The spectrum of decentralisation



As discussed more extensively below, the type of decentralised security provided by systems like Bitcoin and Ethereum is quite costly – at least in operational terms. If there is a trusted third party to secure the ledger, operating costs are likely to be lower than with a decentralised blockchain, as are the costs of achieving consensus among different entities. Trusted third parties, however, do not always exist, which forces reliance on less-secure alternatives or makes some forms of economic activity impractical, resulting in an opportunity cost of foregone value formation. In such cases, a blockchain could still represent a cost-effective solution. There are also situations where trusted third parties exist, but they charge users high rates as economic rents. As discussed below, any decision on whether to introduce a blockchain should weigh the potential to reduce these various instances of the 'cost of trust' against the high operational and social coordination costs of installing and running a blockchain. In the next chapter we discuss numerous costs of trust (physical safes, for example) that are a form of operating cost.

Protocol layers - an analogy to the internet

The internet is built on a stack of open protocols that dictate how a decentralised, global network of computers exchange data in the form of information packets. These protocols include ethernet to connect computers together, TCP/IP to create networks, HTTP/HTML for the web, SMTP for email, SSL/TLS for security, and more (Figure 3). Many applications are built on top of this base-level web, including large centralised platforms like Facebook and Google. Advertising revenues and capturing users' data have become the predominant business models of many internet platforms.

Figure 3 The internet protocol stack

Layer	**Protocol**
Application	HTTP
Internetworking and transfer	TCP/IP
Link	Ethernet

Blockchain technology may represent additional possibilities for open protocols, adding a new decentralised system for exchanging value – in the form of digital assets or tokens – to the existing ones that simply manage information. And once the first blockchain technology layer facilitates the transfer of value, other layers could be added on top that facilitate the application of code or contracts along with more complex digital assets.

However, it is too soon to know which specific protocols will end up forming the layers of what some have called the 'Internet of Value' (Figure 4). In fact, the base layer, comprising a fully digital currency with software features (programmable money), might not be a decentralised cryptocurrency at all. That medium of exchange might just as well be issued by the computers of a central bank rather than by an algorithm that runs over a decentralised computing network.

Figure 4 The internet of value potential stack

Layer	**Protocol**
Decentralised exchange	
Smart contracts	
Transactions and payments	Cryptocurrency or digital fiat

Just as the internet spawned many applications that changed the way we communicate and find information, we expect blockchain technology will directly or indirectly change the way we transact and exchange value. Applications we are unable to predict today may emerge.

One potential area for innovation is micropayments. It is currently infeasible to accept payments in fractions of a cent, but a more scalable version of blockchain technology could in the future allow cheap, fast, tiny payments. These payments might not only be between people and other people or institutions (such as firms), but also between autonomous machines within the Internet of Things. This could fundamentally change business models and allow communities to more precisely manage the allocation of scarce resources. Music platforms, journalism and other internet services might be able to add a micropayment-based revenue model to supplement, or perhaps even replace, existing advertising revenue models.

2 Blockchain technology's opportunities and challenges

Impediments to broad adoption

Blockchain technology offers a commonly agreed record of truth to multiple, mutually distrusting participants in an economic system. Benefits may be derived from removing the requirement for participants to trust a particular person or entity to maintain that record on their behalf, opening the door to more direct, peer-to-peer (or machine-to-machine) transactions or to the independent execution of smart contracts. Thus, the technology could reduce overall friction in the system, cut processing time, lower barriers to entry, and reduce back-office costs involved in reconciling data across organisations. Business models that were previously not feasible because of either trust barriers or the processing costs inherent in specific existing arrangements might now be imaginable. These include those that rely on micro-transactions where payments are in fractions of a cent and highly automated exchanges of money and data between devices in the Internet of Things.

These potential advantages have fuelled rapidly growing enterprise interest in the prospect that blockchains and DLTs could improve business efficiency. In a Juniper Research survey, whose results were published in August 2017 (Juniper Research, 2017), 39% of 400 company founders, executives, managers and IT professionals confirmed that their companies were either deploying or considering deploying blockchain technology, while 36% replied "no" to that question and 25% said "don't know". The number of "yes" responses rose to 56% for companies of more than 20,000 employees, and of all those who said they are working on proofs of concept, two-thirds said they expect to integrate the technology into their systems by the end of 2018. Each of the Big Four accounting and consulting firms has built up blockchain technology advisory teams now staffed in the hundreds, all pushing their clients to engage with the technology. In another measure of enterprise development, there were 406 blockchain technology patents filed in 2017 in addition to 602 separate cryptocurrency patents, according to the *Financial Times* (Noonan, 2018).[6]

Multiple consortia have been formed, comprising mixes of large-scale corporations and start-ups, to explore common open source blockchain technology solutions for particular industries. The biggest banks formed a group called R3CEV, for example, before expanding to a membership of greater than 100 that included many non-banks. Hyperledger, which has been building private enterprise solutions, is similarly large and includes big players such as IBM, Cisco and Intel. Meanwhile, blockchain consortia have also been formed for the music, advertising, energy, Internet of Things (IoT), real estate and various other industries.

6 "China leads blockchain patent applications", *Financial Times*, 25 March 2018.

Government agencies, non-government organisations and international development agencies are also now exploring multiple use cases aimed at enhancing official information, streamlining government-citizen relationships and boosting financial inclusion. The World Bank and the IMF, to cite two examples, have both started their own blockchain labs over the past year.

Yet for all of the possible promise that this flurry of enterprise activity reflects, we currently see relatively little in terms of real-world practical deployment. That is because there are still significant challenges to broad adoption of blockchain technologies.

First, the performance, scalability and efficiency of blockchain technology are currently limited. Though many advances have already been incorporated into the various programs, by their very design most existing blockchains are complex and laden with attendant latencies, which limits their transactional capacity. The complexity, and related inefficiency, may be integral to a design that permits security in a decentralised system. But that doesn't preclude this complexity from posing a barrier to the technology's advance.

Bitcoin is able to process between seven and ten transactions per second, and Ethereum approximately twenty transactions per second.[7] Based upon a centralised trust model, the Visa network can process an estimated 24,000 transaction messages per second. Bitcoin transactions during particularly active times, such as in December 2017, can take many hours to settle – especially if the transaction fees attached to those transactions are not high enough to sufficiently incentivise miners to promptly include the transactions in blocks. This is due to the fact that there is limited space in the blockchain for transactions, so when there is congestion, miners will select the transactions with the highest fees. Meanwhile, Bitcoin and other similar proof-of-work cryptocurrencies use significant energy resources.[8] These expenses and inefficiencies are at loggerheads with the needs of many parts of the financial sector, including payments as well as currency, bond and stock trading, which have very high volumes and require low latency.

It is possible that over time further advances in blockchain technologies will address many of the current performance and efficiency issues. In particular, 'Layer 2' solutions such as the Lightning Network, in part developed at the MIT Media Lab's Digital Currency Initiative, aim to greatly reduce cost and time constraints by shifting small transactions to a cryptographically secure 'off-chain' environment so that only large netting transactions need to be directly settled into a resource-constrained blockchain.[9] Other projects are designed to allow 'cross-chain' interoperability, which could support a bigger, fluid whole of value exchanges.

These nascent solutions, however, remain unproven in the real world. They also involve potential economic and security trade-offs. For some time, it remains likely that use cases requiring low latency or high volumes will be better served by centralised database systems.

7 "Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?", HowMuch.net (accessed 11 June 2018).

8 There is a wide range of estimates regarding exactly how much electricity Bitcoin uses; "How much energy does bitcoin mining really use? It's complicated", *WIRED*, 2 December.

9 See https://dci.mit.edu/lightning-network/.

Second, there are concerns about privacy and security, which create somewhat contradictory tensions. Some stakeholders, particularly in the law enforcement and regulatory sectors, are concerned that the pseudonymous nature of blockchain-based records obscures the identity of actors. By contrast, others – most notably, financial institutions – worry that privacy protection is not strong enough, since the first distributed ledgers were designed with transparency in mind, allowing all participants to view every transaction. Information about participants can be gleaned from patterns in the transaction graph and balances in the unspent transactions outstanding (Meiklejohn et al., 2013).

There is much at stake on both sides of this debate. The official sector wants to foster public policy goals of financial stability, investor protection, customer protection and market integrity, and to guard against illicit activities such as money laundering, tax evasion or terrorism financing. The private sector wants to guard the privacy of their data. Corporations have both commercial and legal reasons to do so. Individuals have legitimate reasons to wish to maintain their privacy, but some also may wish to do so to thwart government oversight.

There are many interesting solutions being developed to address this inherent tension between privacy and detecting illicit activity. These projects aim to preserve privacy while at the same time allowing regulators to gain insight into the operation of the blockchain system. A useful and well-tested cryptography algorithm ('cryptographic primitive') that many of these solutions employ are *zero-knowledge proofs*.[10] Zero-knowledge proofs let someone prove a statement is true (for example, "I am over the age of 21") without revealing the details of exactly *why* that statement is true (for example, "because I was born on 25 June 1980.") Zero-knowledge proofs are used in Zcash, a privacy-preserving cryptocurrency.[11] JP Morgan has also experimented with zero-knowledge proofs in Quorum, its permissioned blockchain system.[12]

A project at the MIT Media Lab, zkLedger, lets participants work together on a blockchain where transactions are completely private but can still be verified by all participants (Narula et al., 2018). In zkLedger, a third-party auditor or regulator can obtain provably correct answers to queries about the system as a whole – for example, to learn the concentration of assets, leverage ratios or real-time price indexes – without needing to uncover the details behind private transactions. This and other zero-knowledge proof projects show that privacy and regulation need not necessarily be at odds, and that cryptographic primitives can help alleviate this tension.

Related to these issues is the security of the data and digital store of value. Though Bitcoin and many blockchains themselves have generally been resistant to hacks, with the integrity of their ledgers preserved, there have been numerous reports of hacks in other areas and layers within the crypto ecosystem. This has been particularly so with trading venues for cryptocurrencies (commonly referred to as 'crypto-exchanges') and certain wallet providers that take custody

10 There are many other cryptographic primitives including for example public key cryptography, digital signatures, and one-way hash functions.

11 See https://z.cash/

12 "JP Morgan integrates Zcash privacy tech into Quorum blockchain", coindesk, 17 October.

of users' funds.[13] Well over 90 % of daily trading volume in bitcoin occurs through crypto-exchanges rather than being recorded as a transaction directly within the blockchain. Many crypto-exchanges, wallet companies and individuals are not sufficiently versed in best security practices and so remain vulnerable to attack.

Third, there are challenges relating to the interoperability of blockchain applications. The success of most use cases will depend upon linking in some way to legacy infrastructures, databases and technologies, raising questions about who to trust in coordinating the transfer of assets and information into the blockchain or across chains. The goal, many experts believe, is to enable decentralised mechanisms for asset transfers in these situations. Though potentially achievable, there is a great deal of work needed to achieve seamless movements of data and applications between and amongst new DLTs and existing architecture.

Many of the solutions aimed at improving the scalability blockchain's processing capacity (e.g., Lightning, Cosmos and Polkadot) might also extend to achieving interoperability across blockchains. Interledger is one of the most promising solutions to help blockchains integrate with the existing financial system. Interledger defines a protocol for moving value across different systems, whether they are decentralised or centralised.

Fourth, there are trade-offs relating to the governance of blockchains, particularly with regard to software updates. In a centralised environment, some trusted authority controls much of the governance of a system. It can develop, test, publish and promote software updates, for instance, without requiring the consent of users. One of the features of blockchains is that, for certain software updates, there must be a consensus amongst a distributed network, for which there is no controlling entity, to amend the underlying software. For contentious software updates, particularly with value at stake, that can be hard to achieve.

When a full consensus has not formed, various blockchains – including Ethereum – have experienced chain splits. These can arise when a change in software that is adopted by some participants is incompatible with the earlier version that fielded and propagated the previous validation rules of the chain and which a dissenting group continues to use. This division leads to what is called a 'hard fork', or a split in the chain.

Fifth, most of the real-world usage so far has been around cryptocurrency speculation. Many established companies are engaging in pilots and proofs of concept regarding how to use blockchain technology, but none has as of yet transitioned to relying on a blockchain for critical functions. In Chapter 5, we discuss several applications under development, but it remains to be seen which use cases beyond cryptocurrency will end up gaining commercial adoption.

Sixth, because blockchain applications derive their value from the participation of multiple parties in a network, adoption requires collective action. This may be why many current projects involve consortia. Regulatory uncertainty also may increase the perceived risks of being a first-mover.

13 More recently, a MIT Digital Currency Initiative team found a vulnerability in IOTA, the 9th ranked cryptocurrency by market capitalisation (see https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367).

Seventh, for blockchain technologies to reach their potential, both in applications as well as for investing, they need to be more fully brought within public policy and legal frameworks – very much as has happened with new technologies in the past. Only with clear rules of the road – adapted in some circumstances, while remaining true to the core public policy goals of existing laws – will there be broad adoption of blockchain technologies, along with their potential to transform the industry.

A framework for understanding transaction costs and trade-offs

Blockchain technology has the theoretical capacity to apply to and disrupt any form of value or data transfer recorded in a ledger. As discussed in Chapter 1, blockchains and other distributed ledgers are distinguishable from existing databases primarily by their distributed architecture and their use of consensus mechanisms that avoid reliance on centralised, trusted intermediaries.

But, given the combination of current challenges outlined above, some people are legitimately asking of proposed blockchain applications: Why a blockchain? For any particular use case, decision makers need to ask: What makes blockchain technology, with all of its complexity and costs, a uniquely qualified tool to solve that problem? One key metric to consider for any project is an estimate of the cost of trust – the costs borne by transacting parties because they have to rely on either their counterparty or a trusted intermediary to honestly record completion of the transaction.

Blockchain technologies have the potential to reduce these costs, by overcoming barriers of trust or by bringing transparency and automation to existing processes. The technology can reduce accounting and reconciliation procedures or forge access to services and business relationships. Blockchain technology achieves trust in a new way and with its own set of costs. Assessing the relative trust-related costs and benefits – of existing centralised systems on the one hand relative to a DLT system on the other – is a key consideration in assessing the potential benefits of a specific blockchain solution.

Ronald Coase's theory of the firm offers a useful way to frame these questions. In 1937, Coase articulated a theory for why most economic activity is carried out by centralized entities – firms – rather than being organized solely by "the price mechanism" in a series of market transactions (Coase, 1937). His theory, which has since become well-established in both the legal and economics literature, pointed to transaction costs as the barrier to a more fully market-based economy. In particular, Coase argued that activity would be organised within a firm when organising the same activity via a series of market transactions would incur higher transaction costs.[14]

Applying Coase's theory of the firm to blockchain-based applications, one may assess the relative costs and benefits of operating a given type of financial transaction on a distributed basis versus relying on an intermediary. To the extent that a blockchain or other distributed ledger solution results in lower transaction

14 "The main reason why it is profitable to establish a firm would seem to be that there is a cost of using the price mechanism. The most obvious cost of 'organizing' production through the price mechanism is that of discovering what the relevant prices are. … The costs of negotiating and concluding a separate contract for each exchange transaction which takes place on a market must also be taken into account" (Coase, 1937).

costs, distributed applications will become more attractive relative to centralised (i.e., intermediated) applications. Understanding how this technology could achieve those improvements comes down to how it can mitigate the transaction costs embedded in incumbent organisations and processes.

Software technology has reduced transaction costs across a vast range of economic activity over the past several decades. This has led to increasing economies of scale, and economic dominance for those individual firms who achieve sufficient scale to make the entrance of competitors prohibitive. Meanwhile, various forms of digital technology have enabled the coordination of global supply chains and the outsourcing of many factors of production, leading in many cases to a disaggregation of the firm – from outsourced call centres and IT functions to on-demand transportation and distributed short-term lodging.

Blockchain technology's disruptive potential may be viewed through a similar lens – where the benefits of an open, decentralised architecture exceed the transaction costs of operating and maintaining such a distributed network, activity will be decentralised.[15]

Blockchain technology makes possible the secure, verifiable transfer of value between parties who do not trust each other, without the use of a mutually trusted third party. This is achieved, however, by requiring a decentralised network to process every transaction, creating latency and capacity constraints, and often consuming significant resources. In other words, blockchain technology can potentially reduce the 'costs of trust' and economic rents imposed by reliance on trusted centralised intermediaries, but only if those collective costs and rents are greater than the costs inherent in achieving distributed consensus in a secure manner.

One may assess the benefits of using a blockchain (or other distributed ledger) technology to overhaul an existing economic activity by asking:

- What are the benefits to managing that activity in a distributed manner as opposed to centrally? Asked another way: What costs imposed by the trusted intermediaries in a given market – in the form of inefficiency or rent extraction, for example – can be eliminated by transitioning to a blockchain or distributed ledger? Or what security benefits may be achieved by decentralisation?
- Which inefficiencies and technical limitations of distributed systems – capacity constraints, governance challenges, privacy – pose particular challenges for the activity in question? Can those constraints be sufficiently addressed while preserving some of the benefits of decentralisation for this particular use case?
- Finally, are the gains to be derived from moving a given process to a blockchain sufficiently large as to compensate for the switching costs (i.e., to overcome entrenched network effects)?

Any given application of blockchain technology must consider certain inherent trade-offs between the relative benefits and costs of centralised market structures versus distributed networks.

15 Taken to their extreme, some proponents contend that blockchain technology could portend fully embedding certain governance and decision-making into the network protocol, with a blockchain, for example, enabling fully disaggregated firms, in which there is no identifiable authority managing the operation. The DAO, mentioned above, was an early attempt at this idea of a distributed autonomous organisation. That particular design ran afoul of US securities laws and collapsed due to a flaw in its code.

There are often benefits to distributed solutions, in the form of reduced costs of intermediation. For example, secure, verifiable transactions can significantly reduce operational and counterparty risk – no more waiting multiple days to see if your counterparty actually pays you or delivers the securities you purchased. Another common cost is the need to reconcile transactions between different centrally maintained ledgers. Among investment banks, blockchain technology could reduce reconciliation and other infrastructure costs by $8–12 billion a year, according to one report discussed below.[16]

But those benefits must be weighed against several disadvantages – at least with regards to the existing state of the technology. In financial sector applications to date, the most notable challenges have been the capacity constraints and latency imposed by proof-of-work consensus, the potential lack of privacy on a decentralised blockchain, and governance constraints.

Vitalik Buterin, the founder of Ethereum, has suggested that existing blockchains cannot achieve scalability – i.e., overcome the capacity constraints described above – without sacrificing either decentralisation or security.[17] The capacity constraints, and associated latency, of decentralised blockchains – in particular those employing proof-of-work consensus – make using them directly untenable for certain applications. Decentralisation currently comes with an added challenge for many financial services applications relating to transparency, which can be incompatible with competitive considerations and regulatory requirements in many markets.

To date, attempts to address the capacity limitations of blockchain-related applications have typically involved moving most transactions off-chain, and periodically recording a 'net' basis on-chain. Other efforts are focused on alternative mechanisms for achieving consensus, such as 'proof of stake', which is still largely untested and risks centralising control in the hands of parties who accumulate large ownership positions. Other efforts attempt to break up a blockchain into several smaller chains that can be interlinked, but these raise risks that any one of those mini-chains may be vulnerable to compromise or centralisation. Meanwhile, there is a promise in zero-knowledge proofs, discussed above, and other proposals to protect privacy on decentralised networks. However, these too remain untested in financial systems.

In summary, proposals to address scalability and privacy concerns also appear to entail some form of trade-off. Utilising a blockchain or distributed ledger for a particular use case will involve assessing the relevant trade-offs and optimising along the dimensions that matter most for that application. In the case of established financial firms' experiments, most of the applications currently under development involve private, or permissioned, networks. The financial sector is, in effect, choosing security and scalability over decentralisation. That has meant that most financial sector applications – outside of cryptocurrency trading on decentralised exchanges – still rely to a significant degree on trusted intermediaries, and thus retain many of the associated 'costs of trust'.

16 "Blockchain could save investment banks up to $12 billion a year: Accenture", Reuters, 17 January 2017.

17 "On the Scalability of Blockchains", The Control, 23 March 2018.

Non-financial sector applications may seek to optimise along other dimensions. Health records, for example, will require solutions that can address privacy and security, but may not require the same capacity as several financial applications. Chapter 5 explores a variety of applications and assesses some of the trade-offs that may be necessary to achieve adoption.

To illustrate the interplay of some of these key trade-offs, and consider how transaction costs may influence blockchain adoption, we examine some basic economic properties of blockchains.[18]

First, a broad range of blockchain and DLT applications appear likely to exhibit demand-side efficiencies of scale, or network effects. One approximation of the utility of blockchain applications might, therefore, be suggested by Metcalfe's Law, a rule of thumb for measuring the value of networks such as fax machines or social networks.[19] While blockchain applications are likely subject to numerous competing considerations, the presence of network effects suggests that the economic benefits of a blockchain application would increase at an accelerating, non-linear rate as the number of users increases.[20] This may apply with respect to some efficiency gains as well – that is, the efficiency gains from reduced reconciliation costs or counterparty risks increases as the number of participants increases. Some 'costs of trust', on the other hand, are likely to be closer to fixed costs – for example, the costs of regulating a market utility.

The permissioned blockchains under development for most enterprise applications might exhibit significantly different properties than the decentralised blockchains discussed above. They will likely operate much like centralised systems. However, by moving to a shared ledger, and digitising and streamlining processes that are currently heavily manual or cumbersome, the entire cost curve may be shifted downward, reducing overall transaction costs. Indeed, many financial services-related blockchain or DLT projects are justified on the basis of cost savings and efficiency gains.

In applications like digital identity or medical records, centralised systems may be inferior because they incur many of the costs and insecurity of centralised systems – think of the Equifax data breach or an equivalent breach of health information. A decentralised solution may therefore be preferable even in the absence of strong network effects or scalability solutions.

In short, the trade-offs for each use case must be assessed relative to the dynamics important to that use case. In the following chapters, we explore several potential use cases and attempt to highlight the relevant trade-offs.

18 These are based, where possible, on data from transactions, but given the early stages of blockchain applications there are few sources of meaningful data outside areas involving cryptocurrency trading.

19 Metcalfe's Law estimates the value of a network as the square of the number of users, as that is the number of connections each user has in that network. Competing theories suggest different valuations for social networks. While the price of bitcoin appears to have borne some correlation with Metcalfe's Law ("Valuing Bitcoin and Ethereum with Metcalfe's Law", *Medium*, 13 February 2018), we caution that this is not an empirically established relationship, and given the diverse array of motivations for purchasing bitcoin it is likely that any simple valuation metric would be misleading at this time.

20 "The internet of things is in your future - the law says so!", Tech Target, 10 October 2016.

3 Blockchain technology and finance

Where could blockchain technology have an impact?

As we have noted, blockchain technology can mitigate the cost of trust, something that manifests itself in numerous ways within the financial system. These costs range widely – from those associated with vault doors, cybersecurity, settlement procedures, user identification, compliance teams, security guards and anti-fraud regimes, to the excess amounts that banks and other centralised institutions can charge customers. Trust exists in the fundamentals of deposit banking, custody, insurance and secondary market trading. Depositors must trust the safety of their money at a bank. Market participants trust that their trades will be executed fairly according to a transparent set of rules. Financial institutions must trust costly back-office processes to reconcile centralised ledgers and accounting systems.

In an effort to address these various costs, DLTs are being explored by institutional actors such as large banks, exchanges, clearinghouses and central banks, as well as by new firms seeking to disrupt existing business models. Incumbent firms are hoping the technology can help them lower costs and risks, particularly for back-office or post-trade functions. Start-ups are aiming to provide the public with better and lower priced services while possibly capturing part of the significant economic rents within the financial services sector. And with the growing public interest in cryptocurrencies and ICOs, many firms are looking to capitalise on this burgeoning market to raise funds.

The financial services sector, like other important sectors of our global economy, has faced numerous challenges and exhibits some flaws. History is replete with banking and financial sector crises. Tens of millions of people around the globe lost their jobs or their homes as a result of the 2008 financial crisis. Though there is a need to carefully explore and consider how adoption of blockchain technologies and DLTs will affect financial stability, it is also worth exploring how these technologies, less reliant on centralised institutions, might help build a more resilient financial sector. Centralised intermediaries concentrate risks and often are able to collect significant economic rents (Zhang, 2017). The 2008 financial crisis is but the latest reminder of the long history of concentrated risk in the financial sector. As such, current methods for clearing and settling transactions, though vastly improved from earlier generations, remain costly with many reconciliation and counterparty risks. Furthermore, many financial products have high transaction costs and financial inclusion is uneven in many parts of the world.

In particular, the duplicative and time-consuming post-trade processes that banks, brokerages, custodians and clearing houses undertake to reconcile multiple ledgers represent a very large cost of trust embedded in the existing system.

As referenced above, for the top ten banks alone, blockchain technology could reduce infrastructure costs by 30%, translating into savings of between $8 and $12 billion. The figure would surely be significantly higher when applied to all institutions within the financial system.

Moreover, the Accenture figure only estimated expenditures on back-office functions, it did not incorporate the opportunity cost that is incurred by institutions that must lock up capital for long periods of time – ranging from two days to weeks, depending on asset class – until trades are settled. Those delays are imposed by the current system not because it is technically impossible for clearing houses such as the Depository Trust and Clearing Corporation (DTCC) to settle transactions in close to real-time, but because the many hops across multiple institutions introduce the risk of errors and delivery failures. The delay, in other words, represents a high-cost compromise for addressing the cost of trust in a cumbersome system of siloed, centralised ledgers.

On the customer-facing side, too, the cost of trust plays out in many forms. Financial inclusion is lacking (including in the developed economies such as the US) and transaction costs are high (for example, there are economic rents in interchange fees, which are high based on the cost of the latest technology.)

Blockchain and DLTs are being explored to address these various costs of trust, with potential use cases that span the lifecycle of transactions from all corners of the financial sector. Below we highlight some of the more fully developed financial services applications, saving a discussion of non-financial applications for Chapter 5. Most of these potential use cases are still in the research and development or proof-of-concept stage, with very few having reached the point of being introduced, even on a pilot basis, into a live production environment.

Payments

The existing approach to cross-border payments is slow and expensive, tying up large amounts of liquidity. Moreover, payment processes are often opaque, creating pricing uncertainty and increasing fraud and counterparty risk. Accordingly, remittances and foreign currency payments were one of the first potential applications of blockchain technology to receive attention.

Foreign exchange payments currently rely on so-called Nostro accounts – accounts held at other banks in those banks' local currencies – or on correspondent banking networks. These layers of intermediation increase costs and introduce operational complexity and counterparty risks.

Ripple uses a blockchain-based protocol, Interledger Protocol, to connect existing bank ledgers to facilitate near real-time cross-border payments. Ripple may also reduce costs and provide additional pricing transparency by running instant auctions to source FX liquidity at the best price available. Twenty-two banks, working with R3CEV's Corda, are testing a real-time international payments solution using Corda's permissioned, 'blockchain-inspired' distributed ledger. Because interbank payments are large and relatively less frequent, the benefits of increased transparency, reduced liquidity constraints and faster settlement may outweigh the limitations imposed by capacity constraints of DLT. SWIFT currently processes around 15 million messages per day, well beyond the

capacity of existing blockchains but not inconceivable in the future with some of the improvements under development. Moreover, to date all DLT initiatives under development rely on private, permissioned distributed ledgers, which makes it easier to address both confidentiality and scalability concerns.

However, those benefits will have to be sufficient to overcome the inertia of existing processes. And existing market infrastructures are not standing still. SWIFT, the dominant existing global interbank payments messaging network, has responded with its own Global Payments Innovation Initiative, presumably designed to achieve enough new efficiencies to stave off competition without making itself redundant. SWIFT recently completed a proof of concept with 34 banks, incorporating DLT – specifically, Hyperledger Fabric – into its own architecture. The SWIFT pilot was designed to streamline Nostro account reconciliation, eliminating one of the largest delays in cross-border payments, and to provide more transparent payment tracking and up-front pricing.

The technical challenges related to speed, capacity, cryptocurrency-to-fiat currency price volatility and transaction costs may inhibit development of a broader blockchain-based payments system. Developments using 'Layer 2' are starting to address these constraints,[21] though it is still early days. Without new developments it is still prohibitively expensive and slow to facilitate small point-of-sale transactions. Requiring users to pay several dollars in transaction fees and wait an hour for a payment to clear is not compatible with purchasing a coffee or a book from Amazon. Current payment rails are generally slower, of course, but the risk associated with delayed payments is borne by all those trusted intermediaries, principally card networks and banks. As such, work is warranted to bring more stability and real-time, decentralised efficiency to most payments use cases.

Digital identity/know your customer

Financial institutions, in order to comply with 'know-your-customer' obligations and 'beneficial ownership' requirements, verify numerous data points about every potential corporate and individual customer. To reduce the massive duplication inherent in existing KYC checks, banks and other traditional service providers are looking to become 'KYC bureaus', with DLT potentially standing in as the cross-institution source of proof. These institutions are creating models by which account-holders can export the institution's one-time attestations of their bona fides to other entities requiring proof of ID, creating a more seamless, digital mode of access to services. In Singapore, a group of banks joined forces with the Infocomm Media Development Authority of Singapore to build such a system on a blockchain platform.[22]

In addition, advances in cryptography being developed for certain blockchains – such as zero-knowledge proofs discussed in Chapter 2 – may make it possible to verify the authenticity of those identity attributes without ever accessing them directly. This could help address data security and privacy concerns related to blockchain-based identity solutions, even in more open blockchains. Moreover, scalability may be less of an obstacle for identity-related solutions.

21 "Why Lightning Network Will Finally Help Bitcoin Beat Credit Cards, Paypal", *Bitcoinist*, 21 May 2018.
22 "Singapore Regulator, Banks Complete KYC Blockchain Prototype", CCN, 4 October 2017.

Finally, there is no existing shared infrastructure for KYC purposes, making adoption simpler (from an economic perspective). The primary challenges to adoption of more streamlined, shared KYC infrastructure are primarily collective action challenges compounded by legal and regulatory risk, including limitations on sharing of sensitive information.

Broader digital identity applications for blockchains and DLT are discussed in Chapter 5.

Primary securities issuance

Several companies have recently tested blockchain-based systems to issue corporate loans. The advantage of issuing a bond or loan on a blockchain or distributed ledger is that all parties have a shared record of the transaction and any updates. Also, the system can automate functions like the distribution of cash flows in accordance with the parties' legal rights via smart contracts. These processes are currently managed manually, with PDF copies of loan documents and any amendments often distributed by email, and with cash flows tracked and managed in databases (sometimes on spreadsheets) by a central trustee. Enormous resources are spent on reconciling all that siloed information simply to execute a fairly mechanical process – the flow of cash payments in accordance with a pre-determined hierarchy.

In the case of catastrophe-related bonds, for example, management of payment triggers might potentially be automatically executed pursuant to a smart contract, replacing the functions currently played by a custodian or trustee. Of course, that means parties will be required to trust the software – the smart contract – to respond to the external trigger event as much as they currently trust the parties who play the role of custodian or trustee.

Blockchain technology has also been used for new means of raising capital altogether. Traditional crowd-funding and peer-to-peer lending are inherently distributed, and thus may be facilitated by a blockchain or DLT. More novel approaches, such as selling or pre-selling tokens in order to fund the development or maintenance of a distributed network, are discussed below.

Securities clearing and settlement

Today, securities transactions globally are often executed in nanoseconds. But the clearing and settlement of those transactions still takes anywhere from one to three days for stocks – and as long as weeks for certain types of bonds. Though there are many market structure-related and technical reasons for such delays, a shared ledger may enable a shift to near real-time clearing and settlement, eliminating the need for reconciliation of duplicative records. This might significantly reduce the counterparty risk – and associated capital requirements – inherent in those delays.

Along with payments, this was one of the first potential use cases to receive significant attention in the financial services sector. There are several projects at various stages of maturity, and we highlight two representative examples here:

- Last year, the Australian Stock Exchange (ASX) announced that it would replace its entire clearing and settlement infrastructure with a permissioned distributed ledger-based solution developed by Digital Asset Holdings. The announcement followed a two-year period in which ASX consulted with the broad public on the best way to update their core systems (called 'CHESS') for clearing, settlement and post trade services (ASX, 2018).
- Nasdaq is experimenting with blockchain for clearing and settlement on its private securities market, partnering with blockchain start-up Chain to facilitate faster clearing and settlement of normally cumbersome private securities transactions for non-listed companies.

Clearing and settlement solutions are also being explored for other assets, including precious metals like physical gold.

Derivatives clearing and processing

Post-trade processes for most derivatives transactions are significantly more complex than securities transactions, with post-trade life cycles of weeks or up to many years. Many contractual clauses of derivatives transactions (e.g., collateral management, payment on expiration) can be coded directly into smart contracts, enabling automatic execution and enforcement of contractual terms.

IBM is working with the DTCC to provide a blockchain framework for their Trade Information Warehouse, which automates record-keeping, lifecycle events and payment management for more than $11 trillion of cleared and bilateral credit derivatives.[23]

Other efforts focus on creating a distributed clearing network to manage cash flows, collateral management, and other derivatives-related work flows. The International Swaps and Derivatives Association (ISDA) is working with Regnosys to produce a digital version of ISDA's Common Domain Model for the numerous swap transaction and life cycle processes.[24] The goal is to provide the market with a standard set of digital definitions and smart contracts. Automating and distributing these functions can reduce costs and counterparty risk.

Pricing for collateral management may be automated with smart contracts, as proposed in the decentralised solution being developed by SynSwap and Altoros together with the Hyperledger Project.[25] One challenge in this model is that any changes to the pricing algorithm would run up against the complex governance that is inherent in distributed systems, making it difficult to respond to new information not previously contemplated by the pricing algorithm. Other functions facilitated by the central counterparty clearing house (CCP) would also need to be automated, including auctions and other default management processes.

23 "DTCC Milestone: $11 Trillion in Derivatives Gets Closer to the Blockchain", Coindesk, 20 October 2017.
24 "Next steps to CDM", ISDA derivatiViews, 21 February 2018.
25 See https://www.hyperledger.org/wp-content/uploads/2016/10/distributed_clearing_platform_short.pdf

These projects illustrate how incumbent market utilities, by adopting certain features of blockchain technology, may improve the efficiency of existing systems, reducing the likelihood they are disrupted or disintermediated. In this way, interest in blockchain technology has acted as a catalyst for financial market participants to upgrade existing systems.

Post-trade reporting

As distributed ledgers include a full audit trail for each transaction, they may also facilitate more streamlined post-trade regulatory reporting. At the least, by standardising the representation of all necessary data elements, a distributed ledger may facilitate streamlined production of reports by participating financial institutions. There is also the potential for regulators to have their own node on a distributed ledger, such that reporting becomes automatic and comprehensive.

Trade finance

In one of the first trade finance applications of the technology, Barclays teamed up with Irish cheese-maker Ornua to process the guarantees and financing assurance for a transaction selling a shipment of cheese to the Seychelles in September 2016.[26] Developments since then include proofs of concept developed by Standard Chartered in Singapore and by Deloitte and the Hong Kong Monetary Authority in Hong Kong to record shipping documents in a blockchain so as to give lenders greater confidence in the veracity of exporter claims and make letters of credit more available (HKMA, 2017). The two Asian financial centres later agreed to link their blockchain platforms to improve cross-border trade finance solutions.[27] With banks rejecting more than half the trade finance requests from small-and-medium-sized enterprises worldwide, projects like this aim to overcome working capital shortages that hold up production worldwide (WTO, 2016).

A somewhat different approach to the same problem has been developed by electronics giant Foxconn, which taps thousands of sometimes very small suppliers to provide the parts it needs to make everything from Apple iPhones to Hewlett Packard printers. Foxconn, whose venture arm has invested in a number of US-based blockchain start-ups, is encouraging its suppliers to submit data to a blockchain ledger of transactions so as to improve coordination of production schedules and availability of parts. In return, the company is shortening the payment terms or providing internal loans on its own account – in effect, boosting its suppliers' working capital and bypassing the role of banks altogether.[28]

In cooperation with the Inter-American Development Bank, the MIT Digital Currency Initiative is working on a blockchain-based trade finance solution known as b_verify.[29] This project is a new protocol for issuing and transacting in verifiable records using a public blockchain. The first use case is warehouse receipts, designed to improve access to credit and price discovery in commodity emerging markets. The b_verify system is designed to use the Bitcoin blockchain as an anchor of trust.

---

26 "Barclays says conducts first blockchain-based trade-finance deal", Reuters, 7 September 2016.
27 "Hong Kong, Singapore to link up trade finance blockchain platforms", Reuters, 25 October 2017.
28 "Foxconn Reveals Plan for Blockchain Supply Chain Domination", Coindesk, 13 March 2017.
29 See https://dci.mit.edu/b-verify/ (accessed 30 April 2018).

Finance starting at the centralised end of the spectrum

It is far from clear that production-scale blockchain technology applications, at least in finance, will look a lot like the elegant, permissionless blockchain introduced in 2008 by Satoshi.

Virtually all of the 'blockchain' initiatives under development within the financial services sector, outside of cryptocurrencies and decentralised crypto-exchanges, have been based on systems with relatively few nodes appointed by the initiators of the system.

In some cases, there is only one node running the validation network. Some models envisage a consortium of leading banks or other institutions forming the backbone of the ledger-keeping functions. The Corda distributed ledger platform developed by R3CEV is explicitly designed for this kind of federated model, one that departs markedly from the open, permissionless principles of Bitcoin and other public blockchain platforms, in which anyone can join the validation network.

In terms of database structure, discussed above, these are far down the continuum towards being centralised systems.

Permissioned blockchains mitigate some of the governance, privacy and scalability challenges that public blockchains face. There is not nearly as much computational capacity needed to secure the network, since validators are incentivised to do so not by competing with hashing power for cryptocurrency rewards, but simply by their shared interest in achieving that security. And identifying these actors is also important for regulatory purposes.

Because these permissioned ledgers still rely on one or several trusted parties, they still involve many of the attendant 'costs of trust'. But by creating a shared infrastructure – a single ledger that each participant has access to – these solutions can eliminate the need to reconcile multiple ledgers and streamline processes. Moreover, early permissioned ledger efforts are largely focused in areas, such as cross-border payments or post-trade transaction processing, that are inefficient or complex today. There may be some low-hanging fruit, where simple improvements can lead to large efficiency gains.

But critics – many from the cryptocurrency community – argue that these closed systems face a real security risk because the validators can collude to change the ledger. Additionally, the identification of a particular authority, such as a legal consortium in charge of the network, becomes a vector of attack that is open to both hacking risks and to pressure from vested interests and/or governments.

Moreover, permissioned networks risk entrenching market power with the incumbents who run them. Their combined power to approve or disapprove, forged in their capacity to act in unison under the umbrella of a consortium, creates the prospect for future gatekeeping powers. Transparent membership rules open to new entrants could be an important feature to promote competition.

While the software is generally described as open source, consortium members might collaborate to limit the introduction of innovations challenging their business models. The offerings emerging out of the securities industry, such as those proposed by R3CEV and by the DTCC, tend to incorporate existing settlement and reconciliation processes even though the peer-to-peer capacity of blockchain technology could eventually make some of these intermediate functions redundant.

Still, until privacy, security and scalability concerns are adequately addressed and until regulations and business processes go through the kind of overhaul needed for the financial system to adopt a permissionless model, permissioned blockchains seem like the default option for financial sector incumbents. Regulators will need to comprehend the market structure implications of these models and design appropriate rules to protect against financial instability, limit illicit activity, protect investors, encourage competition and promote innovation.

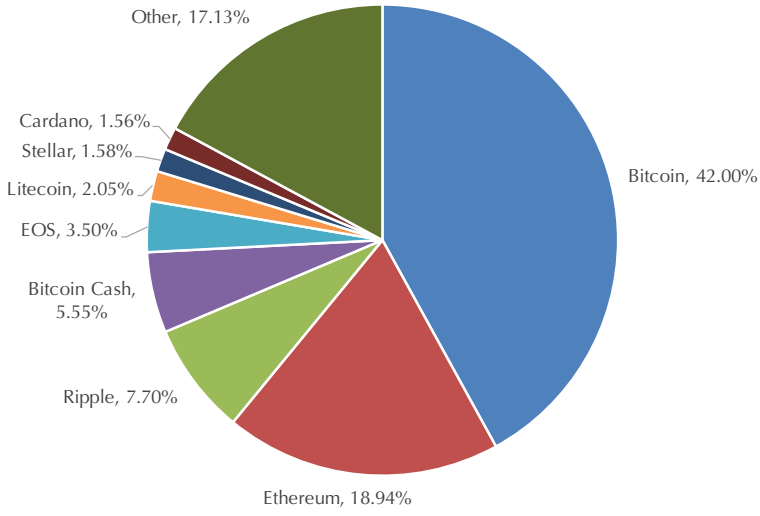
Blockchain technology will still be of value, though, in updating centralized systems and opening them up to more users. The Bank of England's Real Time Gross Settlement System (RTGS) may be headed in that direction. While it is not yet open to permissionless innovation, discussions around the future of RTGS illustrate how blockchain-inspired technologies have broadened the possible users of such centralised systems.

Crypto-finance

Blockchain technology and the crypto ecosystem it has birthed has led to innovative forms of crowdfunding and new models of secondary market trading on crypto-exchanges. One of the latest additions to an ever-evolving global financial system, crypto-finance has so far operated largely outside existing investor protection frameworks.

At the time of writing, the crypto asset market was valued at approximately $300 billion, with nearly 60% of that value in tokens other than bitcoin (Figure 5).[30]

Figure 5 Cryptocurrencies by market capitalisation

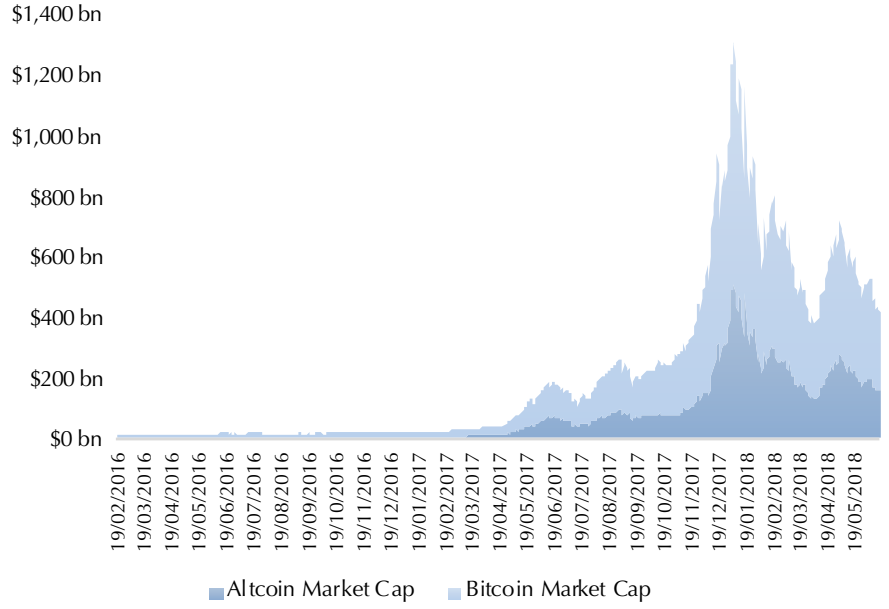


Source: coin.dance

30 As of 14 June 2018; source: https://coin.dance/stats.

The market is volatile but has grown significantly over the years, as shown in Figure 6.

Figure 6 Historical cryptocurrency market capitalisations



Note: "Altcoin" refers to all crytocurrencies other than bitcoin.

Source: https://coin.dance/stats

To date, over 3,000 separate tokens have been issued[31] and 200 crypto-exchanges are operating with tens of millions of customers worldwide.[32]

Token-based economies, as well as burgeoning investor interest in crypto assets, have led to a new means of raising capital for blockchain-based projects: ICOs[33] and similar token sales.

By their very nature and design, these token sales have a mixture of economic attributes that map to both investment and possible consumption behaviour. Token sales are typically marketed online with the release of a whitepaper prior to the launch of a new blockchain-based application.

This new means of crowd-funding generally offers pre-functional digital tokens for possible use on a future blockchain application, or the right to acquire such tokens when the application becomes functional. Thus, purchasers are bearing risk of the eventual success of the development of the new network.

A small number of offerings have involved the sale of tokens for use on already-functioning networks. In these cases, purchasers may be able to use the tokens for consumption immediately.

31 As of 26 May 2018; source: https://icobench.com/stats.

32 As of 26 May 2018; source: https://coinmarketcap.com/exchanges/volume/24-hour/.

33 When using the term initial coin offering, or ICO, in this report, we do not use it to refer to any particular structure of token sale or offering.

Tokens sold through ICOs are generally transferable and fungible or interchangeable with others on the same platform. Development and support of the network, though open-sourced, is largely centralised around the issuing company or foundation and other closely aligned developers. The future supply of a particular application's tokens is determined by the 'monetary policy' applied to the particular token.[34] The company or foundation usually retains a meaningful portion of the tokens, and often also allocates a portion to the promoters or related entrepreneurs in what is called 'pre-mined' tokens. Many of the tokens associated with ICOs are traded either over-the-counter and on crypto-exchanges.

Catalini and Gans (2018) argue that "by revealing key aspects of consumer demand, crypto tokens may increase entrepreneurial returns beyond what can be achieved through traditional equity financing". Their research further suggests that "[c]rypto tokens can also facilitate coordination among stakeholders within digital ecosystems when network effects are present".

Many finance, legal, accounting and consulting firms are now serving this new market.[35] Multiple websites have popped up analysing and reporting on offerings. Venture capital firms have taken to exploring token sales for their portfolio companies as a means to capitalise on the public's interest in crypto assets.

Issuance ballooned in the last 12 months, with nearly $24 billion being raised through the first quarter of 2018.[36] Venezuela purports to have raised $5 billion in an oil-backed ICO called Petro. EOS raised over $4 billion through a year-long ICO ($2.5billion up to 30 March 2018) and Telegram Group raised $1.7 billion in two private offerings.[37]

Elementus reported that, including the Petro purported sale, over $14.2 billion was raised in the first quarter of 2018, far surpassing the full-year 2017 total of $9 billion. There are no authoritative data sources, however, and most aggregators are relying on ICO issuers to self-report the amount they raised. Other sources report the total raised in 2017 at just over $6 billion,[38] and that the tally was $6.3 billion in Q1 2018.[39]

Whatever the true figure, the trends are consistent with issuance volumes continuing to rise. Figures 7 and 8, from CoinDesk, illustrate the growth.

34 While there is no uniform nomenclature within the crypto ecosystem, there is wide use of the term 'monetary policy' for any hard-coded software which limits the future supply of a token. This term, a clear reference to central bank policy, is not to suggest any setting of interest rates within a token economy.

35 "Law firms look to capitalize on initial coin offering boom", *Financial Times*, 26 March 2018.

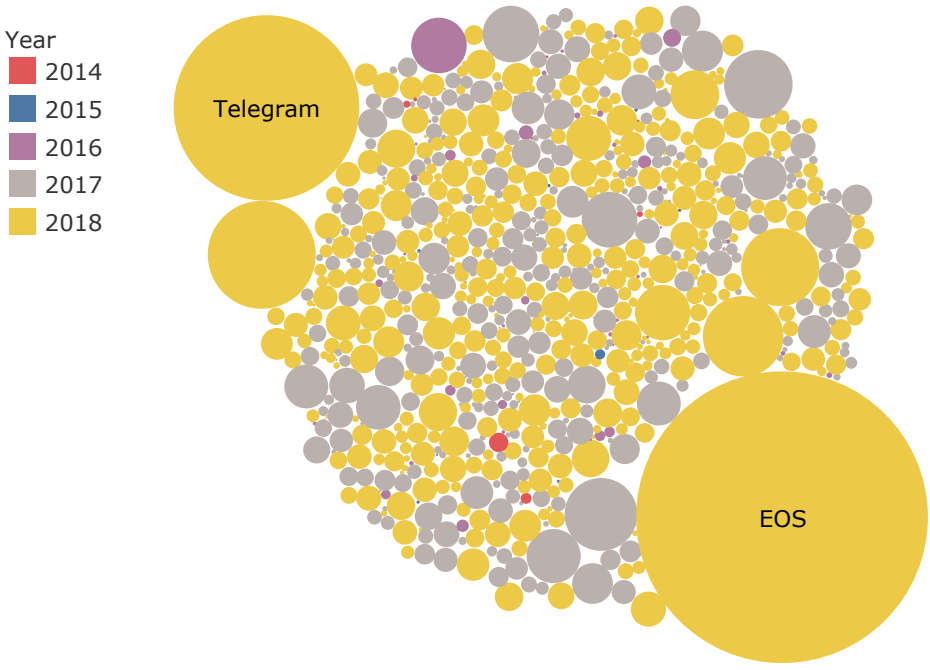
36 See https://elementus.io/tokens-q1-2018

37 "Telegram Raises $1.7 Billion in Coin Offering, May Seek More", Bloomberg Technology, 30 March 2018.

38 "What Bitcoin Rout? Sales of New Digital Tokens Are Still Soaring", *Wall Street Journal*, 22 February 2018.

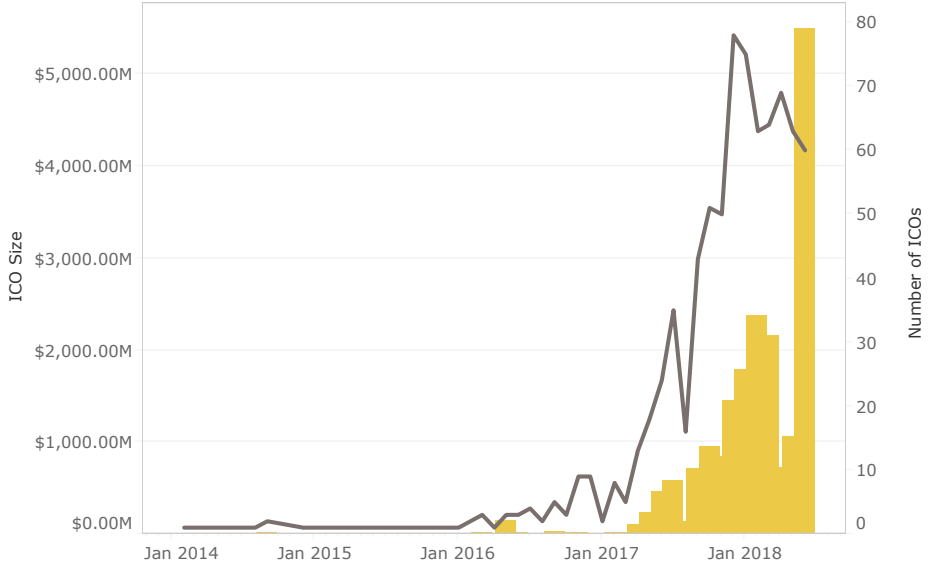
39 "$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total", Coindesk, 19 April 2018.

Figure 7 The token sale explosion, January 2014 to March 2018



Note: Size of circle indicates relative amount raised (in dollars).
Source: https://www.coindesk.com/ico-tracker/

Figure 8 Token sale fundraising volume by month



Source: https://www.coindesk.com/ico-tracker/

Venture capitalists see ICOs as a new and potentially more attractive way to fund start-ups, recognising that they pose a disruption threat to their existing approach to early-stage capital allocation. For many projects there is now a significant potential valuation gap between ICO funding and traditional venture funding – though it is unclear how much of the disparity is due to the public's speculative interest, the potential of token economics or regulatory arbitrage.

It has now become incumbent on entrepreneurs to at least consider how they might tap into these valuation disparities through possibly issuing a token of some sort tied to a blockchain application.[40] In 2017, start-ups exploring blockchain technology raised only $950 million,[41] well below the $6–9 billion raised through ICOs as cited above. As cheap money will always displace expensive money (from the entrepreneur's perspective), and if valuation disparities continue, it is possible that ICO funding will grow further and displace a significant portion of the $160 billion venture capital raised annually around the globe (CB Insights, 2017). This changing venture-funding landscape highlights the need for investor protection to keep pace with these market developments.

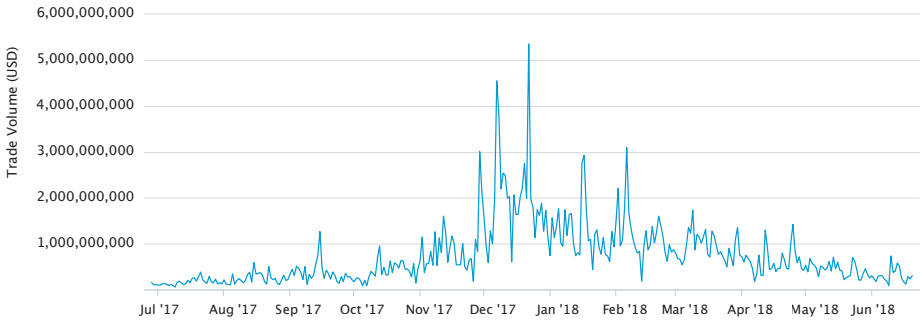
There is a high failure rate for ICOs. One study in February of 2018 found that 59% of a sample of 2017 ICOs had already failed or semi-failed.[42] This, in part, is due to a considerable amount of fraud and scams in this field, with numerous ICOs targeting retail investors, using celebrity endorsers, and promising short-term gains. Estimates vary considerably, with Catalini finding that at least 5% of offerings are clear fraud and up to 25% may be considered scams.[43] In another study conducted by Satis Group, with a smaller sample size of 187 ICOs over $50 million in size, 81% were labelled as scams.[44] The reasons for the wide difference in results are not known but may relate to how definitions of a 'scam' vary.

This proliferation of ICOs has been facilitated by the development of crypto-exchanges, which enable investors in the tokens to trade them for other tokens and, eventually, to cash out into fiat currency. The industry goes back to the launch of Bitcoin Market and Mt. Gox in 2010, less than two years after Satoshi Nakamoto published his initial paper introducing Bitcoin. (Both exchanges subsequently shut down.)

Hundreds of other start-up exchanges have followed. As of 3 July 2018, there were approximately 200 crypto-exchanges that had reported trading volume in the prior 24 hours.[45] Two of these exchanges had daily volumes in excess of $1 billion and 14 more had daily volumes of over $100 million. However, as reported by Blockchain Charts, bitcoin daily trading volume has declined from the highs seen at the beginning of 2018 (Figure 9).[46]

40 "Venture Capital or ICO? Startups Face Cash-Raising Dilemma", Bloomberg, 21 January 2018.
41 "The Rise of the ICO, and What It Could Mean for Venture Capital", *Visual Capitalist*, 3 May 2018.
42 "Nearly Half of 2017 Cryptocurrency 'ICO' Projects Have Already Died", *Fortune*, 25 February 2018.
43 "Initial Coin Offerings: Can Regulators Curb The Risks? How Many ICOs Are Scams?", ValueWalk, 30 March 2018.
44 "ICO Quality: Development & Trading; Sherwin Dowlat & Michael Hodapp of Satis Group", *Medium*, 21 March 2018.
45 See https://coinmarketcap.com/exchanges/volume/24-hour/
46 See https://blockchain.info/charts

Figure 9 Bitcoin exchange trade volume (daily, in US dollars)



Source: blockchain.com/en/charts

In reviewing exchange volume figures, some caution is in order as market data from crypto-exchanges generally is not audited or regulated. Furthermore, exchanges may use wash sales to inflate their volume statistics in an effort to report greater market share. One recent study suggests OKex may be overstating their volume by up to 95% and that Huobi may be doing so by 82%.[47]

These volumes, though, suggest that oversight by capital markets regulators around the globe is worthwhile. In aggregate, these crypto-exchanges have tens of millions of customers. Coinbase alone has over 13 million active accounts opened, more than the brokerage firm Charles Schwab.[48] Possibly due to their operating both as market makers and agents in this largely unregulated market, crypto-exchanges have also become enormously profitable in a short period of time. After just eight months of operation, Binance is reported to have earned $200 million in the first quarter of 2018,[49] more than Deutsche Bank's earnings that quarter. Coincheck earned nearly $500 million in the ten months prior to a hack in January of 2018.[50] While exchanges are located and operated around the globe, many of the largest by volume are originally from Asia.[51]

Beyond providing trade-matching services and order books to buyers and sellers in the same way that traditional securities and derivatives exchanges do, crypto-exchanges also offer a wide range of market-making, advisory and custodial services. Crypto-exchanges also provide direct customer access to their exchange, as opposed to the intermediated access traditionally associated with securities or derivatives exchanges today.

Additionally, a growing number of decentralised cryptocurrency trading platforms are emerging. Though the technology is still developing, these platforms offer matching algorithms for direct peer-to-peer trading, without the exchange or others acting as an intermediary. These decentralised exchanges generally take no custody of funds and provide for peer-to-peer trading based upon open-source algorithms.

47 "Chasing fake volume: a crypto-plague", *Medium*, 10 March 2018.
48 "Bitcoin exchange Coinbase has more users than stock brokerage Schwab", CNBC, 27 November 2017.
49 "Crypto Exchange Binance is More Profitable than Germany's Biggest Bank Deutsche", CCN, 26 April 2018.
50 "Crypto Exchange Coincheck Made $491 Million Profit Prior to Hack", CCN, 28 April 2018.
51 See https://cryptocoincharts.info/markets/info.

Traditional exchange operators are now looking at this world as well. The CME Group and CBOE Global Markets started trading bitcoin futures in December 2017, and NASDAQ is investigating offering cryptocurrency futures and has expressed interest in becoming a cryptocurrency exchange.[52] In 2015, the Intercontinental Exchange (ICE), owner of the New York Stock Exchange, bought a stake in Coinbase, which operates the US exchange GDAX, and announced a cryptocurrency data service in January of 2018.[53] Robinhood, a US-based company with 4 million users of its mobile application for stock and ETF trading, has also announced a new service, Robinhood Crypto, offering trading of a select number of crypto-assets. One million new customers signed up in the first week alone.[54]

Institutional interest is not limited to the US exchange operators. Germany's largest exchange, Deutsche Börse, is considering offering bitcoin futures on its Eurex derivatives exchange,[55] and the Tokyo Financial Exchange is also exploring bitcoin futures.[56] Germany's second largest stock exchange, Börse Stuttgart, announced in April a new cryptocurrency trading app called Bison.[57] The Gibraltar Stock Exchange also has announced the Gibraltar Blockchain Exchange for the sales and trading of ICOs and tokens.[58]

52 "Nasdaq is open to becoming a cryptocurrency exchange, CEO says", CNBC, 25 April 2018; "Nasdaq 'investigating' bitcoin futures that are different from rivals", CNBC, 23 January 2018.
53 "What's Bitcoin Worth? A New Plan to Bring Discipline to Crypto Prices", *Wall Street Journal*, 19 January 2018.
54 "Robinhood rolls out zero-fee crypto trading as it hits 4M users", TechCrunch, 22 Feburary 2018.
55 "German market weighs Bitcoin futures", Handelsblatt Global, 13 December 2017.
56 "Tokyo Financial Exchange Takes First Step Toward Bitcoin Futures", Bloomberg, 5 December 2017.
57 "German Stock Exchange Subsidiary Announces Crypto Trading App Bison", Bitcoin.com, 14 April 2018.
58 "Gibraltar Blockchain Exchange Turns Its Attention to Cryptocurrency", The Merkle, 14 April 2018.

4 Public policy considerations and regulation of crypto-finance

Public policy frameworks

In the 1990s, when the internet was being adopted for use within the financial sector, it too raised novel public policy questions. Healthy debates ensued on the application of existing laws and how they might appropriately be adapted for financial transactions conducted on this new – or new to Wall Street, anyway – medium.

The technology may have been novel, but the core principles of public policy and financial regulation had not significantly changed. Thus, most laws remained the same, and debates arose over how these existing laws and principles applied to the new technologies. In the US for instance, the SEC introduced Regulation ATS in 1998 to address new trading protocols emerging on the internet.

In some instances, though, legislatures and regulators decided not to bring new technologies fully within existing public policy frameworks. One example was with the emergence of the trading of over-the-counter derivatives, in part facilitated by the internet, which allowed for new means of trading swaps electronically. This activity contributed to calls by the financial industry to clarify the legal framework for the trading of these new instruments, generally seeking exemptions for such trading. In Europe, Asia and North America, this lobbying proved quite successful. In particular, swaps, or over-the-counter derivatives, were left largely unregulated around the globe until the calamitous 2008 financial crisis brought a new public policy consensus to bear.

It is important to note that the new financial applications developed during the first phase of the internet – and the regulatory response they prompted – occurred some years after the core, underlying infrastructure had been built out. The foundational protocols, such as TCP/IP, SMTP and HTTP, were developed in the 1980s and first half of the 1990s in universities and corporate labs that were largely out of the mainstream public view. By contrast, the coders working on blockchain technology's core protocols are now doing so with the glare of attention on them and, most importantly, with billions of dollars invested by the public in potential applications.

Still, lessons from the internet remain relevant. It was with clear rules of the road that the financial sector was able to invest in broad adoption of the internet and transform the world of finance.

For blockchain technologies to reach their potential, both in applications as well as for investing, they need to be more fully brought within public policy and legal frameworks. Clear rules of the road today will allow firms – both incumbents and start-ups – to more fully explore investing in crypto assets, token applications or other blockchain technology.

While there are ongoing debates over what specific policies to implement, there is a general consensus amongst global policymakers that we must guard against various societal and systemic threats that blockchain technologies and crypto-finance potentially pose. These threats include the potential for illicit activities such as tax evasion, money laundering, terrorism finance and evading sanctions regimes, areas where this technology presents unique new challenges to national and local authorities. There is also wide agreement that these new markets and technologies must not be allowed to undermine financial stability (Financial Stability Board, 2018), even as central banks and finance ministries tend to differ over how much risk cryptocurrencies, other crypto assets and blockchain applications pose in that realm.

The question of investor protection within the ICO market and crypto-exchanges has stirred some of the liveliest discussions. This starts with the fact that while token sales can be an innovative new way to build a network, token purchasers generally bear investment risk when holding tokens. They stand to profit or fail based on the success of the venture and thus would benefit from basic investor protections such as full and fair disclosure. Similarly, investors trading tokens on exchanges would benefit from investor protections against fraud and manipulation.

As things stand, though, nearly all of these tokens and exchanges currently operate outside of investor protection regimes around the globe. These markets are readily subject to fraud, scams, front-running and other manipulative behaviour.

To protect investors and build broader public confidence, these innovations need to come within public policy frameworks that have helped foster traditional capital markets for decades. The details appropriately may be different for crypto markets, but achieving these policy goals is just as important as for traditional markets.

Developed economies generally learned nearly a century ago that it was not enough to leave it to the markets or to more basic consumer protection laws to protect investors, promote market integrity and ensure for financial stability. The 2008 financial crisis, including the problems caused by the unregulated swaps market, provided a stark reminder of the value of those earlier lessons.

In nearly all countries, there are laws beyond consumer protection laws which protect investors and promote market integrity. These generally include full and fair disclosure to participants in investment schemes, promoting transparency and rules against fraud and manipulation in markets.

Public confidence in markets for cryptocurrencies, ICOs and other tokens ultimately rests on similar rules of the road protecting investors and promoting market integrity. Crypto-exchanges and issuers of tokens would best promote public confidence by coming within the public policy frameworks that have long benefited regulated markets around the globe. As crypto-finance continues to grow, financial stability will also depend upon it.

Global regulatory approach

This burgeoning market and the economic realities of ICOs has led to robust debates around the globe over the appropriate regulations to apply to their issuance and trading. The International Organization of Securities Commissions (IOSCO) board expressed its concerns in a statement stating that: "ICOs are highly speculative investments in which investors are putting their entire invested capital at risk. … the increased targeting of ICOs to retail investors through online distribution channels … raises investor protection concerns. There have also been instances of fraud, and as a result, investors are reminded to be very careful in deciding whether to invest in ICOs." (IOSCO, 2018)

Individual countries' securities regulators have also been active in releasing statements regarding ICOs, cryptocurrencies, and exchanges. IOSCO lists statements from 40 countries regarding ICOs.[59]

The Financial Stability Board (FSB), an international group that makes recommendations about the global financial system, stated in its open letter to the G20 heads of state, that "[g]iven the global nature of these markets, further international coordination is warranted."[60] Due to disparate legal, regulatory and political systems, though, there will be differences in approaches to investor and consumer protections around the globe.

In the US, it is now clear that ICOs, many other tokens and crypto-exchanges must comply with securities, commodities and derivatives laws. Canada has similar such laws. Provincial regulators from Canada joined with state regulators in the US in May 2018, in a coordinated action against ICOs named Operation Cryptosweep with nearly 70 open investigations and 35 enforcement actions.[61]

In many jurisdictions, though, it is not as clear that ICO-issued tokens specifically come within existing securities law definitions, thus possibly leaving investors without the critical protections of securities laws. There has been some debate, for instance, as to whether, depending upon the facts and circumstances, ICO tokens fall with the definition of 'transferable securities' under the EU's Markets in Financial Instruments Directive II (MiFID II). The definition reads "'transferable securities' means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as …"[62] and then includes a non-exhaustive list of examples. Thus, it is possible that ICO-related tokens which trade on a crypto-exchange or otherwise may be considered negotiable on the capital markets.

France's Autorité des Marchés Financiers (AMF) has said that exchanges offering crypto derivatives do fall under MiFID II requirements.[63] More broadly, the European Securities and Markets Authority (ESMA) has put out a consultation relating to contracts for differences including rolling spot forex and binary options sold to retail customers. This may affect regulatory policy with regard to cryptocurrency derivative trading throughout Europe.[64]

59 See https://www.iosco.org/publications/?subsection=ico-statements
60 "Chair sets out FSB priorities for the Argentine G20 Presidency", Financial Stability Board, 18 March 2018.
61 "State and Provincial Regulators in U.S. and Canada Target Initial Coin Offerings", *Wall Street Journal,* 21 May 2018.
62 See https://www.pwc.lu/en/mifid/docs/pwc-markets-in-financial-instruments-directive-2-mifid-2-level-1.pdf
63 "French Watchdog Clamps Down on Crypto Trading", Bloomberg, 22 February 2018.
64 "ESMA Seeks Public Input on Cryptocurrency Derivatives Policy", Coindesk, 18 January 2018.

Earlier this year, Switzerland's Financial Market Supervisory Authority (FINMA) issued guidelines for ICO organizers. The guidelines clarified that FINMA would treat each application on its own merits, and "focus on the economic function and purpose of the tokens."[65] The guidelines established a three-category framework for assessing the applicable regulatory regime:

- "Payment tokens", which FINMA views as "synonymous with cryptocurrencies". While payment tokens are generally not used to fund a development project, they "may in some cases only develop the necessary functionality and become accepted as a means of payment over a period of time". These tokens would be subject to AML laws generally applicable to payments intermediaries.
- "Utility tokens" are tokens which are intended to provide digital access to an application or service and are not subject to securities laws – as long as they *solely* provide access to an *already*-functioning network.
- "Asset tokens" are tokens that have economic properties analogous to equities, bonds or derivatives. If a token functions solely or partially as an investment, it will be subject to prospectus requirements and trading protections.

To date, Japan and a number of other jurisdictions have required registration of crypto-exchanges consistent with money-transmission licensing and with additional provisions for custodial duties. To better protect the investing public, though, crypto-exchanges will need to be regulated more akin to traditional exchanges.

Legal frameworks, largely written prior to the emergence of crypto-finance, may need to be updated to clarify that ICO tokens and crypto-exchanges need to comply with basic investor protection frameworks. To do so may require legislative action in certain jurisdictions, as some statutory definitions of securities may not clearly include ICOs or other similar investment risk-bearing tokens as they may lack the traditional characteristics of stocks or bonds as defined in statute.

Otherwise, though, a growing and potentially significant portion of the capital markets will not benefit from basic investor protections. We have already seen high levels of fraud in these marketplaces. Over time, the results of not bringing crypto-finance within public policy frameworks for investor protection would almost certainly be to lower levels of public confidence and trust in these markets, as well as to increase economic inefficiencies in financial markets.

This is a moment of decision for public officials and leading market participants. Clear rules of the road protecting investors will allow firms – both incumbents and start-ups – as well as the broad public to more fully explore investing in crypto tokens and related crypto-exchanges. Hopefully such clarity will promote a more level playing field amongst start-ups as well as incumbents, at least with regard to regulatory uncertainties, though overly strict regulation can favour incumbents. Currently, firms are investing based upon a varied range of regulatory assumptions.

The social good of investor protection is relevant when a purchaser of an instrument or digital asset bears risk related to a business endeavour.

65 See https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

Tokens and initial coin offerings

ICO investors bear risk related to the success of a network. The tokens sold in an ICO are different from tokens for a neighbourhood laundromat or tickets to the theatre. The company, related foundation and founders usually retain a meaningful portion of pre-mined tokens and are motivated to enhance the value of the tokens.

The token's economic risks, monetary policies, manner of marketing, and the reality that its seller is raising money to fund development are all attributes of investment schemes. In the US there happens to be a legal definition of security which includes "investment contract" directly in statute. Later, in 1946, the US Supreme Court gave further guidelines on this matter with a decision (discussed below) that became known as the 'Howey test'. It would appear that many ICOs meet this definition. As other countries' legal regimes may not cover investment risk-bearing tokens within their investor protection laws, we believe it is worthwhile for them to consider doing so to incorporate a similar treatment of ICOs.

Though typically lacking certain traditional features of stocks or bonds, and often described as a consumable token rather than an investment, it is clear the investing public is hoping for possible appreciation of a transferable token based, at least initially, upon the efforts of a development team, a company or its promoters. Though, to be sure, this expected appreciation might also include an anticipation of network effects derived from the 'community' of token holders and open source developers drawn to the project, and validators incentivised by the scheme.

Giving someone funds with the expectation of profit based upon the efforts of others are the core attributes of the economics of most investment schemes. That is why it is a longstanding criterion for determining when a purchase is an investment contract, and thus a security under US securities laws. To protect investors bearing risk, the securities laws require that investors be provided with full and fair disclosure on which to make an informed decision.

ICO tokens are structured with many attributes to promote marketability and potential appreciation. They usually include a so-called monetary policy which is encoded in the software, limits the future supply of tokens and introduces an element of scarcity. They are fungible, meaning that they are identical and can be mutually replaced by other similar tokens. This fungible or interchangeable quality enhances liquidity. They are often listed on crypto-exchanges, boosting marketability and transferability.

The presence of a transferable or usable token and an expectation of profit further distinguishes this new form of crowdfunding from earlier donation-based crowdfunding carried out on platforms such as Kickstarter or GoFundMe (Vargas et al., 2015). The fungible nature of tokens and an expectation of profit further distinguishes them from concert tickets or personal seat licenses.

The duck test

American poet James Whitcomb Riley wrote over one hundred years ago: "When I see a bird that walks like a duck and swims like a duck and quacks like a duck, I call that bird a duck."[66]

66 See https://www.goodreads.com/quotes/6770726-when-i-see-a-bird-that-walks-like-a-duck

We think this 'duck test' can apply to the broad definition of an investment. With that and the economic realities in mind, it is clear the public benefits from accurate and complete disclosure of all material information related to an *investment*, whether that investment is in new forms of finance, such as ICOs, or investing in traditional forms, such as stocks or bonds. This is the very purpose of securities laws.

Crypto-exchanges

With increased regulatory oversight, and occasional crackdowns, in China, Hong Kong, Korea and Japan, a number of exchanges have announced or are considering relocating to jurisdictions considered friendlier to cryptocurrencies, like Singapore and Switzerland.[67] (Zug, Switzerland, is also where the Ethereum Foundation is based.) Binance[68] and OKEx[69] recently announced intentions to move to Malta, whose prime minister tweeted: "We aim to be the global trailblazers in the regulation of blockchain-based businesses."[70] Financial firms doing international regulatory forum shopping isn't new, particularly to countries with small capital markets. However, this should not allow those exchanges to access investors in countries with deep capital who seek to protect investors. Operating with US persons, for instance, these offshore exchanges would need to comply with US law.

The fact is that many crypto-exchanges have failed. By 2015, one list already had at least 36 failures.[71] In 2018, after the Japanese Financial Services Agency (JFSA) conducted business reviews of exchanges, at least nine suspended their operations.[72]

Concerns about crypto-exchanges

Since their inception, there have been significant concerns expressed about crypto-exchanges. These concerns range across the public policy sphere, from their effect on financial stability and illicit activity to limited customer and investor protections.

Illicit activity

Some jurisdictions have moved forward with regulating exchanges, most notably with regard to guarding against illicit activity. This has generally been done through money transmission laws or bank secrecy laws regarding anti-money laundering (AML), combatting the financing of terrorism (CFT) and KYC regimes. The US Treasury's Financial Crime Enforcement Network (FinCEN) has put out guidance

67 "World's Fifth Largest Crypto Exchange Bitfinex Wants To Move To Switzerland", *Cointelegraph*, 28 March 2018.
68 "World's Biggest Cryptocurrency Exchange Is Heading to Malta", Bloomberg, 23 March 2018.
69 "World's Second Largest Crypto Exchange OKEx Moves To 'Blockchain Island' Of Malta", *CoinTelegraph*, 12 April 2018.
70 See https://twitter.com/josephmuscat_jm/status/977115588614086656?lang=en
71 "36 bitcoin exchanges that are no longer with us", *Brave New Coin*, 23 October 2015.
72 "Nine Japanese Crypto Exchanges Have Suspended Operations So Far", Bitcoin.com, 13 April 2018.

on this regard starting in 2013 and most recently in a letter to Congress.[73] In the US, several states, including New York State through its BitLicense,[74] have acted to bring exchanges within money transmission laws. Japan moved in 2017 to regulate crypto-exchanges primarily for money transmission and their custodial duties. By February of 2018, Japan's Financial Services Authority had inspected 32 exchanges operating in the country.[75] It was subsequently reported that over 100 other exchanges had inquired about registration.[76] Korean authorities banned exchanges from trading for anonymous accounts[77] and subsequently began investigating numerous exchanges for fraud and other misconduct. Bithumb and Coinone were raided by the tax office[78] and UPBit, Korea's largest exchange, was raided over suspected fraud in May of 2018.[79]

As most jurisdictions around the globe do not yet have specific regulatory regimes governing cryptocurrencies, ICOs or related tokens, exchanges are a critical gateway to protect against illicit money transmissions.

Furthermore, absent intermediated access, tax authorities and financial crimes enforcement around the globe must rely solely on investors, exchanges or blockchain forensics companies for reporting on crypto gains or losses. In traditional exchanges, authorities generally have been able to rely upon intermediaries to report on tax events or KYC as they act as gatekeepers for market access.

Custodial duties

In some countries, particularly Japan, authorities have also required crypto-exchanges to register and meet certain custodial duties to protect customer funds, which are usually stored in an exchange's digital wallet. In the US to date, the only regulatory safeguards have been through state-administered money transmission regulations. This approach – regulating exchanges' custodial duties in the same manner that Western Union and MoneyGram are regulated – has not been satisfactory. Exchanges should fully segregate customer funds and ensure that they not lose those funds and not use those funds.

Exchanges are exploring whether new approaches, such as multi-signature wallets, might aid in protecting the security of customer funds.[80] Japan has also begun laying a groundwork to require exchanges to meet statutory capital requirements to protect investors and limit systemic risk.[81]

Customer funds, however, have not always been secure. Many exchanges have been hacked, losing a significant amount of customer funds. Mt. Gox lost $473 million in bitcoin in 2014.[82] Coincheck lost $530 million in NEM (XEM) tokens in 2018. A South Korean exchange, Coinrail, was hacked in June of 2018,

73 "Letter to Senator Ron Wyden", FinCEN, 13 February 2018.
74 See https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm
75 "Japanese Financial Authority Inspecting 32 Cryptocurrency Exchanges", Bitcoin.com, 3 February 2018.
76 "Over 100 Firms Seek Licenses to Operate Cryptocurrency Exchanges in Japan", Bitcoin.com, 1 March.
77 "S Korea bans anonymous cryptocurrency trades", BBC News, 23 January 2018.
78 "South Korea Reportedly Expands Crackdown on Crypto Exchanges", Coindesk, 11 January 2018.
79 "Korea's Biggest Crypto Exchange Raided Over Suspected Fraud", Coindesk, 11 May 2018.)
80 "The sad state of crypto custody", TechCrunch, 1 February 2018.
81 See https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#Japan
82 "12 Biggest Cryptocurrency Hacks In History", Benzinga, 24 November 2017.

losing $40 million, or fully 30% of customer tokens held in custody.[83] Some Mt. Gox coins were recovered, but creditors have not received any compensation. Coincheck had the financial resources to compensate affected holders but none of the actual stolen NEM were recovered.[84]

Investor protection and market integrity

Though a number of jurisdictions are regulating crypto-exchanges as money transmitters, few have yet brought these exchanges within their investor protection and market integrity standards required of traditional regulated exchanges. This is despite the duck test or the clear economics of most of these exchanges facilitating trading in securities, investment-driven contracts, derivatives or retail-leveraged transactions.

This is of additional concern, as crypto-exchanges often act as counterparties to their customers and have limited guardrails against front-running, fraud, or other manipulative practices.

Indeed, these concerns were front and centre in the US SEC's recent statement on online trading platforms for digital assets.[85] The SEC stated that "... many of these platforms give the impression that they perform exchange-like functions by offering order books with updated bid and ask pricing and data about executions on the system, but there is no reason to believe that such information has the same integrity as that provided by national securities exchanges".

In a recent paper, Gandal et al. (2017) review how a trader using two trading bots on the Mt. Gox exchange may have manipulated the price of bitcoin up 8-fold in 2013. The US Futures Industry Association, in a letter to the US Commodity Futures Trading Commission (CFTC), expressed its apprehension about the reference markets for bitcoin futures: "We remain apprehensive with the lack of transparency and regulation of the underlying reference products on which these futures contracts are based and whether exchanges have the proper oversight to ensure the reference products are not susceptible to manipulation, fraud, and operational risk."[86] In January of 2018, there were reports of an investigation into whether bitcoin might have been manipulated on the Bitfinex exchange in a scheme using the token Tether.[87]

83 "South Korean Exchange Coinrail Hacked, $40 Million in Crypto Reported Stolen", *Bitcoin Magazine*, 11 June 2018.

84 "Coincheck: NEM Foundation Stops Tracing Stolen Coins, Hackers' Account At Zero", *CoinTelegraph*, 23 March 2018.

85 "Statement on Potentially Unlawful Online Platforms for Trading Digital Assets: Divisions of Enforcement and Trading and Markets", 7 March 2018.

86 "Open letter to CFTC chairman Giancarlo regarding the listing of cryptocurrency derivatives", Futures Industry Association, 7 December 2017.

87 "Worries Grow That the Price of Bitcoin Is Being Propped Up", *New York Times*, 31 January 2018.

The US path forward

US securities laws – the Howey test

The core principles of investor protection embodied in US securities laws are meant to apply broadly, regardless of the form of investment. The statutory definition of 'security' covers multiple forms of finance well beyond just stocks or bonds, including the term 'investment contract.'[88]

An important early test of this statutory definition related to the Florida orange groves of William Howey. His company sold land and gave the buyers an option to lease the land to an affiliated service company and participate in the profits of the crop. Although not stocks or bonds, the US Supreme Court in 1946 ruled that Howey's land sale agreements satisfied the definition of 'investment contracts' under the 1933 Securities Act and thus should be regulated as securities.

The 'Howey test' from this case states that "an investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party".[89]

The Court further said that: "This definition embodies a flexible, rather than a static, principle that is capable of adaptation to meet the countless and variable schemes devised by those seeking to use others' money on the promise of profits."[90]

In 2004, the Supreme Court similarly ruled in *SEC v Edwards*, adding: "The profits this Court was speaking of in *Howey* are profits – in the sense of the income or return – that investors seek on their investment, not the profits of the scheme in which they invest, and may include, for example, dividends, other periodic payments, or the increased value of the investment."[91]

The SEC has now repeatedly spoken out about the application of securities laws to ICOs and related token sales in many advisory statements and reports, in addition to pursuing a growing number of enforcement actions. Beginning with the 'DAO Report', the SEC clarified that securities laws would apply to offerings like The DAO, regardless of the label applied to the coin or token.[92]

The report put market participants on notice that the SEC was going to review token offerings for compliance with securities laws, and that the Howey test for investment contracts would be the relevant test for whether an offering constituted a security.

Despite its clear intentions, the DAO Report barely slowed down the pace of token issuance. Indeed, after a slight dip in August of 2017, monthly token sales have only continued to increase.

88 Securities Act of 1933, Section 2(a)(1).
89 *SEC* v. *W. J. Howey Co.*, 328 U. S. 293, 299 (1946).
90 *SEC* v. *W. J. Howey Co.*, 328 U. S. 293, 299 (1946).
91 *SEC v. Edwards*, 540 U.S. 389 (2004).
92 *Report of Investigation Pursuant to Section 21(a) Of The Securities Exchange Act of 1934: The DAO* (Exchange Act Rel. No. 81207); SEC (25 July 2017).

In response, the SEC amplified its public pronouncements and began to bring enforcement cases, including the 'Munchee Order'.[93] Sounding very much like the poet Riley, SEC Chairman Clayton stated at a Congressional hearing in February of 2018, "I believe every ICO I've seen is a security… You can call it a coin but if it functions as a security, it is a security."[94]

To date, the enforcement actions taken by the SEC have focused on cases of blatant fraud – promising Visa and Mastercard crypto products when no relationship with Mastercard or Visa existed, for example, or identifying non-existent team members.

General considerations

Overall, the question is how do the markets, this new technology, and regulators go forward? We will first discuss four general areas of questions for consideration: 1) remediation, 2) recovering losses, 3) possible tailoring of rules, and 4) available regulatory tools.

We will then discuss additional considerations regarding ICOs: 1) the need for review of all tokens, including the 1,000-plus potentially non-compliant ICOs as well as all large-cap tokens; 2) possible token design moving forward; and 3) the issues of Simple Agreements for Future Tokens (SAFTs) and other multi-stage token sales and circumstances whereby a token deemed to be a security may evolve into a non-security.

Lastly, we will discuss additional considerations regarding crypto-exchanges: 1) custodial duties, 2) market integrity, 3) decentralised exchanges, 4) financial stability and illicit activity, and 5) types of registration.

Remediation

Regulators will need to sort through how to bring over 1,000 past ICOs and nearly 200 crypto-exchanges – nearly all of which appear to be currently non-compliant – into compliance with US securities laws.

One petitioner has suggested retroactive registration for ICOs that have not defrauded their investors coupled with rescission rights to all purchasers.[95] The SEC, as part of a solution for remediation, could choose to be more lenient on tokens issued a longer time ago, though not technically beyond a legal statute of limitations. For instance, when the SEC issued the DAO Report it did not bring charges or make findings in violation of that report, and in the Munchee Order the SEC specifically noted the fact that the offering had taken place following the issuance of the DAO Report.[96] Since that report and other SEC statements,

93 Order Instituting Cease-and-desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, making Findings, and Imposing a Cease-and-desist Order (Release No. 10445), 11 December 2017. See also SEC vs. Sohrab Sharma and Robert Farkas, 2 April 2018 (hereinafter the "Centra Complaint").

94 "Senate cryptocurrency hearing strikes a cautiously optimistic tone", TechCrunch, 1 February 2018.

95 See https://www.sec.gov/rules/petitions/2018/petn4-719.pdf

96 "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities", SEC, 25 July 2018.. See also "In the Matter of Munchee, Inc.", SEC Release No. 18304, 11 December 11 2017.

though, issuers have been on notice to comply with the law. Many, though not all, ICOs in 2018 Q2 have filed with the SEC as exempt securities offerings. Selling unregistered securities now, though, would be a current violation, regardless of when a token initially started.

The SEC will need to address and possibly adapt requirements for registered or exempt securities offerings, some that may not be readily adaptable to these past ICOs, which were offered without adequate disclosures, appropriate solicitations or full records of beneficial ownership. Currently there are no ready technological solutions to satisfy requirements for issuers (or their transfer agent) to record the beneficial ownership of each token holder, though solutions may be developed in the future.

Regulators will need to decide whether crypto-exchanges which were operating outside of investor protection norms, and might have profited from front-running or manipulating markets, might not be allowed to register.

If large market cap tokens, such as XRP or EOS, are concluded to be non-compliant securities, exchanges offering trading in these tokens will need to adjust their operations and listings.

Where appropriate, regulators will need to decide how long to give crypto-exchanges that have offered trading of ICO tokens or other securities, crypto-derivatives or related leveraged crypto-assets to come into full compliance with securities or derivatives laws. In some circumstances, staging the timing of regulatory requirements for exchanges may be appropriate. Regulators also will need to determine when fines should be assessed for particularly bad past behaviour.

Recovering losses

Investors will ask regulators and the courts for help in recovering losses on unregistered non-compliant ICOs that may have in good faith already failed or were outright frauds. US securities laws provide rescission rights, but in many circumstances the funds might be gone. It may be difficult to recover losses due to fraud, manipulation or custodial errors on crypto-exchanges. The SEC and the investing public each have rights to bring actions seeking remedies for losses as the securities laws provide for various private rights of action (Walter, 2011). The CFTC and international regulators may have a role to play as well.

Compliance and possible tailoring of crypto regulations

ICOs, other crypto-tokens and crypto-exchanges going forward will need to come into compliance with existing laws. Given that existing laws were written prior to the emergence of blockchain technology, it may be appropriate to tailor laws taking into account the novel circumstances of this new technology, while still protecting consumer and investor interests.

Regulatory tools

Regulators will have numerous tools in their toolkit to bring greater clarity in a timely fashion to the application of existing legal requirements. The SEC has initially used public advisory statements, speeches, testimony and enforcement actions to inform the public and bring the market into compliance. Market participants also have petitioned for no-action letters and broad-based remediation plans.

With the emergence of the internet in the 1990s, the SEC issued new rules and interpretations, with notice and comment, though this took a considerable amount of time. A similar approach could apply here. The CFTC recently issued a Proposed Interpretation regarding the exception for 'actual delivery' that might apply for virtual currency.[97] New rules may be appropriate if tailored crypto regulations are determined to be appropriate.

Additional considerations – ICOs

Beyond these general matters for both ICOs and crypto-exchanges, there are a number of specific areas for consideration related to ICOs and other tokens.

Current crypto assets up for review, including all large cap tokens

With over 3,000 past ICOs and other tokens, a review to determine the legal status of all the current crypto-assets is appropriate, including a review of all large-cap tokens to bring regulatory clarity to these markets.

SEC chair Clayton spoke on these matters at a Congressional hearing on 26 April 2018. He divided crypto-assets into two areas: those which represent "a pure medium of exchange" and "tokens, which are used to finance projects." His full statement was:

> "It's a complicated area. Because, as you said, there are different types of crypto-assets. Let me try and divide them into two areas. A pure medium of exchange, the one that's most often cited, is Bitcoin. As a replacement for currency, that has been determined by most people to not be a security."

"Then there are tokens, which are used to finance projects. I've been on the record saying there are very few, there's none that I've seen, tokens that aren't securities," Clayton added. "To the extent something is a security, we should regulate it as a security, and our securities regulations are disclosure-based, and people should follow those and provide the information that we require."[98]

While many market participants have considered these statements with regard to tokens issued as ICOs, it will be important to review the legal status of all crypto assets, including all of the large market cap tokens, regardless of labels.

For illustrative purposes, we consider the top six tokens by market value and find that there are strong arguments that one or both of XRP and EOS are securities.

97 "Retail Commodity Transactions Involving Virtual Currency", *Federal Register* 82(243): 60335.
98 "Bitcoin is Not a Security SEC Chairman", BlockExplorer News, 27 April 2018.

Bitcoin is generally not considered to be a security by global regulators or to trigger the Howey test in the US. Bitcoin came into existence as mining began as an incentive mechanism in regulating the distributed platform at the point when the blockchain became functional. Importantly, there were no pre-mined coins sold to passive investors or retained for promoters or related entrepreneurs. The SEC chairman has said that it will not be considered a security. Others, such as the Israel Securities Authority, have said the same.[99]

For the same reasons, Litecoin and Bitcoin Cash, both forks off from Bitcoin in 2011 and 2017, respectively, also do not appear to trigger the US Howey test.

The SEC's director of the Division of Corporate Finance, William Hinman, spoke to the matter of Ether (ETH) through a speech on 14 June 2018.[100] Hinman said: "*[P]utting aside the fundraising that accompanied the creation of Ether*, based on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions" (emphasis added).

The sale of ETH took place during the summer of 2014, funding the Ethereum Foundation's development, legal and other costs, a year prior to its first live release of the Ethereum blockchain in July of 2015.[101] ETH was purchased with an investment of bitcoin in a common enterprise, the Ethereum Foundation. Purchasers had a reasonable expectation of profit based upon appreciation of ETH, which early on was heavily dependent on the efforts of the Ethereum Foundation. The Foundation also played a central role in the hard fork related to the attack on The DAO smart contract in 2016, as discussed earlier in this report.

However, the SEC's Hinman also noted that "a digital asset transaction may no longer represent a security offering [where] the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts". Hinman explained that decentralisation may reduce information asymmetries, which are part of the concerns underlying the Howey test and the US securities laws more broadly: "[W]hen the efforts of the third party are no longer a key factor for determining the enterprise's success, material information asymmetries recede." In other words, as a network becomes decentralised, there may no longer be a group of insiders whose efforts are relevant to the network's economic success or with superior information that is unavailable to holders of the tokens or coins. Moreover, "[a]s a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful".[102]

Thus, regardless of whether the ETH sale in 2014 may have passed the Howey test, the SEC has said that it is now sufficiently decentralised not to be considered an investment contract.

This leaves XRP and EOS, which might each have been investment contracts, or non-compliant securities offerings, when sold.

The token associated with the Ripple distributed ledger, XRP, was launched in January of 2013 with Ripple Labs initially holding 80% of the total tokens. Ripple, the company, has subsequently sold, distributed or used XRP in operations, so that it now owns approximately 60% of the tokens.

99 "Israel Officially Declares Bitcoin Is Not a Security", Bitcoin.com, 26 March 2018.
100 "Digital Asset Transactions: When Howey Met Gary (Plastic)", SEC, 14 June 2018.
101 "Launching the Ether Sale", Vitalik Buterin, 22 July 2014.
102 "Digital Asset Transactions: When Howey Met Gary (Plastic)", SEC, 14 June 2018.

Purchasers who bought XRP over this time have invested money or given valuable services to a common enterprise, Ripple Labs or its successor, Ripple, the company. These purchasers have had a reasonable expectation of profit based upon the efforts of the promoter, Ripple, the company. For instance, when announcing an escrow arrangement for Ripple's XRP holdings, Ripple's CEO said, "To build XRP liquidity, we have been mindful over the years about how we distribute XRP. ... We engage in distribution strategies that we expect will result in a strengthening XRP exchange rate against other currencies."[103] Additionally, the home page of Ripple maintains metrics on the market performance of XRP and a link to buy XRP on 16 different exchanges.[104] Ripple, the company, continues to lead the development of the platform, partnering with firms to use the network,[105] possibly influencing significant control over which nodes can validate transactions,[106] and releasing new white papers for the payment network, all of which contributes to the value of XRP.[107]

On the other hand, one might argue that XRP has been usable in some fashion on the Ripple network since 2013 and that XRP and the Ripple network might still exist even if Ripple, the company, disappeared. And the economic function of XRP, in Ripple's pilot, xRapid, introduced in May of 2018, is principally to provide liquidity as a bridge currency between two fiat currencies when transferring funds internationally.[108]

A Cayman Islands company, Block.one, has raised well over $4 billion through an ICO, ended 1 June 2018, of the token, EOS.[109] Transparent public auctions were conducted for a year on a nearly daily basis whereby EOS tokens were purchased for ETH from a common enterprise, Block.one. Purchasers had a reasonable expectation of profit based upon the marketing, coordination and early platform engineering efforts of the promoter, Block.one, which also retained unique inside information on the development process. Block.one left much of the EOS.IO software's development to an external, open source community of token-holding coders, reserving 10% of all tokens for their ownership,[110] but has announced a $1 billion venture capital initiative, EOS VC, to foster the EOS ecosystem investing in businesses using the EOS.IO software.[111] Block.one also excluded US citizens, residents or entities from purchasing EOS tokens.[112]

Whether XRP, EOS and others are non-compliant securities under US law will be determined by the SEC and US courts. Regardless, though, purchasers of these tokens have borne investment risk in anticipation of appreciation based upon the entrepreneurial efforts of others – precisely the types of economic risks that underlie global investor protection frameworks.

---

103 "Ripple to Place 55 Billion XRP in Escrow to Ensure Certainty of Total XRP Supply", ripple.com, 16 May 2017.
104 See https://ripple.com/xrp/buy-xrp/.
105 "Ripple (XRP) 2018: 5 Major Partnerships and Announcements", *CryptoRecorder*, 1 March 2018.
106 "The Ripple Story", Bitmex Research, 6 February 2018.
107 "Ripple Papers Pledge New Start for $40 Billion XRP", Coindesk, 21 February 2018.
108 "Ripple: XRP Pilot Cuts Payment Fees up to 70%", Coindesk, 10 May 2018; see also "How XRP Fits Into Ripple's Payment Products Explained", Coindesk, 4 March 2018.
109 See https://eosscan.io
110 See https://eos.io/faq
111 "EOS Mainnet Countdown: $1 Billion VC Giveaway, Collaboration with Virginia Tech", *The Daily HODL*, 22 May 2018.
112 See https://eos.io/faq

The SEC has determined that a digital token having some consumable utility does not preclude it from being an investment contract and subject to US securities laws. It is not an either-or proposition.

Token design for non-securities

Second, going forward, regulators will address how tokens intended to power distributed networks might be structured in a manner such that they are not investment contracts. In essence, in the US how might tokens be designed such that their sale will be essentially for consumption and devoid of investment characteristics as embodied in the Howey test? If the token is sold as an interest in some profit-making venture (whether debt or equity), or in anticipation of profits based upon the venture, it is a security. If the token is itself solely intended to have intrinsic value or productive use, then it is a commodity (like oil). That said, tokens currently generally have characteristics of both, bearing some of the characteristics of securities (such as buyers hoping for tokens to appreciate in value) and some characteristics of commodities. (Perhaps resembling platypuses, to extend our zoological metaphors.)

Lessons might be drawn from the sale of theatre tickets, apartment coops[113] and personal seat licenses for sports arenas.[114] While these non-fungible assets all have important distinctions from most current ICOs, none are currently treated as investment contracts or securities under US law.

In addition, as discussed more generally above, it might be appropriate to modify existing laws that were written prior to the emergence of utility tokens, while still protecting investor interests.

Tokens that incentivise participation in a decentralised network may, however, raise similar investor protection issues as purchasers bear risk related to the issuer's development of the network. For instance, if the token is pre-functional, holders bear the risk that the issuer may fail to complete development of the network. If tokens are functional on a network, holders may still bear the risk of user adoption and further network upgrades, and may be at an informational disadvantage if the efforts of the promoter or other group are still central to the network. Further, it is worthwhile considering what characteristics might bring a token's market value into equilibrium with the value of the services or goods available on the network rather than being reliant upon possible appreciation of the token itself.

The SEC's director of the Division of Corporate Finance, William Hinman, noted during Congressional testimony that "it is certainly possible that there are tokens that would not have the hallmarks of a security". He described such an instrument as "a token where the holder is buying it for its utility rather than investment, especially if it's a decentralized network in which it's used with no central actors". Hinman expanded upon this in his 14 June 2018 speech referenced above, further discussing the relevance of decentralisation. The lack of reliance on the efforts of a promoter or central group may reduce the information asymmetries the securities laws are designed to address.

113 See, e.g., *United Housing Foundation, Inc. v. Forman* 421 U.S. 837 (1975)

114 See, e.g., San Francisco Baseball Assocs. L.P. (available 24 February 2006), granting a request for no-action under Securities Act Section 2(a)(1) where a professional baseball team proposed operation of a service that would facilitate the resale of personal seat licenses.

Achieving this non-security status will take more than semantics or even the ability to currently use a token. And it will take more than a token being functional on a network. As the SEC stated in the Munchee Order: "Even if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labelling – such as characterising an ICO as involving a "utility token" – but instead requires an assessment of "the economic realities underlying a transaction ."[115]

Security token transformation, SAFTs and multi-stage offerings

How should the law treat tokens over time as they evolve? Chairman Clayton and the SEC staff have now indicated that once a security, not necessarily always a security. This view appears consistent with the recommendations of a group of venture capital firms and law firms, who suggested that an ICO or token that was initially deemed a security might, under certain 'safe harbour' circumstances, transform into a non-security.[116] They advocate for such a transformation to an unregulated token when there is 'full functionality' of the token and 'full decentralisation' of the network, along with other characteristics. This approach, if fully adopted by the SEC, may allow a number of tokens to become unregulated over time even if they are initially sold in transactions that meet the Howey test and therefore must be registered.

Some entrepreneurs have already utilised a multi-stage approach to conducting ICOs, registering or complying with exemptions[117] for the first stage of their offering while proposing (or hoping) that the later stage – when the token is capable of use (and the network truly decentralized) – will not require registration. While a variety of legal forms have been used, one recent approach has been that of a SAFT, which is modelled on the Simple Agreement for Future Equity, a replacement for convertible notes employed in certain venture capital investments (Batiz-Benet et al., 2017). In September of 2017, Filecoin raised $257 million, then the largest token sale to date, through a SAFT.[118] Telegram's recent $1.7 billion offering, which used a purchase agreement, may raise similar questions.[119]

These multi-stage offerings raise the question for regulators of whether the forward delivery of a token can be sufficiently separated from the initial investment contract such that when the token becomes usable (when the associated network is also truly decentralised), it will not be considered a security.

115 The Munchee Order, paragraph 35.
116 "Venture Capitalists Seek 'Safe Harbor' for Virtual Currencies", *New York Times*, 19 April 2018.
117 Amongst other exemptions from registration are Regulation D for private placements to accredited investors and Regulation A+ for smaller early stage company offerings; see https://www.sec.gov/smallbusiness/exemptofferings
118 "$257 Million: Filecoin Breaks All-Time Record for ICO funding", Coindesk, 7 September 2017.
119 "Telegram's TON ICO: A Legal Look at the Most Hyped ICO of 2018", Cryptovest, 8 March 2018.

Specific considerations – crypto-exchanges

There also are a number of specific areas for consideration related to crypto-exchanges.

Custodial duties

Crypto-exchanges have had significant challenges in protecting customers' funds. Unlike traditional exchanges, crypto-exchanges hold significant customer funds in digital wallets. The aggregate of these customer crypto-assets is then represented on a particular token's blockchain associated with the public keys of the exchange, not the individual customers. In contrast, customers trading on traditional exchanges with intermediated access have their securities recorded at a transfer agent and held by a broker or dealer, not the exchange.

The public policy goals should be the same whether the asset is crypto in nature or a more traditional security. Exchanges and their affiliates should not lose or use customer funds.

Under US laws, the key question is how will custodial duties be fulfilled? Under US securities laws, this has generally been accomplished through the segregation and custodial duties of broker-dealers. Under CFTC jurisdiction, there are differing custodial requirements for retail foreign exchange dealers (RFED), futures commission merchants (FCM), and commodity warehouses held by designated contract markets (DCM).

Similar questions are ripe around the globe. In some jurisdictions, exchange custodial duties might appropriately align with bank custodial requirements.

When considering existing custodial rules, the specifics of blockchain technology, public keys and cryptography will need to be considered. New technologies, such as multi-signature controls, might protect customers or fulfil certain custodial responsibilities. Added safeguards need be considered for the private keys associated with the public keys of exchanges, asset managers, banks or regulated intermediaries. Additional cyber-security and other safeguards might be appropriate, particularly given the numerous losses and hacks that have occurred in the past.

Market integrity

Investor protection and market integrity rules will need to apply, though possibly tailored to this new scenario. In the US, crypto-exchanges offering post-launch ICO tokens, crypto-derivatives or related products will need to comply with rules established for traditional exchanges for securities, commodities and derivatives. In other countries, this has yet to be established.

Decentralised exchanges

Registration and regulation of decentralised crypto-exchanges may present a challenge. Using blockchain technology, a number of emerging decentralised exchanges have begun trading without a centralised platform or matching engine. These decentralised exchanges generally take no custody of funds and provide for peer-to-peer trading based upon open-source algorithms. This raises a number of novel questions for regulation.

In particular, if an exchange is but a distributed, open-source software protocol, where and how might a registration requirement be applied? Regulators will need to consider how best to enforce any regulatory requirements. For those decentralised exchanges that have a sponsor company, it might be appropriate to attach requirements to that company, but there might be gaps in enforcement. If a decentralised exchange traded fiat currency and cryptocurrency pairs, regulators might be able to use the banking system (through the on-ramps and off-ramps of the exchanges) to effect policy at these exchanges. Further, regulated intermediaries might not be allowed to transact on such platforms. To an extent, though, some pure crypto-to-crypto decentralised exchanges are likely to try to operate outside of regulatory oversight.

Financial stability, illicit activities

Regulators want to ensure that crypto-exchanges do not lead to financial instability or greater illicit activities, such as money laundering or financing terrorism. Many international jurisdictions are moving to require that exchanges comply with AML, CFT, and KYC laws. In the US, in the absence of federal registration, crypto-exchanges are still required to comply with money transmission laws and thus register in the individual states. If exchanges fail to do so, they may be violating federal law.

As a public policy goal, it is important to ensure that crypto-exchanges do not lead to, or add to, instability, particularly in volatile or uncertain markets. While bitcoin futures listed at CME and CBOE require nearly 50% margin, most crypto-exchanges allow for much lower margin (and thus higher leverage) when trading bitcoin and many other crypto assets. BitMEX provides 100:1 leverage (only 1% margin) for bitcoin trading. While few exchanges allow such high leverage, many offer leverage above 10:1.[120] Given the high volatility of the underlying assets, significant leverage could add to instability and stress during down markets. As so many exchanges remain unregulated and lack transparency, however, it may be challenging for central banks and others responsible for financial stability to get an accurate window into these markets.

Type of registration

Crypto-exchanges and regulators will need to consider which type of registration is appropriate.

Around the globe, exchanges roughly fall within three registration categories: a) securities exchanges for issuer-based stocks, bonds or related investment products; b) derivatives exchanges for futures, swaps, contracts for differences, binary options and the like; and c) commodity exchanges for foreign currency (FX) or physical commodities (energy, metal or agricultural). While all registration categories seek to achieve similar policy goals, there are some important differences. Securities exchanges generally have additional requirements related to issuers and investor protection. Derivatives exchanges have additional concerns related to leverage and possible manipulation of underlying referenced data. FX and physical commodity exchange regulation tends to be less robust or non-existent, other than for retail commodity exchanges.

120 As of 27 May 2018; see https://bitreview.com/trade

There have been some initial efforts by Gemini and other crypto-exchanges to form a self-regulatory organisation (SRO), fashioned on similar SROs for traditional exchanges.[121] Such an SRO, though of possible aid, would not fully address the investor and market protection goals of regulatory registration and oversight.

The Securities and Exchange Commission

If a crypto-exchange offers for sale to US persons any post-launch ICO tokens or other digital assets that are securities, then that exchange must register with the SEC as an exchange or an alternative trading system (ATS). This was made clear when the SEC published their Statement on Potentially Unlawful Online Platforms for Trading Digital Assets.[122] The SEC Director of Trading and Markets later stated that: "There are no registered exchanges, there are no registered ATSs (Alternative Trading Venues) trading any of these products … That is a very big concern for us."[123]

This will require many crypto-exchanges to register. Some have already done so. If XRP or EOS are deemed to be investment contracts under US law, though, it would affect which exchanges require SEC registration.

Under US securities laws, there are two principal registration categories for entities providing exchange services: national securities exchanges and ATSs. Registration as an ATS also requires registering as a broker dealer and joining a self-regulatory organisation. These registration regimes were designed to promote investor protection and market integrity in the traditional securities markets. The SEC might consider, though, some new form of exchange registration category, as they did in the 1990s with the emergence of the internet.

The SEC will need to consider how crypto-exchanges might fit within certain features of current regulations for a national market system. For instance, what trade reporting rules would apply to these products, or might ICO pricing be fed into a national market tape? Exchange access, a key feature of current market structure, would need to be granted and achieved with other exchanges, whether existing ATSs or national securities exchanges or newly registered crypto-exchanges.

The Commodity Futures Trading Commission

If an exchange offers derivatives on cryptocurrencies, then that exchange must register with the CFTC. Crypto-exchanges that offer to US persons 'retail commodity transactions' as defined in statute could also be subject to the authority of the CFTC.

Crypto-exchanges registering with the CFTC, might consider registering as a DCM or a swap execution facility (SEF). Exchanges that offer leverage or margin for the purchase of cryptocurrencies may come under the definition of offering 'retail commodity transactions' and thus be required to register as exchanges.

121 "A Proposal for a Self-Regulatory Organization for the Virtual Currency Industry", Gemini, 13 March 2018.
122 "Statement on Potentially Unlawful Online Platforms for Trading Digital Assets", SEC, 7 March 2018.
123 "Stock market principles needed in crypto world: SEC official", Reuters, 22 March 2018.

Given some similarities with retail foreign exchange dealers and crypto-exchanges, the CFTC might allow registration as an RFED (though cryptocurrencies are not foreign currency), while ensuring that cryptocurrencies remain distinct from fiat currencies for other parts of the commodities law.

The CFTC has yet to finalise a proposed interpretation that may help determine the breadth of crypto-exchanges that will need to register. US law treats as a commodity future any retail commodity transaction entered into on a leveraged or margined basis that does not have actual delivery of the underlying commodity within 28 days. Further, cryptocurrencies have been determined to be commodities under US law.[124] As most crypto-exchanges provide margin to retail customers for more than 28 days, these exchanges might arguably be offering trading of a form of a commodity future. Under the commodities laws, such contracts would need to be traded on a DCM and any person soliciting or accepting orders or acting as a counterparty to a retail commodity transaction and accepting customer money to margin, guarantee or secure such transactions must register as an FCM.

The CFTC put out for public comment a proposed interpretation regarding exceptions for 'actual delivery' that might apply for virtual currency. Depending upon the final guidance on actual delivery, many crypto-exchanges may be required to register with the CFTC.

In addition, the CFTC has general anti-fraud and manipulation authority for commodities traded in interstate commerce. As cryptocurrencies have been determined to be a commodity under US laws, this gives the CFTC general anti-fraud and anti-manipulation authority for cryptocurrencies, whether traded on exchanges or over the counter. The CFTC has brought a number of actions under this authority, one related to the trading of Bitcoin and Litecoin[125] and another with regards to the trading of My Big Coin.[126] The CFTC may also consider if this general authority would provide it with the ability to write rules for trading on crypto-exchanges.

Congress

Another question that has been raised is whether Congress might decide to act to require registration of crypto-exchanges that do not currently fall under SEC or CFTC registration requirements. Such exchanges would be those that neither offer for trading any securities or crypto-derivatives, including 'retail commodity transactions'.

Currency exchanges serving institutional customers, such as Thomson Reuters or NEX Markets, are not currently required to register. A different path might be considered for institutional cryptocurrency exchanges. The two chairs of the SEC and CFTC raised such a question in an opinion piece published in January of 2018.[127]

124 "Bitcoin and Cryptocurrencies Are Commodities, Federal Court Rules", Bitcoin.com, 7 March 2018.
125 See https://www.cftc.gov/PressRoom/PressReleases/pr7702-18
126 "CFTC Sues Obscure Crypto Scheme for Fraud", CoinDesk, 24 January 2018.
127 "Regulators ask Congress for more power to police cryptocurrencies", *The Hill*, 25 January 2018.

5 Broader potential economic impact

The global economy has an age-old challenge of mistrust, which has traditionally been resolved by centralised intermediaries. It is here that blockchain technology offers new tools that can be applied beyond finance, creating a decentralised platform for trust management that might more easily allow communities to work together, engage in commerce and attack problems.

The interest in blockchain technology has grown to cover many use cases beyond the financial sector in recent years.

Supply chains

One area of intense research and development for blockchain technologies covers the broad field of supply chain management, shipping and logistics, and trade finance. Supply chains are seen as prime use cases for blockchain technology since their members operate within a context of both common objectives and mutual mistrust. With the capacity to track data from smart devices embedded in factories, depots, vehicles and shipping sites and to automatically execute payments and document delivery via smart contracts triggered by this data, blockchain concepts promise to breach the trust gap that has traditionally hindered communication across members of a supply chain. As such, the technology is seen improving efficiency, resource usage, provenance and traceability, as well as credit availability.

One indication of how effective this could be is found in the ambitions of Hong Kong's Belt and Road Blockchain consortium. Composed of banks, shippers, consultants and tech companies, the BRBC is developing a standardised system of blockchain-based corporate identifiers and a common dispute resolution mechanism to help make this technology the enabling platform for China's planned $1 trillion Belt and Road initiative. That massive project encompasses a network of cutting-edge, smart manufacturing and supply chain systems across 70 different countries covering two thirds of the world's population.

In two high-profile trials, IBM and Walmart used distributed-ledger technologies to trace the movement of Chinese pork[128] and Mexican mangoes[129] along a supply chain by integrating data from farmers, produce buyers, shippers, delivery companies, wholesalers and the retail giant itself. By making information that would not otherwise be shared available to chain members, the retailer was able to more readily identify the origins of tainted food. Walmart, Unilever, Dole Foods and others later joined an alliance with IBM to deploy blockchain technology for the food industry.

128 "Walmart and IBM Are Partnering to Put Chinese Pork on a Blockchain", *Fortune*, 19 October 2016.
129 "Business Interest in Blockchain Picks Up While Cryptocurrency Causes Conniptions", *Wall Street Journal*, 6 February 2018.

In a similar vein, blockchain start-up Everledger has promoted its work tracing diamonds, prompting Anglo American Ltd unit De Beers to team up with BCG Digital Ventures to do the same, in part to achieve compliance with industry rules barring conflict diamonds from global markets.[130] And on the shipping side, shippers such as Maersk are working on blockchain and smart-contract solutions to streamline the processing of customs and shipping procedures.[131]

But these blockchain systems for monitoring the flow of goods and services – as well as work processes along supply chains – will need a means of arbitrating disagreements and correcting potential errors that lives outside of the digital ledger, lest that immutable record lock in unfair or faulty data. This dispute resolution process could be handled by courts in official legal models or, as some have argued, it could be based on a distributed, multi-stakeholder model like that of the Internet Corporation for Assigned Names and Numbers (ICANN), which adjudicates rights to the vital 'real estate' of IP addresses on the internet.

The Internet of Things

Just as there are security/trust questions around the human actors in online transactions, increasingly we are asking whether we can trust the devices we use. This will become an even bigger issue when the Internet of Things, with its billion-connected, transacting devices, is upon us.

Accordingly, another prime area of blockchain research and development is in the field of the Internet of Things. The idea is that if billions of IoT devices are in the future going to transact directly with each other in micro-transactions of currency or valuable data, there will need to be fluid, decentralised systems for overcoming mistrust and allowing machine-to-machine exchanges. For example, Context Labs is using blockchain technology, in combination with big-data-based network analyses, to prove the 'data veracity' of devices that generate uniquely identifying numbers and whose performance can be tracked, monitored and assessed in real time by testing against a blockchain-proven record.[132] Meanwhile, Intel Corp., a member of the Hyperledger consortium to which IBM, Cisco and other big tech companies belong, has developed a blockchain protocol known as Sawtooth Lake that draws upon Intel's existing SGX 'trusted computing module' to enable networks of autonomous devices to work together.

One of the most compelling use cases for blockchain-based IoT deployment is in the energy sector. A team working out of the MIT Media Lab's Digital Currency Initiative is building a prototype for a 'transactive' solar microgrid in which members of a community can trade power directly with each other based on data generated by smart meters and without the intermediation of a rent-seeking utility. The smart meters would also be linked to digital payment systems that can make access to solar power contingent on continued payments to a lender, with the goal of unlocking low-cost collateralised finance. The team hopes to deploy the microgrid pilot in a country with infrastructure challenges, where it could serve as a 'plug-and-play' economic development platform for a local community.

130 "De Beers turns to blockchain to guarantee diamond purity", Reuters, 16 January 2018.
131 "IBM and Maersk Are Creating a New Blockchain Company", *Fortune*, 16 January 2018.
132 See https://www.contextlabs.com/proofworks/

While these areas of development vary in the degree to which they touch the existing financial system, all have the potential to affect how that system functions in the future. As both people and machines move toward decentralised, smart contract-operated systems of direct disintermediated models, traditional financial institutions will have to adapt to a new economic paradigm that may or may not require their services.

With that future in mind, one in which autonomous devices can transact on our behalf in pursuit of new efficiencies and value creation, we can ask whether this vision also requires a decentralised trust architecture and, if so, whether blockchain technology fulfils that. There is general momentum in many sectors towards a decentralised economy, as business models built upon platform services such as Uber and Airbnb push more autonomy out to 'the edges'. Meanwhile, cities and countries, seeking greater energy security and efficiency, are encouraging the spread of decentralised, distributed microgrids and incentivising their citizens to install smart, internet-connected measuring devices in their homes.

Is it possible or appropriate to marry a traditional centralised trust architecture with this emerging decentralised economic model? Should we/can we insert centralised public utilities (which are, among other things, centralised ledger-keepers, checking everyone's meters and invoicing them accordingly) as intermediaries into all those micro transactions? And if not, how are all those autonomous actors and their devices going to trust each other?

Allowing decentralised networks of devices to trade digital assets and currencies directly with each other can create market mechanisms that could be used to signal more efficient resource usage across multiple sectors of the economy as they start to become digitally interconnected. These core problems and opportunities underpin why people are talking about blockchain technology's potential in IoT and in decentralised infrastructure generally. But with all the scaling and governance obstacles that public blockchains such as Bitcoin face, it is not yet possible to roll out this technology as a solution for mass usage.

Does that mean that permissioned blockchains, which do not require the computing power of proof of work and are much more easily governed than the messy open-source structure of Bitcoin or Ethereum, are the best place to start? Perhaps. But how do we guard against those running permissioned blockchains collecting economic rents or building an exclusionary monopoly? Is it best for the economy if GE or Toyota were to run the platform over which electric vehicles trade information? How would start-ups with potentially better models be able to break into that environment? Trusting third parties that operate permissioned IoT systems may undermine the principles of open-access, competition and permissionless innovation that promote a dynamic economy.

Perhaps rules that require open application programming interfaces (APIs) and which establish anti-monopoly governance structures can resolve this without requiring a public blockchain. But, with trust being so important to the functioning of these exchange systems, the perception of centralised control could limit the broad appeal of permissioned networks within the IoT world.

Identity

Research is also focused on improving identity management, both for the traditional identification function carried out by established industries such as banking (as discussed in Chapter 3) and for an emerging decentralised, autonomous concept known as 'self-sovereign identity'. The latter focuses on using cryptographic key pairs and attestations to form a decentralised, user-controlled identity, and is being pursued by both the MIT Media Lab, in the form of Blockcerts,[133] and by Consensys, a decentralised application development lab based on Ethereum. The concept moves away from a centrally issued identity that may leave troves of personal identifying information vulnerable to theft and exploitation to one where people have greater control over how they are identified. The Blockcerts project at the MIT Media Lab is an open-standard suite of applications for issuing and verifying credentials which espouses certain principles – the user is in control of her own credentials and can prove those credentials even if the issuing institution no longer exists or is offline. Since 2016, dozens of institutions around the world have used the Blockcerts standard to issue certificates, including MIT itself.[134]

Like some other use cases, self-sovereign identity requires a high degree of sophistication and effort on the part of the end user – securely maintaining a private key without losing or forgetting it is difficult, and anecdotes abound of bitcoin lost forever due to people tossing out slips of paper or old hard drives being thrown away. Similar challenges must be overcome for fully self-sovereign identities to become practical.

Identity is a difficult challenge to meet and blockchain technology is not a magic bullet. Issues of privacy and security, heightened by a rash of cybersecurity breaches of personal information at various entities, clash with requirements for reliable attestations and proofs of attributes. Reliable forms of digital identity, however, will be critical as a foundation for society to achieve a frictionless interconnected economy.

Healthcare records

In the US, patients often have to manually transfer healthcare records between different providers, and their data are fragmented across different organisations. A project at the MIT Media Lab known as Medrec is attempting to address this problem by creating a blockchain-based system that prioritises patient agency, putting patients in charge of the sharing of their own healthcare records (Azaria et al., 2016). Medrec is provider-neutral and does not store actual patient healthcare data, instead facilitating the sharing of permissions to access those data, which stay in provider databases. The current version of Medrec uses a private Ethereum chain, with smart contracts to facilitate the sharing of permissions to access data.[135]

133 See https://www.blockcerts.org

134 See http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017 (accessed 30 April 2018).

135 See https://medrec.media.mit.edu/.

This project is an example of how blockchain technology can help motivate organisations to agree on data standards and enable users to control their own data.

6 Conclusions

Future developments in technology

Despite the many technical challenges around performance, scalability, privacy, security and interoperability currently inhibiting blockchain technology adoption, there is reason to believe that many of these issues will be addressed over time. Layer 2 solutions like the Lightning Network and scalable off-chain smart contracts will help with performance and scalability; zero-knowledge proofs and other applications of cryptography can address privacy concerns. Addressing interoperability and collective action is more challenging as each requires more than a merely technical solution. In order to develop universal standards, different projects will need to work together.

Public policy goals

As Bank of England Governor Mark Carney recently said, the topline is that "[a]uthorities need to decide whether to isolate, regulate or integrate crypto-assets and their associated activities" (Carney, 2018).

The developed world has so far largely adopted an integration approach, calling for compliance with existing tax, money transmission, anti-money laundering, counter-terrorism, securities and commodities laws. Jurisdictions are also exploring whether to modify regulatory frameworks to balance the public interest in promoting innovation around these new technologies while remaining true to core policy objectives. In some cases, legacy laws may need updating. As is often said, though, 'the devil is in the details'.

More work is needed to ensure financial stability and to guard against illicit activity or tax avoidance. More clarity is needed to underlie the investment required to realise this new technology's potential. Public confidence in these markets, as with traditional financial markets, rests on clear rules protecting investors and promoting market integrity in addition to basic consumer protection frameworks. In our highly interconnected world, global coordination will enhance the chance to achieve these goals. It is only by achieving these goals, though, that governments can enable these markets to persist, businesses to fully invest and the public to more confidently participate.

Overall assessment

In conclusion, blockchain technology has a real potential to be a catalyst for change in the world of finance.

If the technical and commercial challenges discussed in this report can be overcome, this innovation could lower costs, risks and economic rents in the financial system.

For broad adoption – both as a technology solution and as part of the capital markets – the technology and its various applications need to come within existing public policy frameworks.

We continue to see significant non-compliance with respect to many ICOs, crypto-tokens and crypto-exchanges.

The basic norms and principles underlying securities and commodities laws and regulations to protect investors and market integrity should continue to guide public policy. Yet innovation must also be promoted, with policymakers open to the prospect that these disruptive, decentralised systems of exchange and governance could transform the financial and economic landscape and render incumbent business models obsolete.

Clear rules of the road also will allow firms, both incumbents and start-ups, to more fully explore investing in crypto assets or blockchain technology.

Bringing clarity and compliance to blockchain technology adoption and related markets will likely have its challenges. Market participants, the investing public, entrepreneurs, technology developers, regulators and political leaders should all play a role. In particular, ICO issuers and crypto-exchange operators should now seek to comply with the law to the fullest extent possible.

The public, blockchain technology and the financial system will all reap the benefits.

Discussions

Blockchain: Unknown potential

Stijn Claessens, *Bank for International Settlements*[136]
Thank you for giving me a chance to discuss this report. Having been part of this series myself, I know the process, so I want to be as constructive as possible here. This is clearly an important topic, also for policy. Many are focused on this: investors, households, banks, other financial institutions, regulators, and supervisors. We also know (too) little on what is going on in these markets and surely on what may happen. Could this be a development like dot-com was with (eventually) major implications, like the end of the (music) CD? Or might this be more of an evolution?

Let me start with summarising the questions the report asks and the answers it provides. The main question, as in the title, is very clear: What are the potential impacts of blockchain technology on finance? Are the choices it provides small, significant or completely transformative? The answer, at least as I read the report, is: potentially large. The report shows that the new technology can lead to large changes in the forms of financial intermediation and shifts in financial services industries. It could mean that the provision of deposit, lending, capital markets and other financial services to firms and households would change dramatically. It strongly suggests that banks would see their roles in financial intermediation much reduced.

At the same time, the report makes clear that there are still many barriers to the use of these new technologies. Some are related to the technologies themselves, as they are not yet mature or efficient enough. Some are related to the development of the market, which has the usual network and other externalities, making it hard to predict if, when and how certain technologies or approaches will take off. But there are also plenty of legal, regulatory and other such barriers that raise questions about the future development of this technology.

The report is a very useful first pass of the various issues. It reviews the new developments, with many good examples brought together. It provides some economic interpretations of these developments. It looks at both economic benefits and the costs. And it discusses aspects of (actual) regulation and supervision. I say that the report is a first pass not because the report is not of a high quality, but largely because the developments are so new and evolving so fast that it is hard to draw any definitive conclusions. Still, I think more can already be done in the current report. Let me illustrate a few ways where the report can go further.

136 The opinions expressed are those of the author and do not necessarily reflect views of the Bank for International Settlements.

First, the report could present the developments in a more general and broader context. The developments of interest today are more than blockchain (as suggested in the title). For one, DLT is the more general, transformative development; blockchain is the specific application (e.g., as used for Bitcoin and other cryptocurrencies). Much of what is of interest today relates also to fintech, techfin, and especially bigtech. Maybe the report can devote some space analysing whether these are bigger developments than blockchain, or least put the development of blockchain into context.

Relatedly, the report could try to help the reader see the blockchain and other technological developments by making (more) parallels, historical and otherwise, to what is happening today. For example, did transformative (technological) innovations succeed in earlier times, and if so when? What happened during the dot com era? What explained the successes or failures? Was it, for example, network effects that allowed some ideas to take off (or not)? I would also include lessons from history, including on monetary and financial 'experiments'. This could include some parallels to the earlier eras of free banking and wildcat banking, with their less than stellar outcomes, and the subsequent development of central banks. This would allow for a somewhat wider perspective, as analyses of blockchain and related developments in their own right are very hard, in part as history is short and data are limited.

My next major set of comments would be to do more on the economics, not just provide a list of issues and assessment criteria. Currently the paper provides a list of impediments and elements of a framework, but little analysis.[137] While it is early, there are some questions that can be asked and perhaps answered. The very general ones are: What can make this work (or not)? What specific economic problems could the new technologies solve? How do the new technologies compare to current approaches (e.g., in terms of costs and benefits)? What are the resulting policy issues in these new areas? These questions are probably not 'answerable', but could still usefully frame the next level of more specific questions.

Some specific questions that I came up with for which one could use (some) economics to (help) judge various aspects are the following:

1. What are the various cryptos exactly? Can one differentiate cryptocurrencies versus cryptoassets versus cryptocommodities versus cryptotokens versus cryptosecurities? How do their economic roles differ?
2. Can one clarify the role of new technology versus the use of existing financial services and systems? It appears to me that some developments are not necessarily new. For example, the overlays used around cryptocurrency to get easier user interfaces or lower transaction costs are not new.
3. Are the new systems set up for scale? This has a set of well-defined sub-questions, for example, what are the network externalities? Positive or negative? Are costs per unit going down with more users or going up? From an anecdotal perspective it seems that the transaction costs are

137 The impediments listed in the report are (1) performance and scale; (2) privacy and security; (3) Interoperability among DLTs; (4) governance, updates; (5) real world use cases; (6) collective action problems; and (7) public actions, legal framework. The assessment criteria listed are (1) cost of trust reduced; (2) technical limitations overcome; and (3) switching costs smaller than gains.

not only high, but also spike as demand increases. This suggests that congestion problems are large, which does not bode well for scaling up.

4. Another question is whether incentives across all agents are truly aligned to make for a stable system. Again, we have tools here from economics. How is consensus and trust exactly created? Is this 'sub-game perfect'? Can we get 'off-equilibrium' outcomes? Especially for cryptocurrencies, these questions are of major importance. Will there, for example, be (too much) forking (akin to 'free banking')? Is there finality of payment?
5. Another issue that could be analysed is what exactly are the competition policy issues? As in other cases – such as telecommunications with the entry of new providers or technologies, or during the development of the dot-com – we see now competition for the market. But, as network and other externalities are likely to arise, we will have more concentration and then many traditional competition (policy) issues will arise. One could review some of this and develop an approach going forward.
6. On regulation, one question is what could be the best paradigm for ownership and pricing of data now being shared most often freely by users, but that are valuable for the providers? As argued by some, the ownership of data really belongs to the user, but now the provider of services uses the data to cross-subsidise some products. It this the best paradigm? This issue of data ownership may also have applications for fintech.
7. Lastly, can one expect markets to work? Is it best, at least for now, 'to let a 1,000 flowers bloom'? Or is that inefficient? For example, does that come with much wasted resources, as in the current very large energy use for cryptocurrencies? Can we get inferior outcomes (Betamax versus VHS)? It also raises the question of the role of government. Should government help the developments in some ways? If so, when and how could it best intervene? Should it enforce standards and other rules? Can it at times address interoperability? What are the lessons from the development of payments systems, telecommunications and credit cards, among others, where similar issues arose? Here, of course, the political economy and the role of various (vested) interests becomes important. For example, can and will existing financial intermediaries create (wrong) barriers?

A third set of comments would be to reframe the regulation section. Currently, it is very legalistic, about quite detailed questions, and often US centric. The report needs to adopt a more economic view of regulation, which should be more about principles. And it has to take a global perspective.

As always, the starting point should be to ask what are the market failures or externalities. I have already given some suggestions of what issues can be addressed here. I would add to this that, in the case of cryptocurrencies, it would be good to analyse where the system tries to cannibalise, or borrow 'trust' or legitimacy from the formal financial system. Could this be because that part of the system is more regulated and perhaps benefits from a publicly provided safety net? Is this efficient or perverse?

It would be useful to acknowledge the need to have both direct and indirect regulatory approaches. The direct approaches are presumably the ones that apply for example to initial coin offerings (ICOs). This is mainly a question of regulation of securities markets. The grey area is what to do with tokens that are a product and at the same an ICO. Is then both investor and consumer protection necessary and feasible? In terms of indirect approaches, I would think that such an approach applies for ALM/CFT purposes. There the transfer into and out of cryptocurrencies from and to sovereign currencies can be overseen at the commercial banks and other exchanges involved in such transfers. This indirect way of getting at the illicit activity aspects of cryptocurrencies may suffice. But would such an indirect approach also apply to other issues? Is there a need to adapt regulatory paradigms? And if so, where? For example, is there a need to redefine 'legal tender' to address shifting economic roles?

Finally, the regulation section is very US focused, which the authors admit. But in many aspects one needs a global perspective and global approach. To date, this has proven hard, in part since countries have different views on this, and on cryptocurrencies in particular. In some countries cryptocurrencies are banned; in others they are allowed to trade on derivatives stock exchanges; in yet others, they face some regulatory limits. At the same time, it is clear that many of the regulatory approaches cannot succeed unless they are globally and consistently applied. How to go forward will thus not be easy, but perhaps the report can document approaches to date.

Lastly, I think that the presentation can be much improved. For one, it would be good to clarify the nomenclature, for example, what are cryptocurrencies versus cryptoassets versus cryptocommodities versus cryptotokens versus cryptosecurities? This would help many readers and people writing on this topic in making better differentiations. Another suggestion is to use more infographics, which is often an efficient way to clarify the concepts. For example, to explain centralised versus decentralised or permissionless versus permissioned, one could use some charts of various types of networks. It would also reduce the length of the report and avoid repetition. As it is, the report is very detailed in some areas (for example, it would be easy to reduce some of the regulatory details). At the same time it could expand other, crucial areas where it is short, like the economics part.

Finance and the blockchain: A comment

Stephen G. Cecchetti, *Brandeis International Business School (written with Kermit L. Schoenholtz)*

> "Only 1% of 3,138 chief information officers at companies surveyed by Gartner last year said they had 'any kind of blockchain adoption'…." *The Wall Street Journal*, 7 May 2018.

Blockchain is all the rage. We are constantly bombarded by reports of how it will change the world. While it may alter many aspects of our lives, our suspicion is that they will be in areas that we experience only indirectly. That is, blockchain technology mostly will change the implementation of invisible processes – what businesses think of as their *back-office* functions.

In this comment, we briefly describe blockchain technology, the problem it is designed to solve and the impact it might have on finance.

The blockchain is a record-keeping mechanism. In that sense, it is simply a 21st century version of the systems that have been around since people started chiselling marks on cave walls. Over the millennia we have moved from ledgers that are carved into clay to ones that are digital.

To understand the most recent iteration in this process, consider the problem of tracking the ownership of a share of equity in a particular company. Imagine that there is a sequential list of all owners of that share, with the name of each former owner crossed out. The last one at the bottom of the list is the current owner. The key question is the following: Who has the right to cross out that last name and to write in a new one?

Put another way, the challenge we face is to create a tamper-proof and universally accepted way of recording things like ownership of assets, obligations of one person to provide a product or service to another, levels of inventories, personal identities, and the like. The world runs on records of who we are, what we own and what we are obliged to do. Having a secure and trusted mechanism for accessing and changing those records is essential if our lives are to function smoothly.

Before proceeding further, it is worth pausing to make a point about the details of blockchain technology. While it is critical that someone create and implement high-quality security mechanisms, most people will have little concern for the details. For example, we all care that our information is safe when we provide our credit card numbers to make an online purchase. However, few know the details of the encryption technology that secures the transaction. Similarly, our interest in blockchain technology is in the services it delivers, not the details of how or why. In the same way that automobile engines are for mechanics and engineers, hash functions, nonces and the like are for computer scientists and mathematicians.[138] What we require is that the system be reliable and that it cannot be hijacked by people with ill intent.

Returning to the question at hand, in thinking about the challenge of maintaining records – a ledger – it is useful to consider differences along two dimensions: the *structure* of the database in which the records are stored, and how we establish that any changes are legitimate. Along the first dimension – call it *ledger structure and ownership* – the database and its ownership can be either *centralised* or *distributed*.[139] And, on the second dimension – *access rights* – we can have a *limited-access* system in which either a restricted number of people (or entities) have permission to make the alterations, or we can arrange an *open and public* ('permissionless') mechanism whereby anyone can participate. In either case, once someone makes a legitimate modification, all versions are immediately updated automatically, guaranteeing agreement on the current state.[140]

This two-by-two classification system leads to four possibilities that help us to distinguish among various ledger frameworks. To understand this taxonomy, the following two tables regarding the ledger structure and access rights provide a set of nonfinancial and financial examples.[141] It is worth going through each of the four cases separately.

138 See https://en.wikipedia.org/wiki/Hash_function and https://en.bitcoin.it/wiki/Nonce .
139 We abstract from systems that are partially centralised.
140 We assume that the security system in place allows control of who can see what.
141 For a more detailed discussion with examples, see Haeringer and Halaburda (2018) and Dwyer (2017).

Table 1 Ledger structure and ownership, and access rights: Nonfinancial examples

		Access rights	
		Limited/Proprietary	Open/Public
Ledger structure and Ownership	Centralised	Hospital records (Current systems)	Customer ratings (User review websites)
	Distributed	Supply chain inventory* (Closed, trusted networks)	Property title* (Proof of work/stake systems)

Noite: *Potential implementations.

Table 2 Ledger structure and ownership, and access rights:Ffinancial examples

		Access rights	
		Limited/Proprietary	Open/Public
Ledger structure and Ownership	Centralised	Securities ownership records (Current systems)	CFPB Consumer Complaint Database (User review websites)
	Distributed	CLSnet (Closed, trusted networks)	Bitcoin (Proof of work/stake systems)

Note: CFPB is the Consumer Financial Protection Bureau.

The upper left cell of each table is the case of a centralised database with limited, proprietary access rights. This portion of the taxonomy pretty much captures the ledger practices of human civilization until now. That is, there is one central ledger that contains the authoritative record of ownership or obligations and can only be changed by the organisation responsible for maintaining it. Those authorised by this entity not only have the sole right to make changes, but also control who can view the entries. While there may be copies, there is only one definitive version. Examples of this are easy to find: hospital records and records of securities ownership are just two.

Turning to the top right cell, this is the case of an open-access, but centralised recording system that allows anyone to write and read. Since there is little or no security, this mechanism is of fairly limited use. Nevertheless, examples exist. In the nonfinancial realm, these include the customer rating systems employed by Amazon, eBay, TripAdvisor and the like. It also is the mechanism that Wikipedia uses for creating and updating entries. Given the security concerns, financial examples are more difficult to find. We can think of one instance of wide use: the Consumer Complaint Database of the Consumer Financial Protection Bureau (CFPB).[142]

142 See https://www.consumerfinance.gov/data-research/consumer-complaints/

The bottom row covers the range of distributed (or decentralised) databases. The distinction here is that there are now many copies of the ledger, and they all have equal standing. Furthermore, anyone who has one can change it, so long as they follow an agreed set of rules. Put another way, participants directly interact with each other. And, as with the centralised systems, there can be two cases: proprietary with limited access, and open and permissionless.

Blockchain technology is designed to implement distributed systems. It does this by providing automatic mechanisms that create trust, ensure there are no conflicting changes, and prevent malicious actors from making unauthorised or improper changes. It has the potential to record transactions between two parties, maintaining an agreed sequence, without reliance on costly third-party verification.

To prevent people from arbitrarily attacking the system, violating trust and making illegitimate modifications, the ability to alter the ledger is based on a scarce resource. In the closed, permissioned model, that scarce resource is identity – only specific people or institutions with particular attributes are authorised to make modifications. The idea of an open, permissionless system is to make identity irrelevant – anyone can join, leave and re-join as often as desired. In this second case, the scarce resource that allows one to alter the ledger can be something like computational power or a stake (possibly financial) that you have in the system.[143]

In the open system, participants are allowed to make changes so long as they follow the rules. Importantly, the rules must be designed to prevent someone from capturing the system. The original Bitcoin protocol, where the scarce resource is computational power, made the system immune from takeover so long as no one controls more than half of the computing power.[144] But, as has been pointed out repeatedly, Bitcoin is incredibly resource intensive. Electricity cost alone exceeds $3 billion per year.[145] In economic terms, this is a pure deadweight loss. In environmental terms, it is a disaster.

As the opening citation indicates, both financial and nonfinancial uses of the blockchain remain limited, with the obvious exceptions of Bitcoin and other cryptocurrencies. In the first table, we have listed two possible nonfinancial applications – supply chain inventory management and property title records – but as far as we know, neither of these has yet been implemented on a broad scale.

Where is this all heading? Without a further theoretical breakthrough, open distributed systems appear both costly to implement and slow. Estimates for the Bitcoin protocol, for example, are that speeds cannot exceed seven transactions per second.[146] In contrast, there may be some promise in distributed systems that are proprietary. We suspect that most of the CIOs working on such projects have this kind of architecture in mind, perhaps in the hopes of creating a profitable monopoly. Unfortunately, a monopolist would be unlikely to lower transactions costs in the way that the advocates of open distributed systems hope. In the

143 Importantly, the protocol for making changes has to prevent malicious agents from creating a very large number of identities – what are known as 'Sybil attacks' – to overwhelm the system. See https://en.wikipedia.org/wiki/Sybil_attack .

144 See https://en.wikipedia.org/wiki/Bitcoin_network.

145 See https://digiconomist.net/bitcoin-energy-consumption.

146 See https://en.wikipedia.org/wiki/Bitcoin_scalability_problem.

world of finance, one proprietary example is CLSNet, a bilateral payment netting solution that lowers transactions costs using distributed ledger technology.[147] It is owned and operated by CLS, a leader in foreign exchange settlement, and is just getting under way.

Conceivably, a blockchain system could securely track the ownership of every financial instrument and exposure in the global economy. While this is a very tall order, it would be truly revolutionary. Money laundering and terrorist finance would be much easier to police. Authorities could monitor position concentrations and systemic risk. And financial market participants could overcome information asymmetries, improving risk pricing and capital allocation.

This sounds great, but we are still a long way off. For example, before we can map the entirety of the financial system, we need to be able to identify both entities and instruments. We have written about the virtues of the Global Legal Entity Identifier (LEI) and the importance of universal adoption (Cecchetti and Schoenholtz, 2017b). But a complete mapping also would require global financial instrument identifiers (FII). While the LEI process is now well advanced, as far as we know, no one has plans to implement FIIs.

Suppose, for a moment that LEIs and FIIs were all in place and that everything was recorded on a proprietary distributed ledger that the public can view (perhaps for a fee). This would mean that everyone's balance sheet will be public. Put differently, anyone will be able to see everyone else's complete set of financial exposures. They could even ascertain your counterparty's exposures, so they will be able to map even your indirect exposures.

From the point of view of law enforcement, financial regulators and risk managers, such a system could be a dream. However, in a democratic society, we would be astonished if any financial institution (let alone investors) would willingly supply the information needed to make this feasible. It would be a *world without privacy*. Even if a much less invasive version were to become possible, it would be deeply ironic if the blockchain, a technology initially championed by libertarians disenchanted by government and fiat money, ended up by narrowing the range of individual freedoms.[148]

Before we conclude, we should mention the problem of scalability. Before blockchain technology can alter key aspects of the financial system, there will have to be a breakthrough in speed. Today, the fastest proprietary blockchain systems can handle no more than several thousand transactions per second.149 In practice, the speed is likely far slower, unless there are only a small number of geographically proximate nodes in the network.[150] To put this into perspective, at its peak, DTCC processes 25,000 equity transactions per second (this is roughly the level of VISA's payments processing capacity).[151] In a recent report, DTCC

147 See https://www.cls-group.com/products/processing/clsnet/.

148 We do not preclude the possibility that computer scientists will adapt a technique known as zero knowledge proof for the assessment of risk in financial networks. But as of yet, they have not. See https://en.wikipedia.org/wiki/Zero-knowledge_proof.

149 See https://www.fool.com/investing/2018/02/01/3-cryptocurrencies-processing-1500-or-more-transac.aspx

150 Recall that in a distributed ledger all of the copies have equal standing. That means that before one person can record a change, they have to be certain that they have the most current version. This limits the number of transactions to the distance that information can travel through the network, known as the latency of the system. Given that the effective speed of light in a fiber-optic is roughly two-thirds the speed in a vacuum, this means that it would take something like 30 milliseconds for information to go the 5,600 km between New York and London (one way).

151 See https://usa.visa.com/run-your-business/small-business-tools/retail.html .

points out that any new technology would have to have a maximum capacity of 2 to 3 times this peak – that is, it would have to be able to handle at least 50,000 equity transactions per second (Depository Trust and Clearing Corporation, 2018). Considering that computer scientists have been working on this problem for the better part of the past half century, boosting blockchain capacity (in a low-cost, environmentally acceptable way) remains a major challenge.

All that said, we really have little idea where this will all lead. Nearly a decade since the appearance of the paper that launched Bitcoin (Nakamoto, 2008), we have more than 1,000 crypto-clones. But where are the broader applications of the blockchain technology? As CLSNet suggests, we expect that it will find increased use in the clearing, payments and settlement system (Cecchetti and Schoenholtz, 2017a). Perhaps it also will be applied across a range of other activities, such as recording property titles or managing the supply chain both within and across firms or for a variety of accounting and audit functions. Such applications would likely focus on cases with limited numbers of transactions and where speed is less important. But, for now, it looks like the proprietary, rather than the open-access, mechanisms are in the ascendance.

We'll be waiting for the thousands of CIOs to let us know.

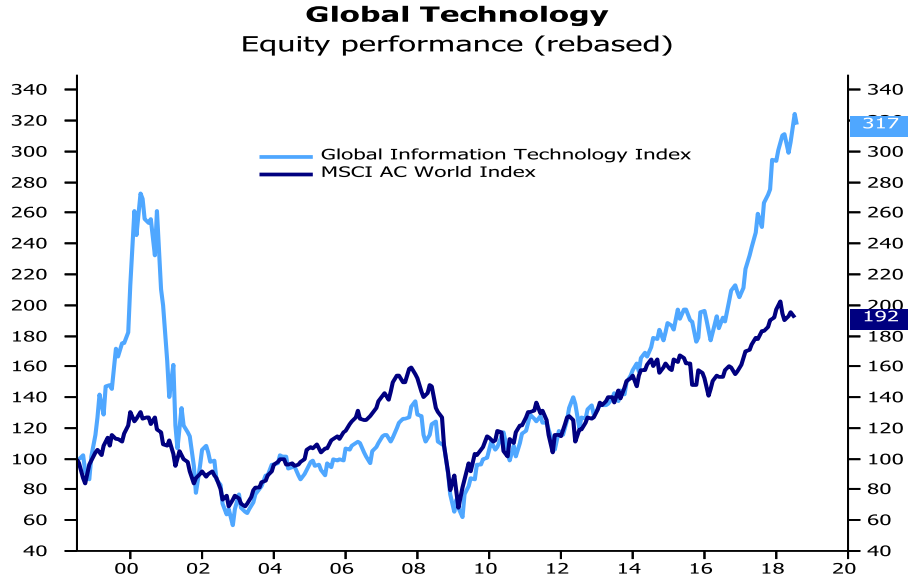
Tech disruption (where is the cash flow?)

Leslie Teo, *GIC Singapore*

I commend the report on a comprehensive discussion of the opportunities and challenges for blockchain. In my view, it rightly points to the transformative, perhaps revolutionary, nature of this technology. From the perspective of a global multi-asset investor – not a VC or founder of a crypto-currency – however, my message is sedate. Blockchain could be revolutionary, but its impact on investment should be no different from other revolutionary innovations such as the telegraph or the internet, or CRSPR and graphene. From an investing point of view, there is not much that is new here. This would make for a short interjection so allow me to elaborate.

Just to be clear, I focus on blockchain not applications such as cryptocurrencies. In addition, while I'm a big fan of technology, the tech sector is one that, at the current moment, closely meets Kindelberger's description of a bubble. Valuations are high both in public and private markets (Figure 1).

Figure 1 Relative performance and market value of global tech



Source: Thomson Reuters Datastream.

Source: Thomson Reuters Datastream.

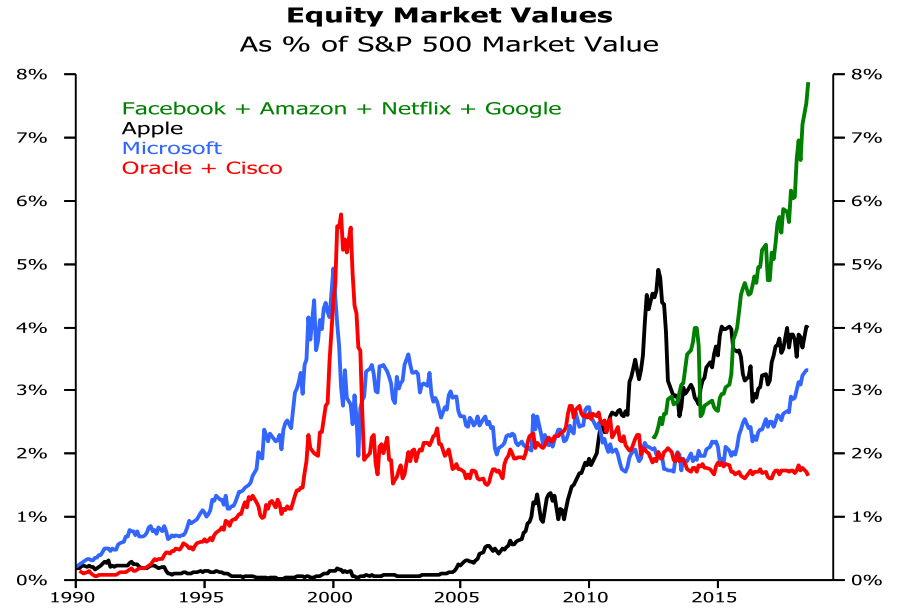
Let me begin with a simple framework to evaluate the impact of disruptive technologies such as blockchain on an investment portfolio. First, I consider the investment opportunity that it creates. Second, I consider its impact on the current investment universe – the incumbents. Third and finally, I consider its impact on us as an investor.

Does blockchain create new investment opportunities? Yes, it does. Indeed, there are even ETFs that purport to give one exposure to 'blockchain'. But buyer beware. In addition, investors face at least three challenges when trying to invest in new tech. First, of course, is finding the right 'company' to invest in. Picking winners is very difficult. And there is no 'blockchain' company per se. No one standard or platform. At my last count there were nearly 20 platforms. Second, even if one could pick a winner, scale is another challenge. One might make 100X on investment, but if the initial investment is $100,000 it isn't going to move the needle for an institutional investor. Finally, perhaps the largest amount of money is going to be made from new business models that take advantage of the possibilities enabled by blockchain. We see this in the case of the internet for example, with Google, Facebook, Netflix or Tencent solving age-old problems on top of the internet. For investors, it is hard to invest in a theme, even one as promising as blockchain. In Figure 2, one might have thought that TELCOs would have benefited from the internet.

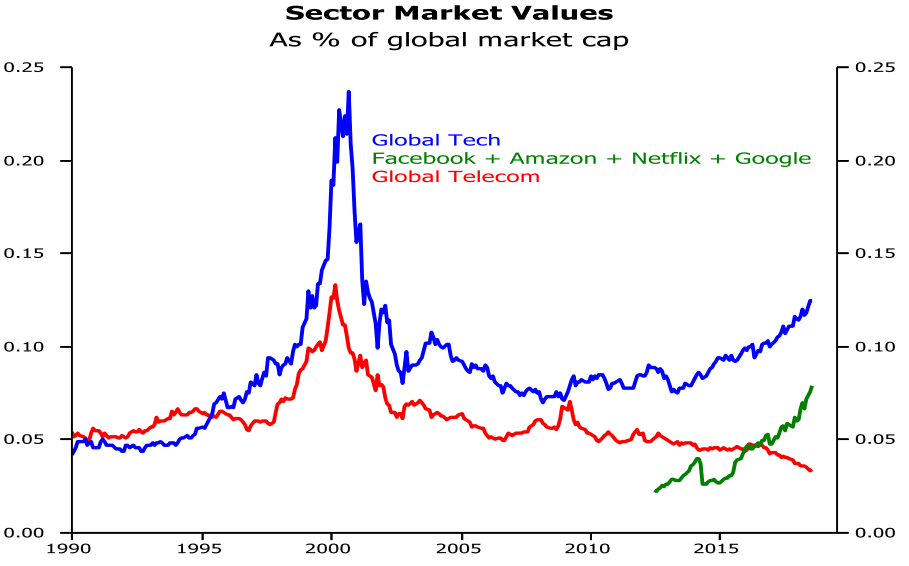
So perhaps the more important impact on blockchain would be its impact on current companies and business models. As the saying goes, if one were long auto stocks since their inception one would have gone bankrupt. What is more certain is being short on horses or railroads.

Which activities would be vulnerable to blockchain? One point to make is that blockchain – a distributed, decentralised ledger – could be used in a vast range of applications that involve intermediaries. We are not there yet, but it's a matter of time. More specifically, as the report points out, I can imagine applications in payment systems, IoT, communications, healthcare, public procurement, cyber security and legal documentation. Second, the hard work, unfortunately, is in understanding how incumbents will adapt, and determining who wins and who loses. Thus far, if my earlier point is that we don't see clear winners, here I make the point that we don't see clear losers either. Figure 3, for example, shows that VISA and MasterCard haven't really 'suffered' from the advent of this technology. Or more precisely, investors do not discount their ability to adapt, including incorporating blockchain. Third, this might be obvious but there are many activities carried out by intermediaries and rent-seekers that for the participants are better and more efficiently done by current centralised systems. As noted by the report, blockchain's architecture is designed to track ownership in a decentralised manner but in a manner that is more costly. If I trust a central authority, I don't need voting by multiple nodes or wasteful proof of work, for example.

Figure 2 Acceleration in adoption of new technology and changing market composition

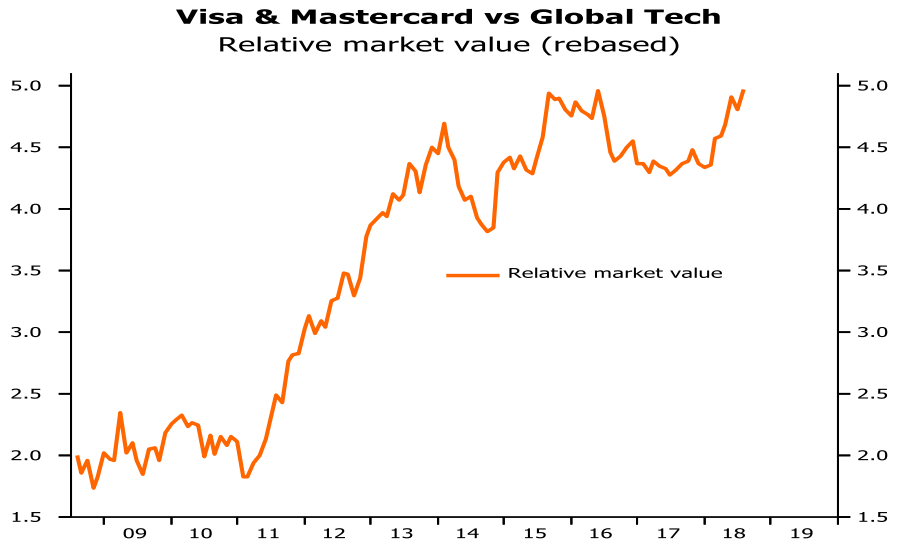


Source: Thomson Reuters Datastream.



Source: Thomson Reuters Datastream.

Figure 3 Not disrupting payment processing stock



Source: Thomson Reuters Datastream.

Finally, what does blockchain do for institutional investors? Two thoughts. First, in contrast to central banks, the threat is less existential and is pretty much good news. Blockchain applications, if useful, will be more efficient. It will lower cost for us. Second, blockchain could enable the creation of much more liquid markets in private assets such as real estate. But it is not clear if blockchain will be the underlying solution since the business problem is not one that is solved by this technology per se. Or put differently, if the underlying problem would be to create financial claims for anyone on physical assets, current financial institutions would have solved them. The reality is that terms are all negotiated

To conclude, blockchain is a great innovation. I do agree with the report that technological constraints will likely be overcome and it will transform many businesses. For investors, however, business model innovation will be as important as the underlying technology as a return driver.

Trust in a better mouse trap?

Alexander Swoboda, *The Graduate Institute*
The key question is how big an impact blockchain technology will have on finance.

Where blockchain fits

If we want to see the impact on finance, it is not going to be the impact of blockchain itself. Blockchain is a part of developments in fintech and techfin, and so on. It is really going to be the impact of blockchain or distributed ledgers together with big data, artificial intelligence, deep learning, smart contracts and the Internet of Things. The combination of these technological developments is what will (perhaps) increase productivity and lead to change, not only in the financial world but in the way we process things.

Fintech and blockchain innovation is, in a way, much more process than product innovation, even if, in services, the distinction between process and product innovation is tenuous. The impact is partly through making it possible to do things better, more efficiently than we could before. As emphasised in the report, the result will be new competitive forces and changing market structure.

From an investment perspective, one things one hears and sees in the press is 'investment in blockchain'. However, one does not simply invest in blockchain, one invests in companies – either in companies that develop technology or in a product or a service that uses blockchain. This is where we get into a lot of hype and a lot of bubbles.

ICOs

ICOs are perhaps a better way to raise funds. They are similar to, but different from, crowdfunding. The fact that all these ICOs are token based, or use tokens to fund, means that many native currencies arise – some of which are simply thin air. The fact that anyone could go online and launch an ICO is problematic, because often there is basically nothing behind these companies. It poses problems for investors, for regulation, and for the few legitimate issuers of ICOs.

As a result, ICOs raise public policy and regulatory concerns. It seems that new blockchain start-ups and native currencies tend to be built on top of existing blockchain protocols, say Bitcoin or Ethereum, increasing the value of the underlying token. Creating new digital currencies on top of older ones increases the demand for the latter. So, are we creating a sort of bubble system? What will happen when the bubble collapses? Eventually, a blockchain bubble will burst.

Market implications

The impact on the structure of financial markets could be better understood. Currently it is very speculative. There are forces that are pushing towards the unbundling of banking activities, a force towards disintermediation or away from banking concentration. At the same time, incumbents have an advantage, especially in terms of data ownership. However, asymmetries of information will still lead to a regrouping of activities within one-stop financial shops. The

reference to Coase is intriguing. The question is whether the services of a seamless one-stop financial shop (from the customer's point of view) will be provided by a coordination mechanism among separate providing entities. In this scenario, blockchain technology may be quite useful.

Trust

Sometimes it is useful to think of the cost of *distrust*. If you think of the electricity costs of bitcoin, this is a cost of mistrust. Mistrust has understandable origins in the financial crisis in libertarian ideas. Reflecting Teo's comments, not every problem has to be solved by blockchain and not every entity is distrusted. However, one of the central problems for our society and for policy is to build trust in institutions, that is, to diminish the cost of distrust.

Floor discussions

Andrea Maechler (Swiss National Bank) opened the floor discussions. She offered a brief summary of comments of the previous session as follows. Stijn Claessens (Bank for International Settlements) had emphasised the importance of specifying the potential economic problems blockchain is trying to solve, along with the associated costs and benefits of such changes. Stephen Cecchetti (Brandeis International Business School) had asked whether hope and hype overlap. Leslie Teo (GIC Singapore) had provided an investor's view, emphasising the role of the business model and cashflow, while highlighting the relevance of potential use cases. Finally, Alexander Swoboda (The Graduate Institute) had wondered how disruptive this new technology would be – in particular, if the use of blockchain or alternative technologies would improve trust, and if so, at what cost. Organising the floor discussion, Maechler categorised two main areas. First while there is plenty of potential in blockchain, concerns remained regarding its relative effectiveness, speed, cost, scalability and trust-building capacity, among other issues. Second, assuming such impediments would be overcome, she asked how blockchain fits in the policy setting and the functioning of the financial system as we know it.

What is the point?

Richard Portes (London Business School and CEPR) used various examples to explain why he does not see the need for this technology. Banks and credit card companies process millions of transactions per day, high-frequency trading seems to function pretty well, and derivatives trading works well too. For example, the ECB collects data on six million derivatives transactions per day, each transaction has 80 to 90 data points, there are algorithms that can put those into a useable format for researcher and regulators alike. Aside from the attraction of cryptocurrencies (which are speculative), the use and effectiveness of blockchain technology seems unclear. Additionally, given the clear vulnerability to hacking, systems seem no safer than the present banking and financial systems. Referring to work by Paul Seabright on trust in economic relationships, he explained that individuals enter into economic relationships with people they never see, and yet these relationships still develop. This process of trust in economic relationships has developed over thousands of years, so again, what's the point?

Simon Johnson (MIT Sloan) responded that the point is that the development of blockchain technology is happening around us anyway – the market is pushing in this direction. As a result, recommendations and policy actions should keep pace with these developments, especially as they stand to act as a catalyst to change around the world. He also responded to **Cecchetti**'s question on the future and "What's the killer app?" by noting that transformation in payment systems is proceeding at a rapid pace. For example, the unified payment interface in India is a fundamental transformation which came from reactions to Bitcoin and other systems, while in China Alipay and WeChat are transforming payments, credit and social interactions altogether.

Gary Gensler (MIT Sloan) added further examples. Noting that a venture capitalist could raise much more in the initial coin market than in the venture capital market, ICOs are a prime example of the increasing presence of blockchain. By mid-2017, Blockchain investment itself had channelled more money through ICOs ($6.5 billion) than venture capital ($1 billion). The most disrupted industry in finance currently is the venture capital sector. If ICOs were to reach $30-50 billion in the coming year, this would already be 20-30% of all venture capital worldwide. However, much of this activity concerns valuation arbitrage and is speculative. In particular, utility tokens are often investment schemes. All of this provides further support for consumer and investor protection to keep pace with these market developments.

Centralised versus decentralised debate and transparency

Gensler further agreed that centralisation lowers costs and can lower risk, but at the cost of concentrating risk. As a result, in some cases, trust may be better addressed in a distributed way. In addition, disruptors will act as a catalyst to change the world of finance, in which there are currently many opportunities for economic rents.

Avinash Persaud (Intelligence Capital Limited) noted that when **Gensler** had asked how many in the audience had invested in bitcoin or another cryptocurrency, very few raised their hands – this epitomised that we are in two parallel universes. For those who spent a lot of time managing the global financial crisis, many of the blockchain ideas seem to be in contradiction to what was learned during the crisis. For example, in the case of the Lehman Brothers collapse, part of the issue seemed to be that the OTC bond market was a classic distributed market (not a centralised market). He mentioned the work of Darrell Duffie which documents efficiency gains from netting and centralising clearing across assets, across institutions and across credit. However, risk prevails in a centralised system since there is still a node where the system is vulnerable. He suggested that it would be efficient for central banks, or perhaps someone else, to be a lender of last resort if we can regulate the central clearing house. This stands to be a very efficient way of getting a lot done (central clearing does millions of transactions every second) with a lot of trust. We still miss cost curves that can tell us whether blockchains will be more efficient, more trustworthy and better than what we already have.

Echoing this concern, Cecchetti explained that if we move away from central clearing, we face a new problem, namely, that an individual needs to know about the counterparties, the counterparties' counterparties, and so on. To address this concern, **Neha Narula** (MIT Media Lab) observed that leading

up to the financial crisis, the previous decentralised infrastructure was lacking transparency. New technology provides the ability to improve transparency through public verification, so decentralisation can mean we are all publicly verifying information.

Jonah Crane (FinTech Innovation Lab) advocated keeping an open mind to costs and benefits. A more distributed or shared infrastructure presents the possibility of obtaining some benefits of centralisation while avoiding some of the costs. However, this will involve supervision and regulation, and raises questions related to stress testing at CCPs.

Benoit Coeuré (European Central Bank) remained unconvinced that moving from centralised to decentralised would improve the resilience of the system. He remarked that over the last ten years a key objective of financial regulation has been to shift the financial industry from decentralised to centralised, in particular for clearing. He recalled that the risk being 'thinly spread' in 2006-07 proved destabilising rather than stabilising. Separately, he remarked that the ECB provides an example of open centralised ledgers in finance – its asset-backed security (ABS) loan-level initiative mandates the disclosure of information on assets underlying ABSs as a condition for eligibility as collateral in monetary policy operations. Though this is not a decentralised ledger based on blockchain, it is mandatory public information that has been useful to enhance the transparency of the securitisation market.

Systemic risk and regulation

Michael Burda (Humboldt University) commented on the dismissiveness of systemic risk he interpreted from **Gensler**. He saw risk when traditional means of payment and cryptocurrencies become interconnected. He expressed concern that blockchain-based exchanges can become banks or intermediaries. Who is regulating them?

Gensler agreed that there is risk, but he noted the general consensus among central banks (as stated by Mark Carney at the Financial Stability of Board) that monitoring is sufficient at this stage. He remarked that given the space this $400 billion asset class could be systemically important, especially if there is tax evasion. Technically, one could buy ICOs crypto-to-crypto, completely off the grid of regulators. These exchanges should be regulated around the globe, not just for money laundering but for investor protection. However, while these new systems and infrastructure could destabilise central banks, overall they have the potential to deliver better payment systems.

Robert McCauley (Bank for International Settlements) followed up by asking how organised exchanges could set margins on this new asset class. In response, **Gensler** replied that the CME had posted a 40% margin (approximately) using highly volatile valuation models. In comparison, many of the crypto-exchanges were asking for 2-5% margin. As a result, in the unregulated space, bitcoin can be sold and purchased fifty to one, rather than two to one in the regulated space. This is an example of the opportunities for regulatory arbitrage in valuations (between ICO and venture capital) and in margins (between regulated futures and off-regulation exchanges).

Coeuré commented on potential issues of international coordination and consistency. In Asia, regulators have been much tougher when cracking down on bitcoin exchanges and platforms. On the other hand, when CME started trading bitcoin futures, this development was controversial. It was hailed by some as a step towards stabilising the price of bitcoin, and criticised by others as giving the cryptocurrency space too much. Given that these issues are controversial, how can we ensure that there is enough international cooperation and consistency around these issues?

On the potential destabilisation of central banks by cryptocurrencies, **Jean-Pierre Danthine** (Paris School of Economics) argued that we have learned in the past that good money is centralised money, managed by an independent central institution with a clear mandate. The value added of these new technological developments is not as currencies. If cryptocurrencies are pure bubbles, why do we let them continue? Responding, **Johnson** observed that there had been a monoculture of ideas and institutions across all countries in 2008 which has led the markets to become involved in challenging central banks. Facing this challenge, central banks and regulators may attempt to stifle innovation, but it must be recognised that there is plenty of innovation that is positive and could be guided for better outcomes, jobs and stability. He further questioned the ability of regulators to properly regulate more centralised systems, especially given the single points of failure in centralised systems. To what extent do regulators have visibility into potential systemic risk? Now that alternative methods of clearing and settlement are developing, we will see how they perform in various crises.

Currency or asset?

Focusing on the cryptocurrency application of blockchains, **Angel Ubide** (Goldman Sachs) asked what the role of these new coins is. On one hand, coins are an incentive mechanism that facilitates the working of the system, yet at the same time coins can be used as a medium of exchange or as assets. He suggested more work should be done on the difference between coins and money as we know it, since the traditional role of money is not an incentive mechanism. How would this incentive structure impact the sustainability of the new technology and of coins as currency or assets?

Philipp Hartmann (European Central Bank) referred to the statement by SEC Chair Clayton, cited by the authors, that bitcoin is not a security, but rather a medium of exchange. He suggested that bitcoins could be regarded more as a store of value rather than as a medium of exchange – and not a particularly good one, given their instability and regular use for illicit activities. So, it would be valuable if the report was to scrutinise such conclusions more thoroughly. **Crane** responded that once regulators decide whether tokens are securities, there would be implications on their use as an incentive mechanism. He expressed optimism on tokens and the token economy, as there are benefits of open innovation and interoperability.

Technology uncertainty

On technology, **Coeuré** brought up possible limitations of the widespread application of blockchain. He hypothesised that there might be a trade-off between scalability/performance and safety. Since proof of work on blockchain is slow and costly, inevitably there will be temptation to dilute and weaken the

proof, which could come at the expense of legal certainty. A major concern for financial market infrastructure is whether blockchain can assure settlement finality in the legal sense. The weaker the validation method (e.g., moving from proof of work to proof of stake), the more challenging it would become to assure finality. **Swoboda** added that an immutable ledger in a permissionless system can create challenges for the legal system. **Gensler** agreed that immutable ledgers could create problems. However, inasmuch as there are benefits from such a system, we face economic trade-offs. **Carlo Monticelli** (Council of European Development Bank) asked if tail risks related to blockchain technology warranted consideration – especially since this technology could have such a pervasive implication on finance and everyday payment systems.

Narula addressed the scepticism about the technology and discussed how to reconcile this scepticism with the hope and hype trade-off. She argued that the issue is not what the problems with the technology are today, rather, the question should be what are the problems that are fundamental, and what are the problems that are fixable? Once they are fixed, what is the potential for a better (more efficient) technology? For instance, it is sometimes thought that blockchain technology might not work in finance if everything is public. However, there are cases where privacy can be established. Scalability is also developing. On the concern that the underlying cryptography could break, she remarked that this already occurs within existing financial systems – this fear applies to both blockchain and non-blockchain technology. She recognised that cryptocurrencies are resource intensive, but it is possible to develop other mechanism of consensus and to move away from such high energy use. She echoed scientist Roy Amara's view that a space can be over-hyped and under-hyped at the same time. We tend to overestimate some effects in the short term and to underestimate them in the long term

Ubide stated that 1% of bitcoin holders hold 80% of bitcoins. He thought that it was the opposite of what was expected – a decentralised system should lead to the democratisation of finance, but it was leading to the opposite. Furthermore, proof of stake may lead to more concentration. He asked whether the technology was creating the seeds of its own demise. **Johnson** agreed that bitcoin has become quite centralised and that the vision of decentralisation has not been realised in mining or ownership. However, there are a lot of cryptocurrencies competing among themselves. He viewed this level of competition as healthy, though is unsure of which player would prevail.

Katrin Assenmacher (European Central Bank) observed that the report focuses on centralised blockchains. However, with decentralisation, as the system relies on participation of a broad range of people who contribute to proof of work, how does the system continue to incentivise? With bitcoin there are mining fees, but a lot of computing power is in China. What happens if there is monopolisation of participation on decentralised exchanges? **Narula** noted that the focus tends to be on the miners and the users of cryptocurrency. However, a third class – called the full nodes – are often left out of the discussion. Full nodes consist of people that are running software, completing public verification but not actually mining. There are intricate dynamics between miners, public verification and the actual holders of cryptocurrencies.

Applications

Hartmann suggested that focusing on the applications of blockchain technology – the ends and not the means – will reduce the hype. For example, the assessment of the technology is likely to be very different for different applications. Moreover, he observed that many of the current applications seem to be in areas previously governed by mutualist structures, for example in settlement. He asked whether this means that the technology would remove mutualist structures, or whether such governance would be preserved. He also expressed the view that within the spectrums of centralised versus decentralised applications, or permissionless versus permissioned systems, mixed models could well prove to be the most valuable. **Johnson** was uncertain which application would prevail. High competition is a benefit for payments and when looking for a programmable language on which applications can be built.

Crane explained another benefit of the technology. Blockchain applications act as a catalyst and push to rearchitect outdated systems. For example, Ripple has developed a blockchain solution to rival SWIFT. In turn, SWIFT has been incentivised to explore its own blockchain-based solution to streamline settlement process systems. If incumbents manage to narrow the gap between what disruptors are offering and their own solutions, then existing relationships that are already not trusted may not change much. Additionally, most financial institutions are working on these problems through consortiums. It seems unlikely that disruptors will completely replace the financial market infrastructure, yet new technology will bring existing institutions to a new and more efficient technology platform. An example of modernising old infrastructure is the Australian Stock Exchange, exemplified in the report. Crane also insisted that blockchain technology is a tool, so the question really is whether it is the most appropriate tool to solve a particular problem, consistent with investor protection, and safety and soundness with respect to financial stability.

Cecchetti encouraged the authors to think about the economic problems that the systems in place are solving, and how new systems could improve upon them. For example, there is a move to implement instantaneous clearing of securities, which could be a fool's errand. Real-time gross settlement may be great for wholesale payment systems, but not for security settlement, as it would require huge inventories of securities and cash sitting idle. Netting is far more efficient and cheaper. The down side is counterparty risk. However, such risk can be managed with margining practices and other institutional arrangements we already have in place. The point is that we need to start by understanding the economic problems being solved by the current framework, and then ask whether a new system can solve these problems more cheaply.

Narula explained that permissionless cryptocurrencies and protocols were important for standardisation and interoperability. The internet was developed thanks to developments in universities and government labs; the protocols were not owned by a single company. This example illustrates that open protocols are important for creating the next set of applications. On the application of new technology for the financial systems, she remarked that building software to make payments, take money and create value is arduous and difficult. If innovations and disruptors push incumbents and make innovation faster and more effective, then there are benefits from these developments.

Chair conclusions

Summarising the discussion, **Maechler** concluded that there is great potential for transformation and disruption. A lot of work needs to be done to prove that the technology can work and to develop more compelling use cases. It may not only be blockchain, but ultimately big data, machine learning and the combination of these digital innovations that could be disruptive. Then, the question is how broad the application and impact of the technology will be and where it fits in the financial system. Comparing the merits of centralised and decentralised systems, the debate suggests that the best systems may lie somewhere along the spectrum, and that we are currently hovering around permissioned blockchains. This discussion matters for policy. If there are concerns, ultimately we need to build trust, and for that we need an adequate policy framework. This will have to bring together disruptors and incumbents, as well as regulators and central banks.

References

ASX (2018), "CHESS Replacement: New Scope and Implementation Plan", Consultation Paper, April.

Azaria, A., A. Ekblaw, T. Vieira and A. Lippman (2016), "Medrec: Using blockchain for medical data access and permission management", presentation at the 2nd International Conference on Open and Big Data (OBD), 22-24 August.

Batiz-Benet, J., M. Santori and J. Clayburgh (2017), "The SAFT Project: Toward a Compliant Token Sale Framework", SAFT Project White Paper, Cooley.

Carney, M. (2018), "The Future of Money", speech to the inaugural Scottish Economics Conference, 2 March.

Casey, M.J. and P. Vigna (2018a), "In Blockchain We Trust," *MIT Technology Review*, 9 April.

Casey, M.J. and P. Vigna (2018b), *The Trust Machine: The Blockchain and the Future of Everything*, St. Martin's Press.

Catalini, C. and J. Gans (2018), "Initial Coin Offerings and the Value of Crypto Tokens", MIT Sloan Research Paper No. 5347-18.

CB Insights (2017), *Venture Capital Funding Report 2017*, New York.

Cecchetti, S G and K L Schoenholtz (2017a), "Modernizing the U.S. Payments System: Faster, Cheaper, and More Secure," www.moneyandbanking.com, 31 July.

Cecchetti, S G and K L Schoenholtz (2017b), "Managing Risk and Complexity: Legal Entity Identifier," www.moneyandbanking.com, 30 October.

Coase, R.H. (1957), "The Nature of the Firm," *Economica* 4(16).

Depository Trust and Clearing Corporation (2018), *Modernizing the U.S. Equity Markets Post-Trade Infrastructure*, January.

Dwyer, G.P. Jr., (2017), "Blockchain: A Primer", in B.E. Gup (ed.), *The Most Important Concepts in Finance*, Edward Elgar Publishing, pp. 12-27.

Financial Stability Board (2018), "To G20 Finance Ministers and Central Bank Governors", 13 March.

Gandal, N. J.T. Hamrick, T. Moore and T. Oberman (2017) "Price Manipulation in the Bitcoin Ecosystem", CEPR Discussion Paper No. 12061.

Haeringer, G. and H. Halaburda (2018), "Bitcoin: A Revolution?", unpublished manuscript, 6 March.

Hong Kong Monetary Authority (HKMA) (2017), "Whitepaper 2.0 on Distributed Ledger Technology", 15 October.

IOSCO (2018), "IOSCO Board Communication on Concerns Related to Initial Coin Offerings (ICOs)", Media Release, 18 January 18.

Juniper Research (2017), "Blockchain Enterprise Survey August 2017".

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

Meiklejohn, S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker and S. Savage (2013), "A fistful of bitcoins: characterizing payments among men with no names", Proceedings of the 2013 Internet Measurement Conference, Association for Computing Machinery.

Nakamoto, S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", 31 October.

Narula, N., W. Vasquez, and M. Virza (2018), "zkLedger: Privacy-Preserving Auditing for Distributed Ledgers", 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), USENIX Association.

Pease, M., R. Shostak, and L. Lamport (1980), "Reaching agreement in the presence of faults", *Journal of the ACM* 27(2): 228-234.

Rosenbush, S. (2018), "The Morning Download: CIOs Say Blockchain Adoption Barely Registers," *The Wall Street Journal*, 7 May.

Vargas, F., J. Dasari and M. Vargas (2015), "Understanding Crowdfunding: The SEC's New Crowdfunding Rules and the Universe of Public Fund-raising", *Business Law Today*, December.

Walter, E. (2011), "The Interrelationship Between Public and Private Securities Enforcement", Harvard Law School Forum on Corporate Governance & Financial Regulation, 11 December.

WTO (2016), *Trade Finance and SMEs*, Geneva.

Zhang, J.Y (2017), "The Rise of Market Concentration and Rent Seeking in the Financial Sector", John M. Olin Center for Law, Economics, and Business Fellows' Discussion Paper Series.

Blockchain technology has the potential to change many aspects of the financial services sector and the broader economy – by providing new ways to intermediate capital and risk, and by being a catalyst for change to incumbent financial sector firms. There are currently significant issues to be resolved, but with thousands of developers worldwide working on open-source projects that aim to improve blockchain protocols and applications, there is reason to be optimistic that the technology will become easier and safer to use.

Numerous companies and financial market utilities are trying proofs-of-concept or pilots, but none (to date) has applied blockchain technology to core business processes. Given that this technology's strength depends in part on multiple organisations using the same network, a structure that requires coordination among many parties, the path to incremental adoption is not clear.

In addition, blockchain projects need to be brought more fully within existing public policy frameworks. Rules that establish fair and efficient markets – and that protect investors – are just as important for blockchain-based decentralised financial products as for more established dimensions of finance. Also important and highly relevant are the policy goals of ensuring financial stability and guarding against tax evasion, money laundering, and terrorism finance.

The 21st Geneva Report on the World Economy first provides a summary review of the basics of blockchain technology and its challenges, costs, and benefits. It then gives an overview of blockchain technology and the potential direct impact on the financial sector, including a discussion of tokens, initial coin offerings (ICOs), and crypto-exchanges – all salient regulatory and market issues today. Building on this, it assesses possible use cases beyond the world of finance.

ISBN: 978-1-912179-15-2

Centre for Economic Policy Research
33 Great Sutton Street • LONDON EC1V 0DX • UK
TEL: +44 (0)20 7183 8801 • FAX: +44 (0)20 7183 8820 • EMAIL: CEPR@CEPR.ORG
WWW.CEPR.ORG

ISBN 978-1-912179-15-2
9 781912 179152 >