Distributed Ledger Technology / Blockchain: Perspectives

CPA
CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

Institute for Management & Innovation
UNIVERSITY OF TORONTO
MISSISSAUGA

DISCLAIMER

This paper was published by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance. The views and opinions expressed in this paper are those of the authors and do not necessarily reflect those of CPA Canada.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

Foreword

Distributed ledgers and blockchain are powerful and challenging technologies for business and accounting. They are powerful because of their potential to create new social and economic models much like the new business models enabled by Internet technology; they are challenging because of their complexity and our lack of understanding.

To reduce the mystery and to highlight the power of these technologies, CPA Canada is pleased to present this publication on the *Distributed Ledger Technology / Blockchain: Technology, Governance and Social Innovation* conference in collaboration with an important academic stakeholder, the Master of Management & Professional Accounting (MMPA) Program at the Institute for Management & Innovation, University of Toronto.

The conference papers gathered here complement CPA Canada's existing guidance publications on cryptocurrency and blockchain.[1] As thought papers, they introduce the *possibilities, limitations, and disruption* the technologies present and open readers' eyes to new ways of becoming involved.

In this volume, thought leaders:

- in **technology** start us with primers on blockchain, cryptocurrencies, and distributed ledgers and take us to real-life-use cases of blockchains and "smart contracts" in action
- in **governance** show us tension and co-operation between innovators, regulators, and tax authorities
- in **social innovation** introduce us to another dimension – the use of blockchain in sustainability reporting, an area in which accountants have played a key role[2]

Where there are ledgers, there are accountants or the potential for accountants. Fraud detection, verification of ownership in transactions, decision rules embedded in smart contracts, and many other areas could benefit from accountants' traditional training, judgment and professional skepticism. We learn that smart contracts – with their ingredients of contract law, computer code, ethics, etc. – require an interdisciplinary approach and have the potential to automate many elements of business transactions.

[1] See CPA Canada, *CPA perspectives on blockchain* (www.cpacanada.ca/blockchain).

[2] See CPA Canada, *Sustainability, environmental and social reporting resources* (www.cpacanada.ca/en/business-and-accounting-resources/financial-and-non-financial-reporting/sustainability-environmental-and-social-reporting).

This conference brought cross-industry views together and showed us how the lines of “disciplines” can be blurred. It is a timely adjunct to CPA Canada’s *The Way Forward*[3] report that presents insights from CPA Canada Foresight: Reimagining the Profession*,* a multi-stakeholder consultation exploring how drivers of change will impact the future of the accounting profession. In responding to the exponential change around us, *The Way Forward* cautions that we can let innovation happen around us or be agile enough to be a part of it. We can develop new skills and competencies beyond our traditional ones or be left behind. We can show adaptability or lose our relevance. All the while, we must remain stewards of the public trust and place ethics at the forefront as we explore these new technologies.

This collection of papers shows that while everyone has a potential stake in blockchain – not just the technologists – our inclusion is not a given; it must be proactively seized. Accounting professionals, business leaders, technologists, lawyers, educators, and others will learn about collaborative possibilities from this publication and about new academic areas that will enable multiple disciplines to develop new value-creation models on new frontiers.

On behalf of CPA Canada, we invite you to read on and join the conversation.

Michael Wong, CPA, CA
Principal
Research, Guidance and Support
277 Wellington Street West
Toronto ON M5V 3H2
michaelwong@cpacanada.ca

Davinder Valeri, CPA, CA
Director
Research, Guidance and Support
277 Wellington Street West
Toronto ON M5V 3H2
dvaleri@cpacanada.ca

[3] See CPA Canada, *Foresight Report: The Way Forward: Transforming Insights Into Action* (www.cpacanada.ca/foresight-report/en/index.html, [2019]).

Table of Contents

GOVERNANCE PILLAR

SOCIAL INNOVATION PILLAR

Distributed Ledger Technology / Blockchain: Technology, Governance and Social Innovation – an Introduction

By Irene M. Wiecek, Professor of Accounting, Teaching Stream, University of Toronto

Bitcoin (a crypto-asset) and its underlying blockchain technology (a form of distributed ledger technology) keep resurfacing, sometimes in a positive way because of their unique architecture and the applications blockchain has inspired, and sometimes in a not-so-positive way. For example, new instruments can have new problems (the disappearance of $260M in bitcoin from Quadriga[4] because encryption keys were lost when the founder died) and sometimes the same old ones (what started as lost encryption keys may have ended in fraud).

Wearing both my CPA and academic hats, I have been intrigued with this area for the last two years. Most of my accounting colleagues at the University of Toronto initially seemed to shy away, especially from the crypto-asset area. Given the high profile frauds and lack of (or low level of) regulation in the cryptocurrency exchanges, this did not surprise me. I have heard the crypto-asset world being referred to as the "wild west" more times than I can count. On the other hand, many of my colleagues, especially in economics, finance, strategy and organizational behaviour were intrigued by the distributed ledger technology itself and the possibilities for adding value. They were also interested in how organizations and people respond to the changes the technologies present.

With these ideas in mind, the University of Toronto organized a one-day conference on November 16, 2018, entitled "Distributed Ledger Technology / Blockchain: Technology, Governance, and Social Innovation." As part of the Institute for Management & Innovation (a multi-disciplinary Institute at the university), our goal was to examine these developments from these three different perspectives (the technology, governance and social innovation pillars). The audience included faculty members, students and members of industry and the accounting profession. We greatly appreciate the support of CPA Canada and the CPA / Rotman Centre for Innovation in Accounting Education and enjoy working together to tackle these challenges as they emerge.

[4] Doug Alexander, *Quadriga Crypto Mystery Deepens With 'Cold Wallets' Found Empty* (www.bloomberg.com/news/articles/2019-03-01/quadriga-has-6-cold-wallets-but-they-don-t-hold-any-crypto, March 1, 2019).

Originally structured around the three pillars, the day soon showed that the *pillars* might have been called inter-related *supports* because of the transdisciplinary nature of most of the presentations of the eight speaker and the three moderated panel discussions (one for each pillar) where the audience was given a chance to ask questions (some of which have been captured in this publication). The panels were moderated by Professors Yue Li and Soo Min Toh as well as myself. Our goal was to challenge everyone to be open to, yet critically analytical of, the ideas presented and issues raised.

Below, I have noted some highlights and insights from that fascinating day.

The technology pillar

Analyzing the impact of blockchain on the world of accounting is a challenge if a person does not understand the underlying technology. Our first and foremost challenge was to bring the technology alive for our audience so that everyone could begin to really think about its impact in a meaningful way.

Three speakers from academia and industry presented different layers of the technology. Garrick Hileman talked about the profound influence this technology will have on our world as part of a set of broader changes, including artificial intelligence and a move toward more peer-to-peer interactions. This fitting introduction reminded us that we are in a time of significant technological change of which blockchain is just one part. In addition, he opened our eyes to the game-changing nature of the technology and the implications of moving to a more decentralized (i.e., away from intermediaries) world, where trust is minimized and where blockchain replaces the handshake – the traditional gesture representing trust and co-operation – with computer code.

Many people have concerns about moving to a distributed ledger platform, but Peter Patterson reminded us that existing platforms and business processes are not perfect either. For instance, take supply chain management as an example. Because of inefficiencies, multiplication of effort in paperwork, individual ledgers, and contract disputes, there are many problems. In addition, individual companies such as banks, house a lot of information centrally, making their information systems vulnerable to attack.[5] Peter compared and contrasted permissionless, anonymous blockchains (e.g., Bitcoin) to the private, permissioned blockchains for business networks. Both have their advantages and disadvantages. Blockchain architecture allows network participants to share a ledger on which transactions are secure, authenticated and verifiable, where disputes are more easily reconciled and therefore efficiency gains can be huge.

[5] Many experts in the cyber-security field caution that it is not *if* you get attacked but *when*.

Andreas Veneris discussed the breakthroughs that Bitcoin and Ethereum represent from a computer science viewpoint. He introduced us to methods for addressing their key challenges, such as increasing transaction volume and transaction speed (extremely slow compared to systems such as VISA and PayPal), while reducing their enormous energy consumption. As with all emerging technologies, hurdles exist, but they are not insurmountable. The technologies are continuously evolving and changing.

Andreas also introduced us to crypto-economics, an emerging field of research. In the panel discussion, Andreas emphasized that a smart contract has significant legal, even philosophical, implications, and finance, law, computer science, management, and accounting are fields that merge in blockchain technology.[6] This makes the topic truly transdisciplinary.

The governance pillar

Secondly, we wanted to highlight the regulation issue (or lack thereof). As accountants, we live in a much-regulated environment where entities and individuals are governed by regulations and laws such as securities acts, tax acts, bank acts, anti-money laundering acts, and many more. Laws and regulation play a big part in our capital markets and more broadly, in our society. In our capital markets, they help with efficient and effective resource allocation, protect investors, lower risk and increase stability of the financial system. In our society, they ensure at least a systematic approach to sharing much of the cost of running our governments (through the taxation system),[7] help protect our economy, and keep our standard of living high.

This section of the day included presentations by a securities regulator, the auditors' auditor and a tax practitioner.

The governance pillar:

- explored concerns about whether our current systems are ready to deal with distributed ledger technologies and crypto-assets – or not
- addressed issues encountered in trying to keep up with the technologies
- outlined steps already taken

Pat Chaukos talked positively about technology as a disruptive force that will help create new business models and add value in the economy if properly supported.

[6] Andreas Veneris was recently awarded $250K for the creation of the UTLedgerHub for studying crypto-economic blockchain technology. It will bring together researchers from business, computer science, engineering, global affairs (policy/regulation), law, economics, and social justice. For more information, see *U of T Engineering Blockchain Project Receives Funding Injection from Connaught Fund* (https://startupheretoronto.com/partners/uoft/u-of-t-engineering-blockchain-project-receives-funding-injection-from-connaught-fund, July 20, 2018).

[7] In Ontario, according to the audited financial statements for the 2017-2018 year, 66% of the government's revenue came from taxes (excluding transfer payments from the government of Canada, which are likely partially sourced from federal taxes). See Ontario Treasury Board Secretariat, *Public Accounts of Ontario: Public Accounts of Ontario Annual Report and Consolidated Financial Statements 2017–2018* (https://files.ontario.ca/pa18_annualreport_cfs_en.pdf, 2018), p. 12.

Pat and Carol Paradine discussed the need to protect investors yet encourage innovation.[8] Pat noted that the Ontario Securities Commission (OSC) has proactively taken steps to get involved early by creating and being involved with experimental "regulatory sandboxes" to help innovators navigate securities regulation.[9]

Carol referred to a "blockchain-enabled world" as a new frontier and noted that there are over 50 public companies in Canada already working in this new world. She noted that while there is not a lot of guidance for auditors in this area, there were some very challenging issues. Who, for example, has examined the effectiveness of internal controls of crypto-exchanges? She cautioned that auditors' professional skepticism would not be replaced by machines any time soon.

Laura Gheorghiu commented that many feel bitcoin and other crypto-assets are outside our current regulatory systems, including the law and taxation. She affirmed that this is not the case. Crypto-assets are a challenge, since they do not fit neatly into our current regulatory environments. Although the Canada Revenue Agency (CRA) recently issued guidance on digital currency,[10] the number of different kinds of cryptocurrencies and applications of blockchain has burgeoned. As a result, the CRA is playing catch up. Laura sees promise in the underlying technology, noting that ironically blockchains could actually help the CRA collect taxes.

All the speakers stressed the need to modernize current regulation and that many regulatory bodies are already hotly debating issues surrounding crypto-assets and their related technologies.

As an aside, accounting-standard setters are similarly looking to provide some structure among accounting principles. The IFRS® Discussion Group (a subcommittee of Canada's Accounting Standards Board [AcSB])[11] has had numerous discussions relating to cryptocurrencies.[12] The IFRS® Foundation is also dealing with these topics on a project basis.[13, 14]

With all of these types of innovation, accounting-standard setters have two challenges:

[8] In the technology panel discussion, Andreas Veneris said that the biggest problem for distributed ledger technology adoption may be regulation. While many feel that regulation stifles innovation, deregulation is often considered one of the ingredients of the 2008 financial crisis. Garrick Hileman and Andreas Veneris talked about how blockchain technologies could prevent fraud through real-time visibility of assets on the balance sheet and enhance levels of transparency that were missing in 2008 and are still missing today.

[9] Ontario Securities Commission, *OSC LaunchPad: Navigating Securities Regulation* (www.osc.gov.on.ca/en/navigating-regulation.htm, 2019). The OSC is also involved on a national and international level with other regulatory bodies to help Ontarian fintech do business globally.

[10] Canada Revenue Agency (CRA). *Virtual Currency.* (www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency.html, June 26, 2019).

[11] AcSB, *IFRS® Discussion Group* (www.frascanada.ca/en/acsb/committees/ifrsdg).

[12] Past IFRS® Discussion Group meeting topics are searchable at www.frascanada.ca/en/acsb/committees/ifrsdg/search-past-topics.

[13] IFRS, *Holdings of Cryptocurrencies* (www.ifrs.org/projects/2019/holdings-of-cryptocurrencies, June 2019).

[14] IFRS, *The IFRS Foundation Technology Initiative* (www.ifrs.org/news-and-events/2018/11/the-ifrs-foundation-technology-initiative, November 2018).

- understanding the underlying technology / innovation
- determining how existing accounting standards apply

Because many standards were developed before these technologies even existed, applying them to new technologies might feel a bit like trying to fit a square peg into a round hole. Within IFRS, crypto-assets would most likely be categorized as inventory if they are held for sale in the ordinary course of business. However, in the view of many, if crypto-assets are *not* held for sale in the ordinary course of business, they would meet the definition of an intangible asset.

Garrick noted that crypto-assets make us question many things we take for granted, for example, what exactly money is. I found myself doing the same. We have already moved past the point where most of the money we use has physical form as most of us carry credit or debit cards (or use our phones to pay for things). It is digitized. So why is a crypto-asset so foreign to us? There are more similarities between money (as we have come to understand its use in our daily lives) and crypto-assets than not.

Andreas talked about how the technical complexity and cross-border character of blockchain technologies are creating unprecedented challenges for lawmakers, regulators, and tax authorities. He insightfully noted that people in the blockchain world may not even speak the same "language" as those in the regulatory world because the blockchain terminology is so unfamiliar.

Carol talked about auditor collaboration with machines, which keep getting smarter, and joint audits with both humans and machines – something quite different from a joint audit with another auditing firm.

The social innovation pillar

Thirdly, we wanted to view the issues from the human side. Can blockchains be used for social good? What are the possibilities in terms of improving the way we live in general; for instance, in ensuring food safety, monitoring environmental compliance, and removing supply chain inefficiencies?

Two speakers, one from a financial institution and the other from the blockchain industry, talked about the social innovations that distributed ledger technologies could offer. Michael Torrance talked about the technology being socially revolutionary because it allows for the disintermediation and decentralization of formerly highly centralized processes. He feels the potential to advance sustainability is significant. The tracking of corporate reputation is also a possibility.

Marc Lijour gave us a survey of blockchain innovations that showcased real-world socially innovative blockchain applications and experiments for financial services (e.g., benefiting the bankless by providing alternatives to centralized financial services), social good (e.g., benefiting people in war zones or disaster areas by mobilizing help, and by providing early warning systems, and asset documentation), and the environment (e.g., by incentivizing cleanup efforts). Marc, Michael, Garrick, and Peter all spoke about blockchain applications that track products for consumers (e.g., cheese, wine, diamonds, fish, etc.) to ensure veracity, provenance, proper treatment, and sometimes safety.

How do we effect change and acceptance of new technologies? What about the trust factor? Can we trust computer code instead of humans? Garrick talked about blockchain "replacing the handshake." Do we feel comfortable with this? Most speakers throughout the day identified and addressed barriers and hurdles that we all face in embracing change.

The rest of this publication provides condensed versions of the presentations by pillar.

Given the speakers' differing perspectives, we heard many different views. That was the beauty of the day for us because those perspectives sparked discussion and debate while providing a deeper understanding. Something Peter said resonates here: blockchain technologies have the potential to *exchange different forms of value* in a *cross-industry* network; non-traditional partners can collaborate to innovate, build new value propositions, optimize costs, risks, and capital, by using digital platforms and marketplaces.

These types of discussion come at a good time for the accounting profession. The profession is having to rethink its future in the face of so much change, much of it driven by technology.[15] As accountants, many of us are coming to realize that crypto-assets and distributed ledger technology are innovations we need to examine more closely because they are here to stay in one form or another.

The technology affords opportunities for creating new ecosystems, new business models, new market mechanisms, and new ways to track and measure things that are important. It also challenges the *status quo* and many of our fundamental beliefs. Where will these new technologies take us?

[15] CPA Canada established a working group to examine where we are as a profession and where we might be headed. Scenario planning was used to develop four possible futures allowing platforms for rethinking where we might be in the future. See CPA Canada, *Foresight Report: The Way Forward: Transforming Insights Into Action* (www.cpacanada.ca/foresight-report/en/index.html, [2019]).

Keynote Speech: Blockchain Technology – Past, Present and Future

By Garrick Hileman, head of research at Blockchain.com and researcher at the London School of Economics

Introduction

In 2018, Mark Carney, Governor of the Bank of England said, "The economy is reorganizing into a series of distributed peer-to-peer connections across powerful networks … revolutionizing how [people] consume, work, and communicate."[16]

Although not directed specifically at blockchain, Carney's comments place blockchain not in a silo but in the context of bigger changes in automation, robotics, artificial intelligence, peer-to-peer economic activity, digitization of economic activity, and so on. Leaders like Mark Carney recognize that these changes can have a profound influence on our world.

Differences between blockchain and the traditional financial system

Blockchain systems and our traditional financial system have important differences, and this is one of the most fundamental: traditional assets (e.g., cash, bonds, and stocks) are distinct and separate from the networks and ledgers on which they are traded, transferred, and recorded. So think of cash, stocks, and bonds as **train cars**, and think of VISA, PayPal, Swift, and stock exchange networks as **train rails**.

Cash can be moved onto VISA's "rails," and then picked up and transferred to PayPal's "rails." In effect, the train car can be moved onto a different set of train tracks. That action is *not possible* with a blockchain system. Bitcoin, for example, cannot be moved off its blockchain, because it is *locked* to it. Bitcoin the asset is locked to its rails and cannot be transferred from one set of payment tracks to another. The *integrated nature of the system* is the design characteristic that marks a key difference between a blockchain-based system and the traditional financial system.

[16] Mark Carney, *Speech: New Economy, New Finance, New Bank* (www.bankofengland.co.uk/-/media/boe/files/speech/2018/new-economy-new-finance-new-bank-speech-by-mark-carney, June 21, 2018).

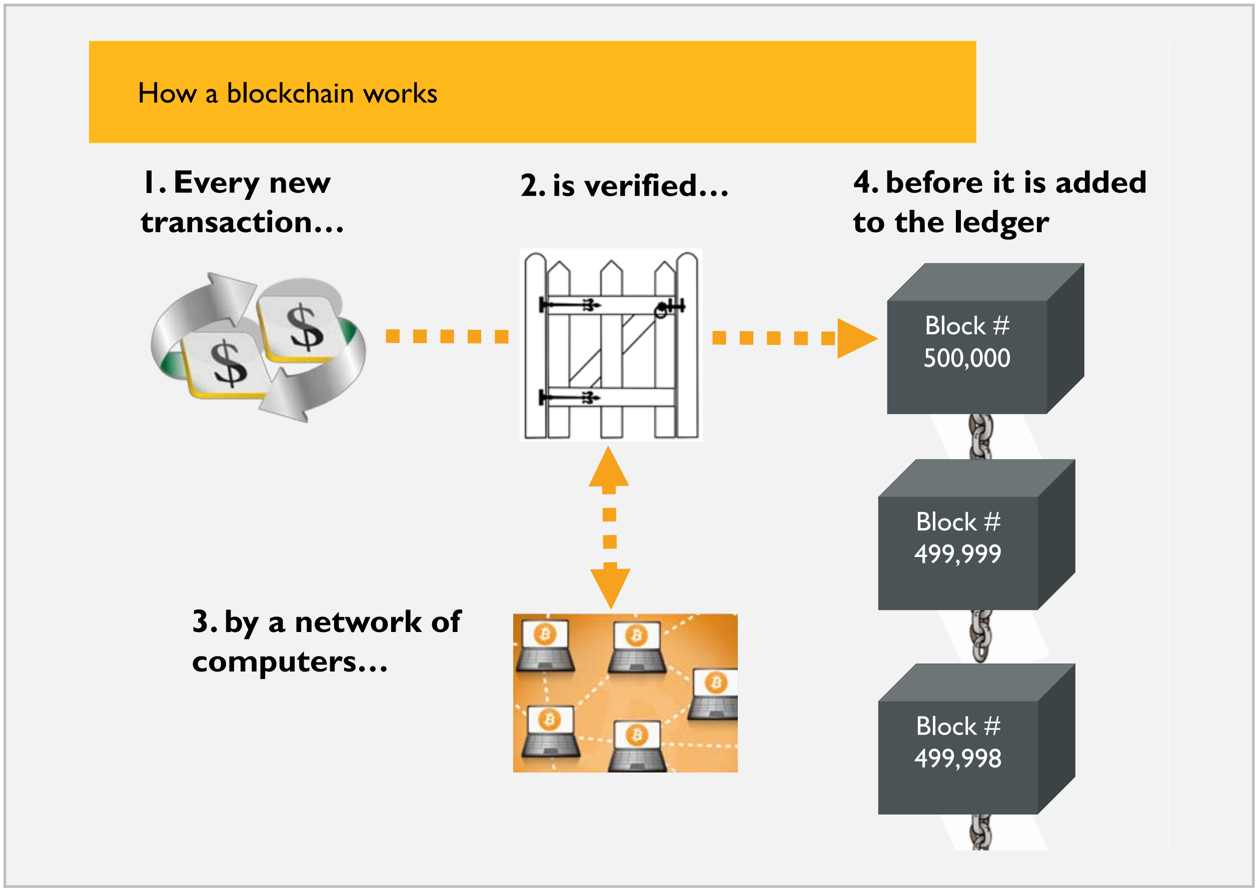
How a blockchain works

For those who have not actually used a cryptocurrency, it can resemble email. Using Bitcoin as an example, the same five things are needed to use email as to use the Bitcoin blockchain, for example:

- the internet
- a computer application (i.e., a browser or email client; a "wallet" with bitcoin)
- addresses to send and receive
- content (i.e., a subject line and message in email; how much will be sent with bitcoin)
- a password (to access email; a private key to spend bitcoin)

Sending bitcoin between people or companies through a blockchain works like this (Figure 1):

FIGURE 1: HOW A BLOCKCHAIN WORKS


How a blockchain works
1. Every new transaction...
2. is verified...
3. by a network of computers...
4. before it is added to the ledger
Block # 500,000
Block # 499,999
Block # 499,998

Before the intended recipient gets the bitcoin, the transaction must be verified by a network of computers that act as a gate. They check to see whether the sender a) actually has the bitcoin being sent; and b) is not "double spending" (i.e., sending the same coin to someone else at the same time). If the transaction is valid, the network of computers lets the transaction pass through the gate and be added to what is called a "block."

The **block**, in the case of Bitcoin, is simply a bundle of transactions – a few thousand on average – that are bundled together every 10 minutes and "appended" (i.e., cryptographically chained) to the previous bundle of transactions. In Figure 1, Block #499,999 is appended to Block #499,998, the prior set of transactions from 20 minutes earlier, and so on, and so on, all the way back to the first block created in January 2009, when Satoshi Nakamoto started running the Bitcoin blockchain software. Satoshi Nakamoto's blockchain invention is as much an economic advance as it is a computer science advance.

Miners are the computers powering the network. Incentives are in place so that these computers are both *competing* with and *co-operating* with each other at the same time: co-operating to maintain the network, but also competing to be the first computer to *mine* (i.e., solve a complex problem that allows them to form and be rewarded for) a new block.

The blocks, replicated on multiple computers, collectively represent the history (i.e., the **distributed ledger** of all the transactions that have occurred on the Bitcoin network cryptographically linked together). This recordkeeping provides security and integrity to the system.

One of the most remarkable things about the Bitcoin blockchain is that it has not suffered *any* down time in its 10 years of operation. This is the most powerful computer network assembled in history. It is massive, consuming as much electricity (many people think) as a small country, yet it *has never* "gone down."[17] So organizations that run critical infrastructure (e.g., transportation systems, energy systems, payment systems, central banks) think blockchains and distributed ledger technology (DLT) have something to offer because they are so resilient.

Five key components of a blockchain

Structurally, all blockchains have these five things:

1. cryptography
2. peer-to-peer network: distributed computers connecting and talking with each other
3. consensus mechanism: a way by which those computers can all agree

[17] Koomey, Jonathan, Estimating Bitcoin Electricity Use: A Beginner's Guide (https://coincenter.org/entry/bitcoin-electricity, 2019).

4. ledger: a record of transactions
5. validity rules: rules about which transactions are valid and which are invalid

Using a blockchain may help in many ways, for example, to:

1. reduce the need for trust between stakeholders, particularly between adversaries, thus creating a **trust-minimized** system
2. build secure transfer systems
3. streamline business processes across multiple entities
4. increase transparency and the ease of auditability using a distributed ledger (e.g., by providing real-time visibility in transactions)

Myths about blockchain

Many myths exist around blockchain. For example,

Myth 1: Blockchains are "trustless."

Reality: Blockchains always require trust and, if nothing else, require trust in the cryptography that underpins blockchains. The cryptography underpinning Bitcoin, for example, has never been mathematically proven to be secure. It *seems* secure because it has not yet been cracked.

Myth 2: Blockchains are tamper-proof or "immutable."

Reality: They are *tamper-resistant*, but they are not tamper-proof. They can be reversed by network participants (**community**) under certain circumstances. In the case of Ethereum, for example, the community of a big decentralized autonomous organization (DAO),[18] came together a couple of years ago and decided to rewrite history to undo a hack that had siphoned off funds. The community basically rewrote history to give that money back to the people who had given the money to the DAO. The blockchain was not immutable: history was *changed*.[19]

Myth 3: Blockchains are 100% secure.

Reality: Bitcoin's structure, for example, as a proof-of-work system, has an inherent vulnerability called a "51% attack," which occurs when more than 50% of the computer power in the network do things such as double-spend coins or rewrite history. This happened in 2018 to Bitcoin Gold – a fork[20] of Bitcoin – when an attacker deposited some Bitcoin Gold on an

[18] Editor's note: For more information on DAOs, see the Veneris and Berryhill paper also in this volume.

[19] David Siegel, *Understanding The DAO Attack* (www.coindesk.com/understanding-dao-hack-journalists, June 25, 2016).

[20] Editor's note: For more information on forks, see the Veneris and Berryhill paper also in this volume.

exchange, converted it to bitcoin, withdrew the bitcoin, and then reversed history to show that that the transfer of Bitcoin Gold to the exchange had never happened – an $18 million dollar theft.[21]

Myth 4: Blockchains are truth machines.

Reality: the same principle applies to blockchains used to input external data as to any other database: garbage in, garbage out.

Use cases: smart contracts

Smart contracts are code (i.e., a software application) that lives on a blockchain and verifies when conditions of contracts are fulfilled then transfers funds between the contracting parties.

An example of an application of smart contracts with potential wide applicability is for travel insurance. When a flight is cancelled or delayed, travellers are entitled to reimbursement. However, in the UK during a single year, about 600,000 travellers annually that were eligible to collect insurance did not do so. Since flight delays and cancellations are public information, a smart contract could check a database to see whether the flight is delayed or canceled. After verification, the smart contract could reimburse eligible travellers automatically without requiring any further steps or claims process from the insured party. An important feature of the smart contract is that the insurance company *would not hold or control the insurance funds*. The funds would be on the blockchain, sitting in the smart contract between the traveller and the insurance company.

A traveller's ability to fully collateralize insurance in a smart contract on a blockchain, where the insurance company does not have access to it, could prevent companies running off with the money in certain markets where institutions are not well regulated or capitalized. This is an example, again, of *trust minimization*: reducing the need for trust between the parties, escrowing funds in a smart contract, and keeping the funds visible and only releasable after a certain set of rules has been executed.

Key inhibitors of corporate DLT adoption

Given that corporate distributed ledger technology has been hyped for over three years, why is there little progress and DLT adoption in banks and other traditional institutions?

For banks and other institutions participating in the *Global Blockchain Benchmarking Study*,[22] the top three barriers to adoption are:

[21] Jeff John Roberts, "Bitcoin Spinoff Hacked in Rare '51% Attack,'" *Fortune* (http://fortune.com/2018/05/29/bitcoin-gold-hack, May 29, 2018).

[22] Hileman, Garrick, and Michel Rauchs, *Global Blockchain Benchmarking Study* (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224, 2017).

1. Legal risk and regulatory uncertainty: European regulators have come under heavy pressure from the DLT industry to create regulatory certainty, yet they are reluctant to create new regulations for uncertain uses of the technology.
2. Confidentiality: Given that a blockchain is a network of computers storing data, legal problems might arise if customer data – even if encrypted – sits on a competitor's computer.
3. Reluctance to change established business practices (a classic IT problem).

HOW CAN THE BLOCKCHAIN CONCEPT BE IMPLEMENTED IN A SOCIETY THAT IS BASED ON CENTRALIZATION?

GARRICK HILEMAN: Blockchain doesn't make natural sense for many hierarchical centralized organizations to implement. Satoshi Nakamoto, creator of Bitcoin, was a "nobody." He needed a technology that established credibility and trust: a blockchain. Many central banks, however, already have credibility. They have the rule of law. They control legal tender. Central banks don't necessarily need a blockchain, although there are arguments for how some central banks could benefit by introducing one.[23]

Who is going to decentralize themselves? That is one of the big barriers to broader adoption of this technology by traditional institutions.

Looking ahead

The right way to think about corporate blockchains might be as a process improvement technology similar to double-entry bookkeeping or the invention of joint stock companies; they don't seem dramatic when first introduced, and their effects may not be felt quickly, but mundane process improvements can pave the way for major economic impacts.[24]

Industry impacts

Where is blockchain going to cause the greatest disruption? Without empirical data to work from, data from the *Global Blockchain Benchmarking Study*[25] helps give a sense of where the impact will be most widely felt. Most DLT service providers, when asked which

[23] Lwanda, George, *Zimbabwe Needs Its Own Cryptocurrency* (www.project-syndicate.org/commentary/zimbabwe-needs-blockchain-cryptocurrency-by-george-lwanda-2019-06, Jun 21, 2019).

[24] See *The Economist*, issue entitled, "The trust machine: How the technology behind bitcoin could change the world." Oct 31 to Nov 6, 2015.

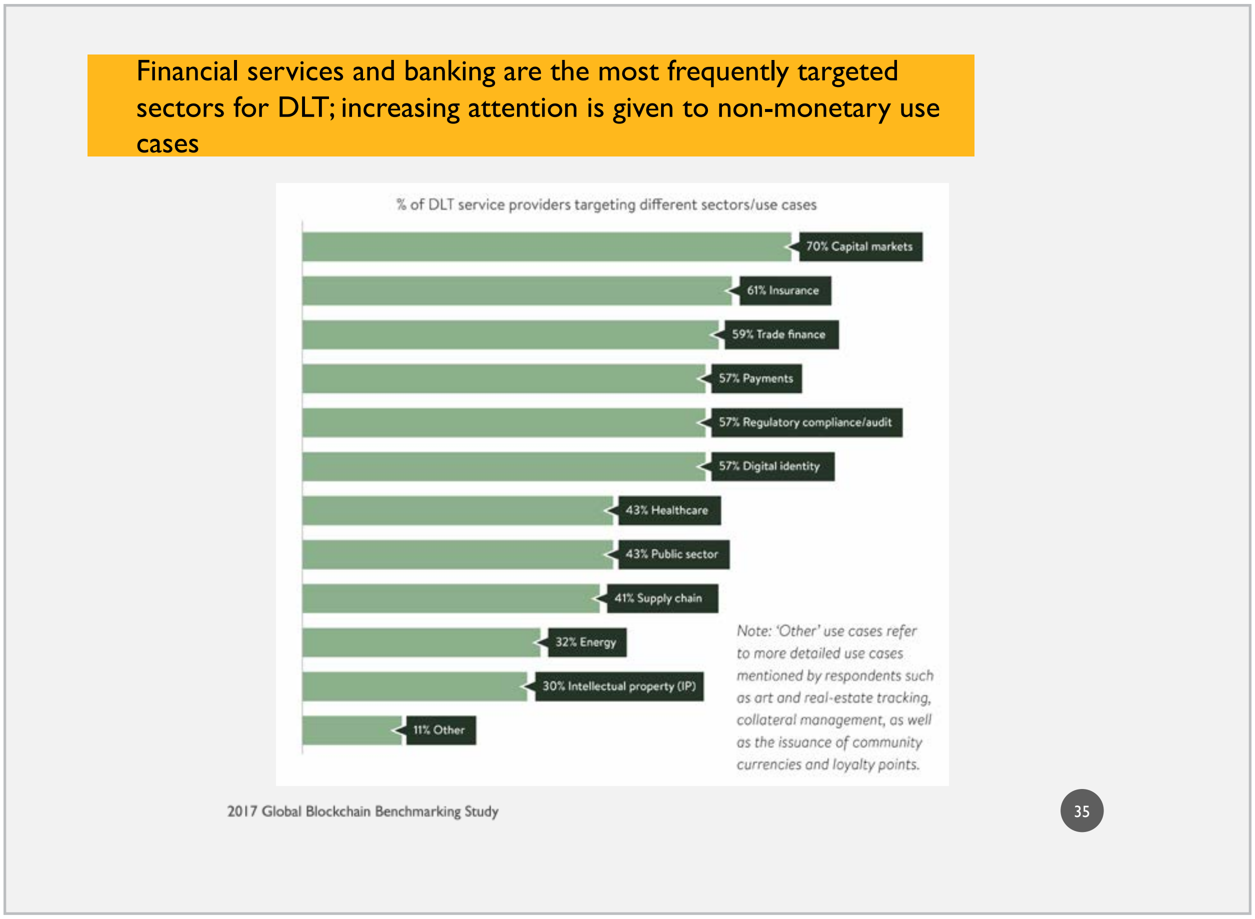
[25] Hileman, Garrick, and Michel Rauchs, *Global Blockchain Benchmarking Study* (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224, 2017).

industries or markets they are targeting, answered finance (i.e., capital markets, insurance, trade finance, payments), and some cross-disciplinary areas (e.g., digital identity, supply chain, intellectual property), among others. (See Figure 2.)

Another crude measure[26] to see where the most disruption and impact will occur is simply by counting the number of use cases. The study counted over 130 different use cases in DLT and grouped them into different industry sectors. Banking and finance lead with over 30% of all use cases, government with 13%, insurance 12%, and healthcare 8%. (See Figure 3.)

In addition, we can look at public cryptocurrency markets.

FIGURE 2: SECTORS TARGETED FOR DLT



Financial services and banking are the most frequently targeted sectors for DLT; increasing attention is given to non-monetary use cases

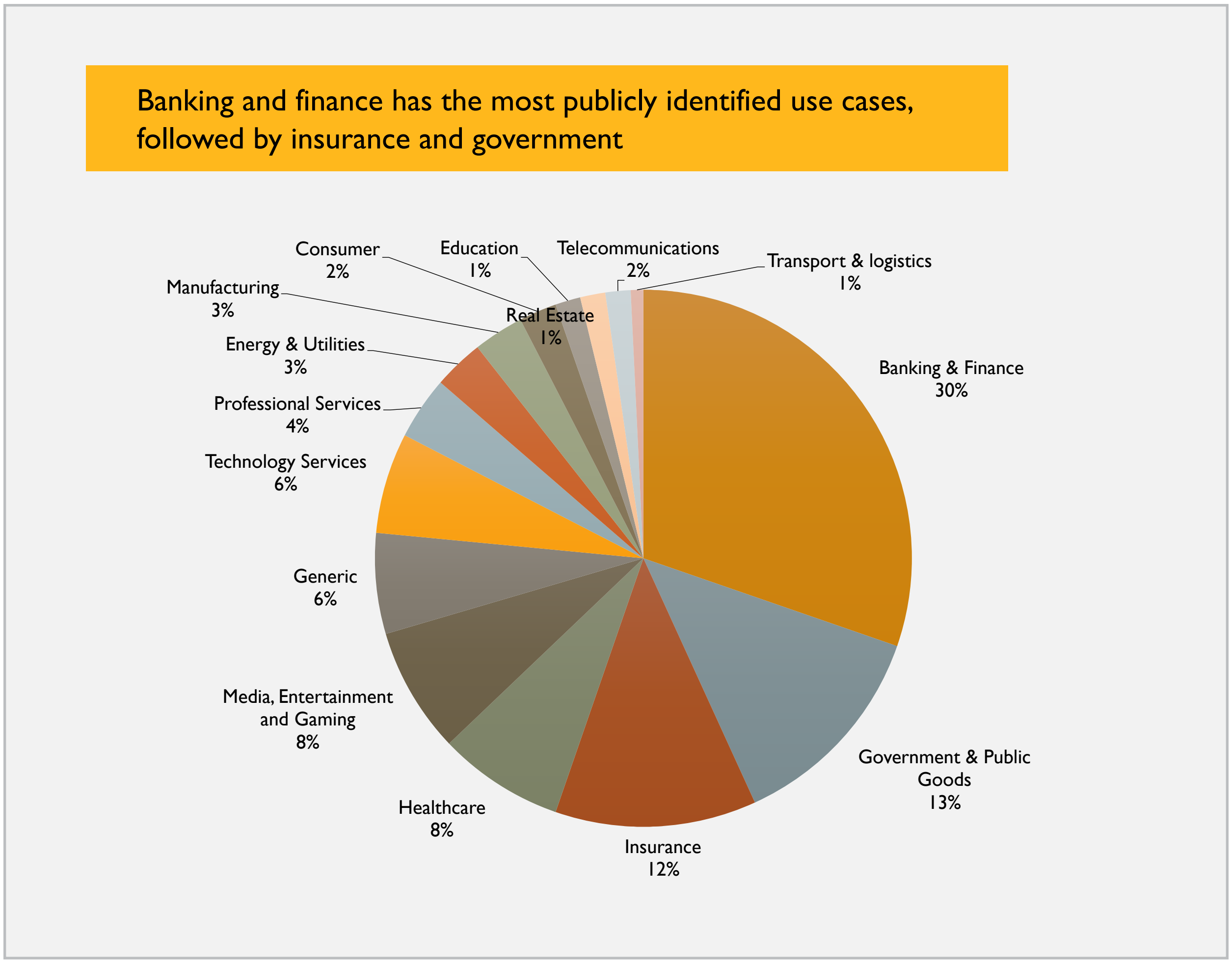
Note: 'Other' use cases refer to more detailed use cases mentioned by respondents such as art and real-estate tracking, collateral management, as well as the issuance of community currencies and loyalty points.

2017 Global Blockchain Benchmarking Study

35

[26] Crude, because the number of use cases tells nothing about how big they are and gives no sense of how impactful they are. In addition, blockchain technology was probably more obvious to banking and finance than to healthcare, because bitcoin shares similar characteristics to a financial instrument. Even so, it might be that healthcare will feel a greater impact from use of blockchain by changing the handling of electronic medical records.

FIGURE 3: DLT USE CASES BY SECTOR

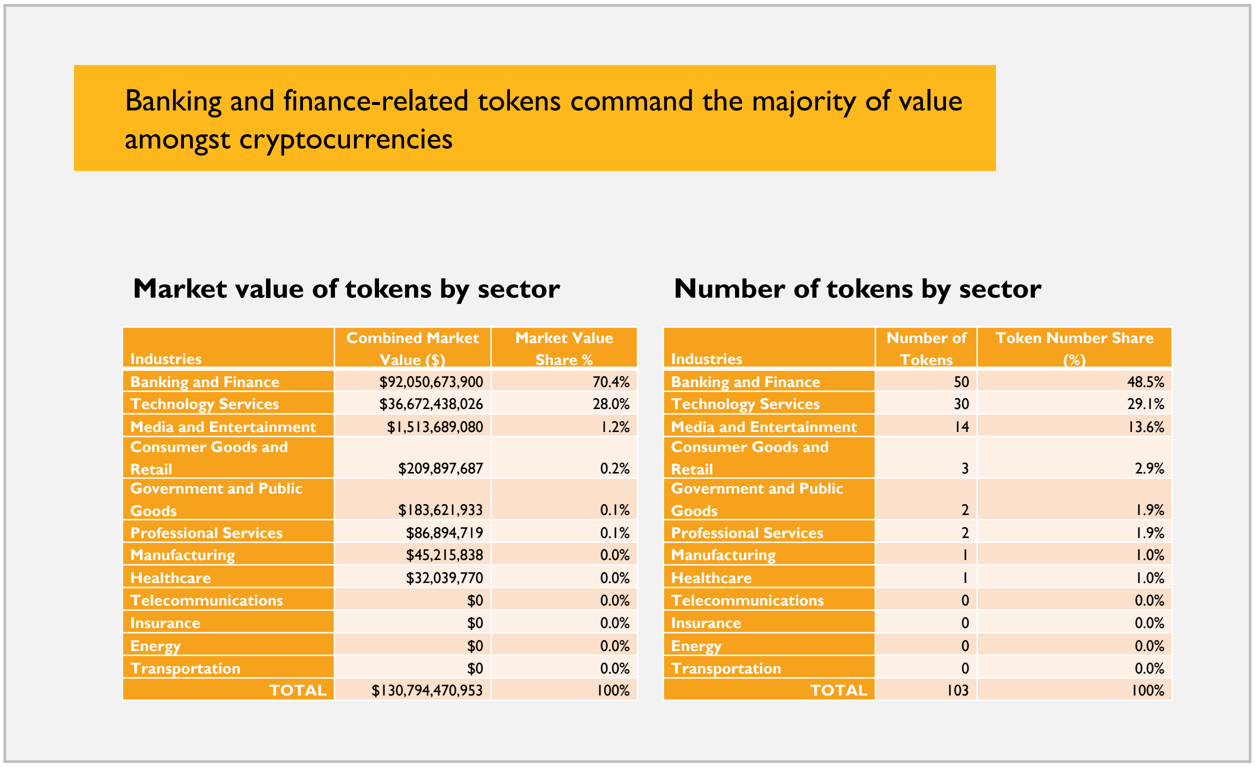


Banking and finance has the most publicly identified use cases, followed by insurance and government

Cryptocurrency markets

If the top 100 cryptocurrencies are categorized by industry, about 70% of the market value – about 50% of the coins (70%/50%) – target banking and finance; technology services (e.g., decentralized cloud storage; 28%/30%), and media and entertainment (1%/14%). (See Figure 4.)

FIGURE 4: TOP 100 CRYPTOCURRENCIES AND MARKET SHARE



Banking and finance-related tokens command the majority of value amongst cryptocurrencies

Market value of tokens by sector

Industries	Combined Market Value ($)	Market Value Share %
Banking and Finance	$92,050,673,900	70.4%
Technology Services	$36,672,438,026	28.0%
Media and Entertainment	$1,513,689,080	1.2%
Consumer Goods and Retail	$209,897,687	0.2%
Government and Public Goods	$183,621,933	0.1%
Professional Services	$86,894,719	0.1%
Manufacturing	$45,215,838	0.0%
Healthcare	$32,039,770	0.0%
Telecommunications	$0	0.0%
Insurance	$0	0.0%
Energy	$0	0.0%
Transportation	$0	0.0%
TOTAL	$130,794,470,953	100%

Number of tokens by sector

Industries	Number of Tokens	Token Number Share (%)
Banking and Finance	50	48.5%
Technology Services	30	29.1%
Media and Entertainment	14	13.6%
Consumer Goods and Retail	3	2.9%
Government and Public Goods	2	1.9%
Professional Services	2	1.9%
Manufacturing	1	1.0%
Healthcare	1	1.0%
Telecommunications	0	0.0%
Insurance	0	0.0%
Energy	0	0.0%
Transportation	0	0.0%
TOTAL	103	100%

Even if blockchain and distributed ledger technologies succeed, what is the future for bitcoin and cryptocurrencies? Some are prognosticating that cryptocurrencies like bitcoin will replace fiat currencies and become the dominant global currency within five[27] to 10[28] years, or hail cryptocurrencies as a technological revolution or modern miracle.[29] However, cryptocurrencies are influenced by a complex, constantly evolving intersection of technology, politics, and economics. What are some potential barriers to adoption?

Bitcoin in the beginning, for example, was used mostly for gambling and by criminals on the "dark web."[30] Today, while the amount of economic activity on the dark web is roughly the same as a few years ago, the big change is that the use of cryptocurrencies for investment

[27] Tim Draper, billionaire Silicon Valley venture capitalist.

[28] Jack Dorsey, CEO and founder of Twitter.

[29] Rosti Behnam, U.S. Commodity Futures Trading Commission Commissioner. (Remarks of Commissioner Rostin Behnam at the BFI Summit: "Fostering Open, Transparent, Competitive, And Financially Sound Markets" United Nations Plaza, New York, NY. June 4, 2018. Available at www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam7).

[30] Visible on the Internet, not indexed by search engines, but accessible by only special software that allows users to remain anonymous.

dwarfs their illicit use. For example, Blockchain.com Research estimates that over 30 million people own some cryptocurrency, up significantly from 2017's estimate of between five and 10 million.[31]

With cryptocurrency, complexity and difficulty of use explains some of lack of adoption to date. When it comes to financial value, people want an instrument that is easier to understand and use.

Cryptocurrencies need a network effect (i.e., a bandwagon effect and subsequent momentum) to drive greater adoption. Because of competition in the crypto space, bitcoin's dominance has dropped. This competition may undermine bitcoin's network effect and may prevent any one cryptocurrency from gaining the needed network effect to gain billions of users. Other contributors to cryptocurrencies' lack of momentum could be:

- Environmental impact – high-energy use might be solved by new consensus algorithms, but right now these are a real concern amongst many people and turn off some users
- Business strategy miscalculation – bitcoin and other cryptocurrencies would have more utility in countries with less developed financial systems and unstable inflation (e.g., sub-Saharan Africa and South America) than in regions where it is being used most widely today (USA, Europe, Asia)[32]

The biggest barrier to wider adoption of a cryptocurrency for everyday payments, like a cup of coffee, is that very few people are actually paid in cryptocurrency. Until that happens, the probability is low for a cryptocurrency to become widely used as cash and other fiat-based payment systems. That said, one group is already paid in cryptocurrency: machines that mine cryptocurrency.

Machines that underpin blockchains are compensated in cryptocurrency for processing transactions and running the consensus algorithm. If the machine-to-machine economy grows, and cryptocurrency is the coin of the realm in the machine economy, services from the machine economy will be purchased using their currency. Therefore, the machine-to-machine economy may become a key driver of greater cryptocurrency use for payments.

In the meantime, people are primarily using cryptocurrency as a *hard asset* or investment. For example, bitcoin offers a fixed total supply that doesn't increase with increases in price, in contrast with gold and other commodities. Ironically, arguably the hardest asset in history is virtual.

[31] Hileman, Garrick, and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2965436, 2017).

[32] Hileman, Garrick, The Bitcoin Market Potential Index (2014) https://ssrn.com/abstract=2752757.

Challenges in the Era of Crypto-Decentralization: Where Do We Go From Here?

By Andreas Veneris, Professor, University of Toronto, Department of Electrical and Computer Engineering, and

Ryan Berryhill, PhD Candidate (2019), University of Toronto, Department of Electrical and Computer Engineering

Introduction

Bitcoin. Ethereum. Blockchain. Crypto-economics. Over the past year, these words made global headlines. The promise of "decentralized ledger-based technologies" has created a level of excitement for technology last seen in the 1990s when the Internet entered the mainstream. Originally tied rather narrowly to the concept of "electronic cash," fully decentralized governance, because of its likely widespread adoption and its underlying technological philosophy, promises to change:

- commerce and finance
- governments and regulation
- personal privacy
- national security
- law
- property rights
- healthcare
- the socioeconomic fabric

on a global scale.

This paper presents an introduction to Bitcoin and Ethereum. It also outlines a view of the future of blockchain technology and the challenges it presents in academic and industrial communities.

The wide adoption of the Internet and smart phones further expands the technology's reach to billions of people in countries that have no access to a reliable financial system or legacy infrastructure.

Bitcoin: a distributed ledger

In 2009, Bitcoin introduced the world's first peer-to-peer electronic cash system, implemented as a ledger of monetary transactions in the form of a proof-of-work blockchain. Electronic cash systems existed before Bitcoin, but none had solved the fundamental double-spending problem in a decentralized peer-to-peer network. Instead, such systems relied on a third party – a centralized entity – to perform the bookkeeping thereby requiring trust in, and introducing a centralized point-of-failure to, the system.

The Bitcoin approach is revolutionary, because:

- Transfers of bitcoins (e.g., as payments) do not require the financial system; anyone can participate.
- Bitcoin's value as money is entirely determined by the market; no government or central authority can directly affect its value.
- Transaction fees are (in principle) transparently determined by the competition of parties who secure the network.
- Cross-border transaction times are a fraction of those of wire-transfers and are much less complicated for the user.
- Financial transactions and activity levels are transparent.

Cryptographically certified transactions

In Bitcoin, a user creates a transaction in the form of message like "I, Bob, send four bitcoins to Alice." To enable trust in the network, the message must have:

- authentication: it can only come from Bob
- integrity: it cannot be modified by others
- non-repudiation: Bob cannot later disavow it

To ensure these features, Bob must attach his cryptographic digital signature to the transaction, which is stored in the digital ledger alongside the transaction. The ledger stores a chain of digital signatures leading from a coin's creation to its current owner, which can be verified by anyone.

Solving the double-spending problem

Authentication, integrity, and non-repudiation were largely solved in electronic cash systems that pre-dated Bitcoin. The problem of "double spending" (i.e., Bob sending four bitcoins to Alice and, at the same time, sending four bitcoins to someone else, or possibly even to himself) had not been solved. A centralized authority was required to account for these transactions, but Alice could not be sure the transaction history would not be changed by the centralized authority in the future even if the transaction history were stored on a peer-to-peer network.

Essentially, relying on a network of peers, rather than a trusted third party, makes agreeing on a version of history very difficult. The solution to this problem was Bitcoin's key innovation: the proof-of-work blockchain. Once signed by the sender, a transaction diffuses through the peer-to-peer network of miners (i.e., the computers running the network). Miners compete in a sort of decentralized lottery by which the winner earns the right to append a new block of transactions to the ledger and receives a reward in the form of newly minted bitcoins. This lottery, known as proof-of-work, is a computationally intensive race by the miners to solve a cryptographic puzzle. The winning miner of this race, whose solution is easily verified by the rest of the network, broadcasts:

- a block consisting of a list of transactions
- a reference to the previous block of transactions
- a nonce (i.e., an artifact of the mining process)

In a typical operation, the block is then considered to be appended to the ledger.

However, if two or more miners solve the puzzle at approximately the same time, the event is known as a fork (i.e., two incompatible chains). The forking process is a computationally intractable one. The rule to choose the head of the chain is that the longest valid chain (i.e., the one that has accumulated the most proof-of-work) is the valid chain. Using this rule, forks normally resolve on their own.

This simple rule of the longest chain being determined by the quantity of proof-of-work has profound implications: it solves the double-spending problem. Through mining, miners are forced to commit to a specific ledger state: the one described by all transactions leading up to the block referenced in the previous block hash and the list of transactions in the current block. Any work committed to this version of history cannot be re-used to commit to any other history. For instance, if Bob used four bitcoins to buy a slice of pizza from Alice, ate the slice, and then wanted to fork the chain to regain the four bitcoins, his success would be improbable. Even using an extraordinary amount of very costly computation (i.e., orders of magnitude more than the rest of the Bitcoin network) he would not likely succeed, because new blocks (each representing hundreds of transactions) would already have been added to the chain by other miners.

The 'third' ledger

Bitcoin accounting has the following characteristics:

- agreement on an objective reality
- congruent transactions between two external parties sealed via cryptographic protocols

- blockchain entries that act as both receipt and transaction so that falsifying or deleting entries remains an essentially impossible task
- blockchain acting as a public, distributed, interlocked, permanent and transparent-to-all "third" ledger, instead of the two independent ledgers of double-entry accounting

HOW MIGHT ACCOUNTING CHANGE?

ANDREA VENERIS: Accounting will be one of the major areas that will be impacted by this technology. Not much is going to change the way we do accounting. The big change is in its registration. With a third, trustless party that acts as the golden ledger where all transactions exist, we'll have a level of transparency that is missing today. So, at that point, everybody can indeed check that the books match.

The biggest innovation is the mental shift that we don't need a central authority, but can use a centralized trust-worthy machine that everybody can see.

Ethereum: a distributed computing platform

Another major blockchain innovation started in Toronto when 18-year old University of Waterloo dropout Vitalik Buterin, leading a global team of developers, launched the Ethereum network in 2015. Ethereum generalizes the blockchain concept introduced by Bitcoin. In Bitcoin, transactions are simply transfers of money; by contrast, Ethereum supports Turing-complete programs called smart contracts,[33] which have with the ability to store their state in the blockchain. Each transaction is one of:

- a simple transfer of money
- the creation of a smart contract that uploads its code to the blockchain
- the execution of code (i.e., a set of transitioning software states) contained in a smart contract that has been already deployed on Ethereum

Ethereum implements the 1990s vision of Nick Szabo's decentralized autonomous organizations (DAOs).[34] Buterin describes DAOs as "long-term smart contracts that contain the assets and encode the bylaws of an entire organization."[35]

[33] Vitalik Buterin, *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform* (https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf, n.d., p. 1.).

[34] Nick Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday* v.2 (9) (https://firstmonday.org/ojs/index.php/fm/article/view/548/469.DOI:http:/dx.doi.org/10.5210/fm.v2i9.548, September 1, 1997).

[35] Vitalik Buterin*, ibid*.

Ethereum's decentralized smart contracts present a whole new set of opportunities as wide-ranging as:

- decentralized commerce
- decentralized trading of securities
- fully automated supply chain management
- automatic enforcements and transfers of artists' property rights

Smart contracts come with challenges. For instance, a smart contract program could increase the size of the blockchain by entering an infinite loop or by storing lots of states / data. Problems like these are solved in Ethereum by charging for computations with a certain amount of "gas" (i.e., Ether). A user requesting a computation must send an amount of Ether along with a gas price they are willing to pay miners to execute the computation. Each computational step in the program costs gas in proportion to the computational cost borne by the miners.

An important point is that Ethereum is not a supercomputer. Instead, it is an extremely limited computing platform that is very expensive to use. However, its benefit is to allow anyone to run stateful, auditable computations without the need to trust a centralized authority to attest that, for example, an Ethereum-based casino is playing fair. In theory, the code is available to all participants to an audit to check that they are not being cheated.

Key challenges in moving forward

Blockchain technology faces several technological and regulatory barriers.

Scalability

At the time of writing, Bitcoin blocks are limited to 1 MB of transactions, which limits throughput to roughly seven transactions per second (tps). Similarly, Ethereum's throughput is less than 20 tps. Throughput is low compared to PayPal (at 200 tps) and VISA (at 24,000 tps on average).[36] Moreover, as both protocols use proof-of-work, they consume an inordinate amount of the world's electricity to maintain their ledgers: 0.25 per cent for Bitcoin;[37] 0.04 per cent for Ethereum.[38]

[36] Crypto Account Builders, *The Fastest Cryptocurrency Transaction Speeds for 2018* (https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1baf87ef, October 5, 2018).

[37] Digiconomist, *Bitcoin Energy Consumption Index: Key Network Statistics* (https://digiconomist.net/bitcoin-energy-consumption, 2019).

[38] Digiconomist, *Ethereum Energy Consumption Index (beta): Ethereum Network Statistics* (https://digiconomist.net/ethereum-energy-consumption, 2019).

For blockchain to gain wide adoption and reach its full potential (e.g., in supporting the Internet of Things[39]), throughput must be increased dramatically, and power consumption must be reduced. To those ends, several proposals have been made, including:

- on-chain scaling: increasing block size
- off-chain scaling: allowing some transactions to occur outside the blockchain (e.g., the Plasma framework[40] for executing smart contracts, and the Lightning Network[41])
- proof-of-stake: selecting miners to add blocks using algorithms that choose miners based on their stake in the system
- directed acyclic graphs and network gossiping: other blockchain topologies

Smart contracts

Smart contracts (as software programs) may contain bugs. In the last three years, attacks against smart contracts have stolen or destroyed hundreds of millions of dollars in crypto-currency. In practice, it is impossible for most users to audit smart contracts to verify their functionality. Techniques such as automated formal verification and automated synthesis for smart contracts are in their infancy today, but they promise to make smart contract auditability a reality for a wider set of users.

A unified foundation for crypto-economics

Crypto-economics is a term coined by Vitalik Buterin to describe the blockchain ecosystem where economic incentives, cryptographic principles, decentralized consensus on distributed systems, and game theory all mix together to provide the foundation for the "trustless" nature of the ecosystem.

Blockchain systems call for new research in the area of game theory:

- mechanism / market design
- reputation systems
- challenge-response games
- escalation games
- appropriate economic incentives for distributed fault tolerance

Further, because smart contracts allow any corporate or individual entity to generate new tokens to represent its underlying economy, and because popular assets today (including bitcoin and ether) are characterized by a large amount of volatility, the emergence of

[39] Stephen Ornes, "Core Concept: The Internet of Things and the explosion of interconnectivity," Proceedings of the National Academy of Sciences of the United States of America (PNAS) (www.pnas.org/content/113/40/11059, October 4, 2016).

[40] Dave Kajpust, *Blockchain Scaling Solutions: Cosmos and Plasma* (https://medium.com/tendermint/blockchain-scaling-solutions-cosmos-and-plasma-b5ee09456f80, September 24, 2018).

[41] See Lightning Network (https://lightning.network, n.d.).

tokenized economies on distributed ledgers necessitates the development of new theories for fiscal and monetary policies / governance, and the design of stable-coins (i.e., digital currencies that maintain their value when pegged to other assets [USD, gold, etc.])

Governance, regulation, and law

Blockchain's cryptographic technical complexity and its cross-border character impose unprecedented challenges for lawmakers, regulators, and tax authorities. Blockchain technologists and regulators often do not speak the same "language." As a consequence, government bodies issue contradictory, abstract, or confusing statements for the ecosystem. For instance, cryptocurrencies are legal tender in Japan, treated as securities in the U.S. and Canada, viewed as assets / securities / utility in Switzerland, but outlawed in Bangladesh and Vietnam. This disparity:

- creates an uncertain regulatory environment for new businesses
- amplifies international regulatory imbalances
- encourages capital flows to jurisdictions that favour sheltering such ecosystems

All of these things call for a global effort to regulate blockchain.

An Introduction to IBM's Blockchain for Business

By Peter Patterson, IBM Blockchain – Canada Market Leader

Background

The cryptoworld of Bitcoin, Ethereum and other coins has its place, but what we are trying to accomplish at IBM, is blockchain from a business perspective.

Different types of blockchain

While all blockchains aim to provide irrefutable proof that a set of transactions occurred between participants, different types of blockchain exist. For example, Bitcoin is an example of a permissionless, public blockchain. As the first blockchain application, it defines a shadow currency and its ledger and is resource-intensive. Put simply, it is anonymous, does have some security issues, and is not very environmentally friendly.

Blockchains for business are generally permissioned, private, prioritize identity over anonymity, use a selective endorsement (i.e., agreement on success criteria) instead of a proof-of-work system of transaction verification, and deal with assets instead of cryptocurrency.

In 2014, an IBM team calling themselves the Chain Gang started thinking about how and why blockchain would become important. Its first project (with Samsung) was called Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT), and used groundbreaking Ethereum as the underlying blockchain to settle transactions. Simplified, the concept was that washing machines, connecting to a network, could replenish their own supplies.[42]

A fundamental problem apparent with the blockchain was the small number of transactions per second compared to the thousands of transactions per second a large enterprise requires. So IBM created its own blockchain and decided early on that to gain the network effect[43] it should not be owned by IBM but should be an open-source technology. The code was turned over to the Linux Foundation, experts in governing open-source projects. That is how Hyperledger – open-source blockchain for business – was born.[44]

[42] Editor's note: For more on the ADEPT project, see Higgins, Stan. 2015. "IBM reveals proof of concept for blockchain-powered internet of things." *coindesk*. Available at www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things.

[43] Editor's note: For more information on the network effect, see the Hileman paper also in this volume.

[44] IBM does not own Hyperledger Fabric; it is an open source tool. IBM built an infrastructure platform and some tools, but anyone can download Fabric for free. IBM is a major player in a consortium but expects its role to diminish over time as collaboration increases. For enterprises, IBM fences off and modifies the system.

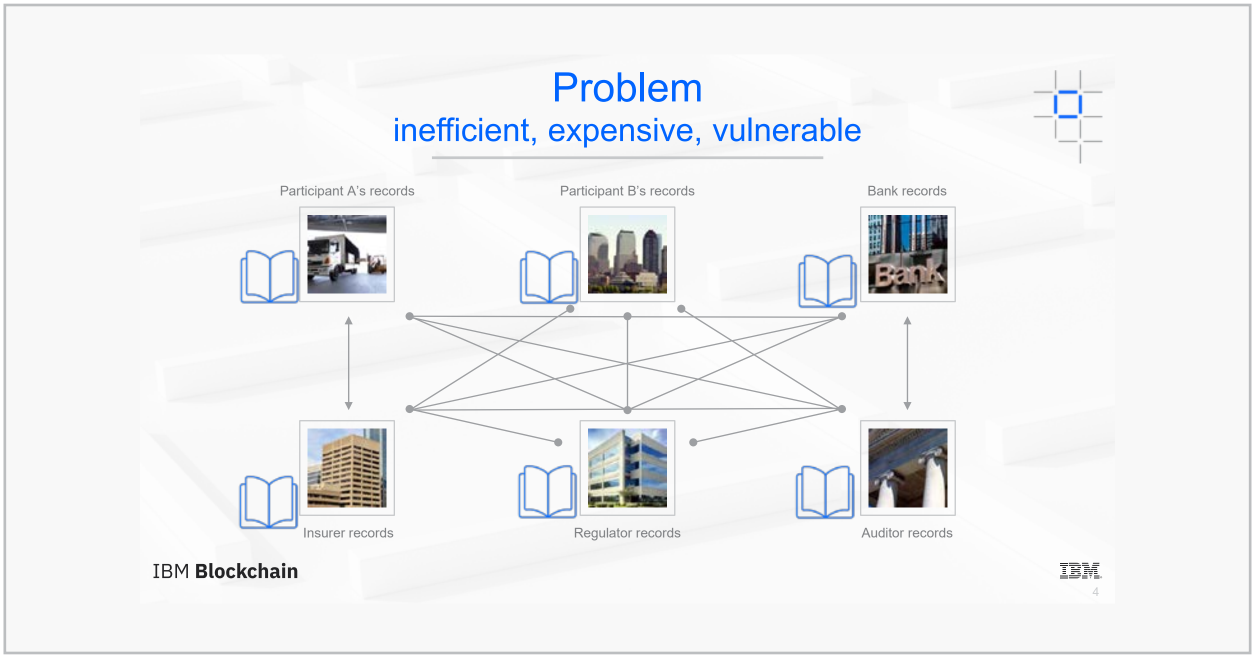
This paper looks at the characteristics of blockchain for business and the problems it has the potential to solve. These are illustrated by in-production projects and actual-use cases that cross industrial boundaries through collaboration.

Business networks 'before' and 'after' blockchain

Before blockchain

Figure 1 represents the *status quo* for most business networks (i.e., networks before blockchain). Participants update their own ledger(s) to document business transactions as they occur. This duplication of effort plus intermediaries adding margin for services is *expensive*. It is also clearly *inefficient* since the contract (i.e., business conditions to be satisfied) is duplicated by every network participant. It is also *vulnerable* because, if an incident compromises a central system (e.g., a bank), the whole business network is affected. Incidents can include fraud, cyber attack or a simple mistake.

FIGURE 1: BUSINESS NETWORKS BEFORE BLOCKCHAIN



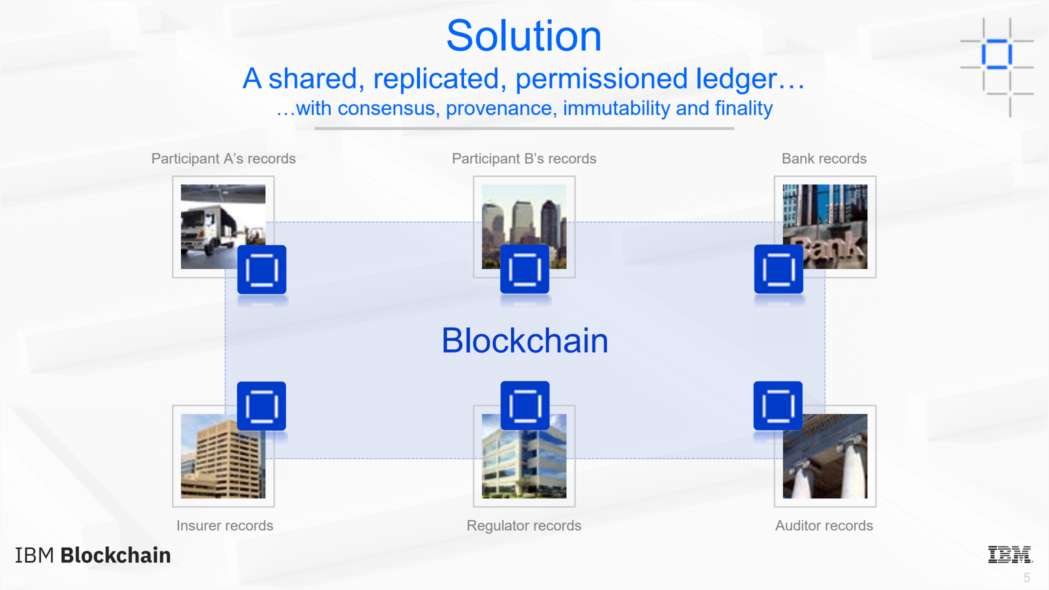
Problem

inefficient, expensive, vulnerable

After blockchain

Figure 2 illustrates the potential solution to "before problems" that blockchain can offer to business networks.

FIGURE 2: BUSINESS NETWORKS AFTER BLOCKCHAIN



Solution

A shared, replicated, permissioned ledger…

…with consensus, provenance, immutability and finality

Blockchain architecture allows participants to *share* a ledger that is updated every time a transaction occurs through peer to peer replication. Cryptography ensures that network participants see only the parts of the ledger relevant to them (i.e., "need to know"), and that transactions are secure, authenticated and verifiable.

Blockchain also allows smart contracts for asset transfer (i.e., the conditions under which the transaction can occur) to be embedded in the transaction database.

Network participants agree through consensus (or other mechanism) on how transactions will be verified. The number of participants is the same as before (i.e., this is not a form of disintermediation), but government oversight, compliance, and audit can be part of the same network.

The four core tenets of blockchain for business are:

- Consensus: All participants agree that a transaction is valid.
- Provenance: Participants know where the asset came from and how its ownership has changed over time.

- Immutability: No participant can tamper with a transaction once it has been agreed upon. If a transaction was in error, then a new transaction must be used to reverse the error, and both must remain visible.
- Finality: There is *one* place to determine the ownership of an asset or the completion of a transaction. This is the role of the shared ledger.

WHAT AREAS DO YOU THINK WILL BE IMPACTED MOST BY BLOCKCHAIN?

PETER PATTERSON: Aside from financial services, etc., I think government and engaged citizenry are really interesting potential areas. For example, to engage with citizens in a new and different way or create new value for constituents or make their voices heard. **Broadly speaking, though, all of the interest right now is around supply chain.**

Real-life examples

To make blockchain networks meaningful, IBM contributes technologists but collaborates with organizations with other areas of expertise to develop projects with wide applicability, such as the following three.

Example 1: Food Trust – a 'provenance engine' to track food from farm to fork

Food-related recalls have real economic impacts. In 2006, all spinach was removed from grocery shelves, and all spinach growers were affected when spinach from just one supplier carried *E. coli*, yet caused hundreds of people to become sick.[45] In an example of food fraud, 13 Walmart stores were closed in Western China in 2011[46] when meat was mislabelled as organic. While not the source of the problems, stores were perceived as guilty by association. At the time, tracing problems was slow.

Because of that history, and many other incidents affecting many retailers, Walmart's former head of food safety, Frank Yiannis, was extremely interested in hearing about IBM-sponsored research to identify pathogens with the potential for food-borne illness. In collaboration first with Walmart and now nine other food giants, including Dole, Nestlé, and Unilever, IBM has built a "provenance engine" using blockchain technology, to track food from "farm to fork."

[45] John McChesney, *FDA Links Spinach E. Coli Risk to Calif. Company* (www.npr.org/templates/story/story.php?storyId=6084158, September 15, 2006).

[46] Reuters, *Wal-Mart workers detained in China pork probe* (www.reuters.com/article/walmart-china/wal-mart-workers-detained-in-china-pork-probe-idUSN1E79A08O20111011, October 11, 2011).

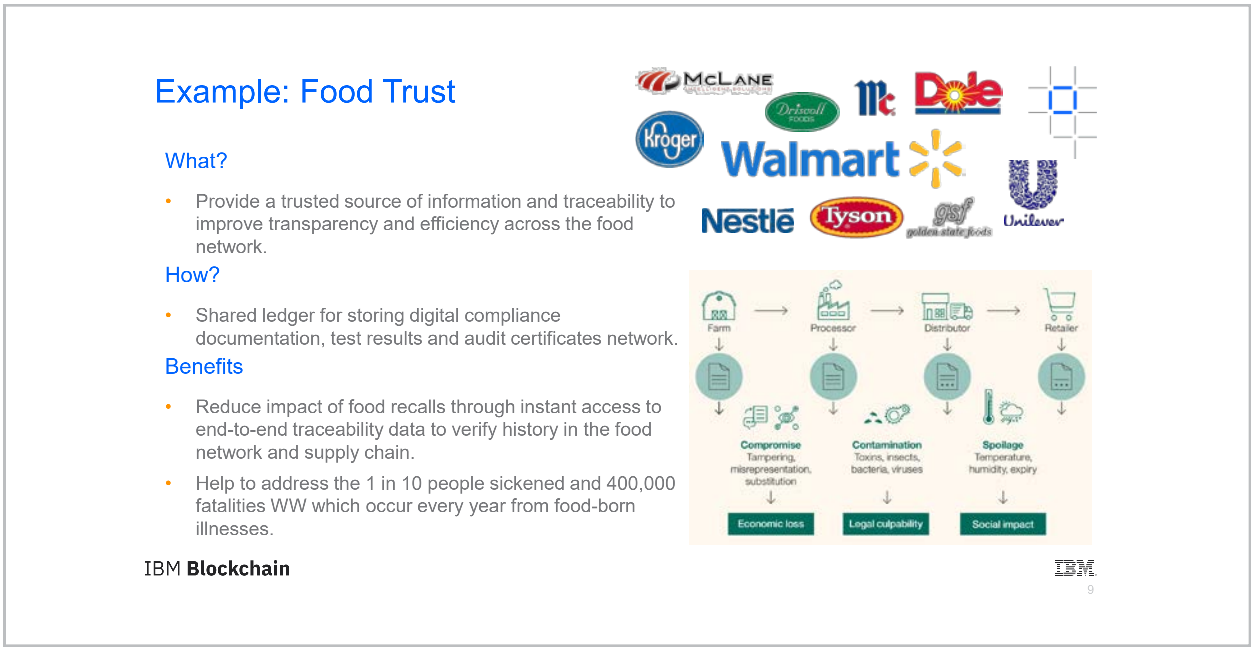
Set up with a focus on combatting food-borne illnesses, the "IBM Food Trust"[47] software's goal now is to make the food supply chain transparent by digitally tracing food products from an ecosystem of suppliers to consumers.

The Food Trust blockchain (Figure 3) provides a permanent record of food supply chain transactions, digital product information (e.g., farm origination details), processing data, and shipping details that are digitally connected to food items. The shared ledger also stores digital compliance documentation, test results, and audit certificates.

In a video[48] explaining Food Trust, Frank Yiannis says that identifying the source of mangoes after implementing Food Trust was reduced to 2.2 seconds from six days or longer. The speed and accuracy of the system means that recalls are faster (i.e., resulting in improving food safety), and targeted (i.e., reducing any economic impact).

In addition, the software helps manage inventory more tightly, reduces waste and spoilage, and drives supply chain efficiency and visibility.

FIGURE 3: THE FOOD TRUST BLOCKCHAIN



Example: Food Trust

What?

- Provide a trusted source of information and traceability to improve transparency and efficiency across the food network.

How?

- Shared ledger for storing digital compliance documentation, test results and audit certificates network.

Benefits

- Reduce impact of food recalls through instant access to end-to-end traceability data to verify history in the food network and supply chain.
- Help to address the 1 in 10 people sickened and 400,000 fatalities WW which occur every year from food-born illnesses.

IBM **Blockchain**

[47] For more information, see IBM. (n.d.) *IBM Food Trust: adding trust and transparency to our food* [webpage and video]. Available at www.ibm.com/blockchain/solutions/food-trust?cm_mmc=OSocial_Youtube-_-Blockchain+and+Watson+Financial+Services_Blockchain-_-WW_WW-_-Walmarts+food+safety+solution+using+IBM+Food+Trust+built+on+the+IBM+Blockchain+Platform+Description+Food+Trust+Webpage&cm_mmca1=000026VK&cm_mmca2=10008219&.

[48] Anonymous. August 22, 2017. *Walmart's food safety solution using IBM Food Trust built on the IBM Blockchain Platform* [YouTube video]. Available at www.youtube.com/watch?v=SV0KXBxSoio.

Example 2: Maersk – trade digitization

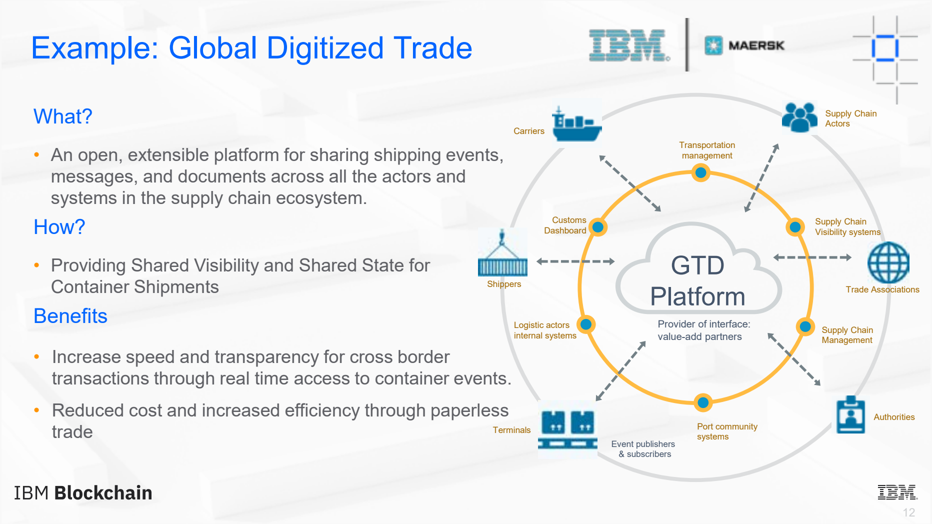
Maersk, the world's largest shipping company, in partnership with IBM, has built a global trade digitization (GTD) platform (now called TradeLens[49]) using Hyperledger's open-source fabric blockchain.

The first project looked at a shipment of avocados from Mombasa to Port of Rotterdam, a shipment that involved 30 actors, more than a hundred people, and more than 200 paper-based exchanges over the journey. If all that paper could be digitized and replaced by a trust system, the different legs of the journey could be better organized, ports would receive documents before ships docked, changes would be processed faster, and harbour waiting times and stacking (i.e., storage) fees before inland transportation would be reduced. Inter-modal transport would be faster, cheaper, and more efficient.

Digitizing the end-to-end supply chain process using TradeLens (Figure 4) can increase transparency and security among all trading partners, reduce fraud and errors, decrease the time products spend in transit, and lower waste and cost. The blockchain provides real-time tracking for the shipment of goods across multiple global supply chain checkpoints.

In Canada, Canada Border Services Agency (CBSA), Port of Montreal, Port of Halifax and CN Rail have all signed on to use this product, in addition to nearly 100 enterprises in other countries.

FIGURE 4: DIGITIZING TRADE – TRADELENS



Example: Global Digitized Trade

What?

- An open, extensible platform for sharing shipping events, messages, and documents across all the actors and systems in the supply chain ecosystem.

How?

- Providing Shared Visibility and Shared State for Container Shipments

Benefits

- Increase speed and transparency for cross border transactions through real time access to container events.
- Reduced cost and increased efficiency through paperless trade

IBM **Blockchain**

[49] For more information, see Anonymous. 2019. *TradeLens: Digitizing the global supply chain* [website and video]. Available at www.tradelens.com.

Example 3: transactive energy – Project Spark

Every province has its own electricity grid operated by a provincial system operator (PSO). The PSO supplies electricity demand in real time from all available sources: not only power plants, but also distributed energy resources connected to the grid (e.g., solar panels on roofs, batteries, including the batteries in electric vehicles (EVs), small hydroelectric, industrial surplus energy, etc.). Managing all the distributed resources (i.e., the supply side) is a challenge because these resources pop on and off the grid at any given time.

The PSO's job is also to supply balanced power (i.e., no brownouts or blackouts). As an illustration, suppose everyone drove EVs and plugged them in for a full charge immediately after arriving home at night. Suppose the PSO had not planned for that excessive electricity demand. It might need to go to the spot market to buy power from other grid operators. Since one of the PSO's roles includes setting rates and planning for future energy needs, it might decide to raise rates or decide that more electrical infrastructure (i.e., plants, poles, wires) is required. Both are unpopular and expensive.

Managing the demand side (i.e., changing consumer behaviour) and smoothing out the supply side (i.e., by finding and adding those distributed power resources to the grid) is where blockchain and the Spark project come in. Called transactive energy, it is the way of the future by making use of microgrids and peer-to-peer power sharing.

Using the EV example again, suppose the PSO wrote a contract on blockchain for EV owners and measured their electricity-consuming behaviour. If they trickle-charge their vehicle in off-peak times, instead of full-charging at peak times, they would get a token (i.e., a Spark). In addition, if owners allowed the PSO to *take power from* their EV batteries at peak times, spending on infrastructure would be reduced and owners would get another Spark.

The Spark is an example of a stable coin on Hyperledger fabric backed by fiat. The owner could take it to any merchant in Canada and tap-to-pay using a wallet on a phone. Interac rails would complete the transaction. The PSO's capital for deferred infrastructure expenditures would be in a bank account with one of the banks in Canada. The merchants would not even know the Spark is a coin; it would just look and feel like cash to them. The EV owner could redeem the Spark through e-transfer by self-transferring cash along the e-transfer rails.

The magic of the system lies in how it affects carbon offsets. Because the provenance of that electron is known, whether it is green energy is also known. When it was generated, who owns it, who sold it, and who bought it are also known. For a business, it would be important to know that the electron could qualify as a carbon offset and could potentially work into sustainability metrics to earn tax credits. The business's environmental, social and governance (ESG) ratings might actually give the business cheaper access to capital through innovative banks (e.g., BNP Paribas in Europe).

The Spark project is an example of the power of blockchain technologies to *exchange different forms of value* in a *cross-industry* network, where non-traditional partners can collaborate to innovate, build new value propositions, optimize costs, risks, and capital by using digital platforms and marketplaces.

WHAT SKILLS BESIDES TECH AND COMPUTER SCIENCE SKILLS WERE COMMON AMONG TEAMS THAT SUCCESSFULLY IMPLEMENTED BLOCKCHAIN TECHNOLOGIES IN THEIR SYSTEMS?

PETER PATTERSON: Tech skills at a core level are a requirement on a team, but most successful teams had deep industry knowledge, for example, MBAs with a tech background and a deep industry view.

In terms of roles and titles, I typically get the best traction and most successful ideas with advanced planning groups and innovation groups and teams. **I think accountants and lawyers will become more and more valuable over time as more projects are implemented.**

OSC LaunchPad and Innovation

By Pat Chaukos, Deputy Director, Ontario Securities Commission (OSC)

Introduction – what is OSC LaunchPad?

As a regulatory agency, the Ontario Securities Commission (OSC) administers and enforces the *Ontario Securities Act* (the *Act*). The purposes of the *Act* are to:

- provide protection to investors from unfair, improper or fraudulent practices
- foster fair and efficient capital markets and confidence in capital markets
- contribute to the stability of the financial system and the reduction of systemic risk[50]

In recent years, technological innovation has been the most disruptive force to affect the financial industry and the capital markets. It has transformed consumer and investor behaviours and expectations, operates irrespective of borders and industry lines, and has changed the way we think of the word "fast." It has also introduced new assets and new business models that do not fit neatly within existing regulatory frameworks.

As a regulator, the OSC plays a critical role in integrating new innovations in the marketplace to keep Ontario capital markets globally competitive. The creation of OSC LaunchPad in 2016 was a reflection of the need to keep securities regulation in step with financial technology (fintech) innovation. We recognized we needed to invest resources to understand developments and trends in fintech, as well as the unique challenges encountered by businesses. The goal of OSC LaunchPad is to take a modern approach to securities regulation to help innovators navigate the rules while at the same time fulfilling our mandate to protect investors, promote confidence in our capital markets, and reduce systemic risk.

[50] *Securities Act*, RSO 1990, c. S.5, as amended by s. 1.1.

OSC LaunchPad's three major responsibilities are to:

- engage with the fintech community and businesses to ensure they understand they may be subject to securities regulation, including important investor-protection requirements
- understand emerging trends, help innovators navigate regulation and, where appropriate, provide exemptions from requirements
- take lessons we are learning and apply them to other areas of regulation to keep Ontario capital markets globally competitive

Engagement and investor protection

Technological innovation happens at a rapid pace, and innovators are working on projects that have the ability to transform and disrupt the way we currently do many things.

Unfortunately, some innovators are not aware that securities regulations may apply to their businesses and that they may be required to provide certain investor protections. For example, an online portal or website that recommends an investment to an individual is generally required to have processes in place to ensure the investment is suitable for that individual. Another example is in the case of an initial coin offering (ICO) that facilitates a transaction of a security. The ICO requires registration with the OSC and compliance with several rules, including those that prescribe important disclosures for investors. These rules serve the public good and are fundamental to the fairness and integrity of the capital markets.

Unfortunately, if consideration is not given to securities regulation at the early stages, a business may experience significant costs and delays detrimental to success. Because we do not want to see Ontario businesses fail, OSC LaunchPad is highly focused on engaging with the fintech community. We are working to improve awareness among businesses that we will take the time to discuss their ideas with them, the regulatory requirements that will apply, and how OSC LaunchPad may provide flexible support.

Helping innovators navigate regulation

OSC LaunchPad offers a formal support opportunity for novel fintech businesses that have innovative products, services or applications that benefit investors. To date, we have received over 200 requests for support from a variety of businesses, including those offering digital trading, lending, and crowdfunding platforms; crypto-asset investment funds; token offerings; and technology solutions to regulatory challenges. We have met with businesses at various stages of development and that require various levels of support. In some instances, where business models have not fit neatly into our existing regulatory framework, we have provided exemptions on a trial basis with specific time limits and restrictions, such as limiting investments by retail investors.[51]

OSC LaunchPad is also involved in both national and international technology sandboxes where Ontario businesses have the opportunity to test their ideas in a live environment, with valuable access to investors across Canada and the globe. Because technology-based enterprises often want to operate in multiple jurisdictions, we work with other regulators to co-ordinate requirements and standards to increase the efficiencies of these businesses and allow them to scale. This happens in Canada through the Canadian Securities Administrators (CSA) Regulatory Sandbox;[52] internationally, through formal agreements with other countries (including Australia, the U.K., Abu Dhabi, and France); and as part of the Global Financial Innovation Network, where 11 financial regulators collaborate to create easier cross-border navigation for innovative firms.[53]

Modernizing regulation

Engaging with the fintech community and start-up businesses also gives us the opportunity to learn about regulatory challenges, innovations, and trends, so we can reduce regulatory burden and develop modern regulatory approaches.

The emergence of distributed ledger technology and crypto-assets, for example, has led to the creation of a completely new asset class and has raised unique challenges for regulators and risks for investors. Since these technologies are international phenomena, operating across borders and without intermediaries, a global response is required.

The OSC plays a central role in the International Organization of Securities Commissions (IOSCO),[54] which develops, implements and promotes adherence to internationally recognized standards for securities regulation. With the interests of Ontarians firmly in mind, we are involved with IOSCO at both the board and committee levels to develop international standards.

[51] Through the Canadian Securities Administrators (CSA) Regulatory Sandbox, the OSC has provided exemptions in connection with two initial coin offerings. See the Ontario Securities Commission's *OSC LaunchPad: Navigating Securities Regulation: How We Help Fintechs* (www.osc.gov.on.ca/en/navigating-regulation.htm#how-we-help-fintechs, 2019) and follow the links for *Impak* and *Token Funder* to go to the decisions for exemption.

[52] Canadian Securities Administrators, *CSA Regulatory Sandbox* (www.securities-administrators.ca/industry_resources.aspx?id=1588, 2009 [*sic.*]).

[53] Ontario Securities Commission, *OSC LaunchPad: Navigating Securities Regulation: Regulatory Partnerships* (www.osc.gov.on.ca/en/navigating-regulation.htm#partnerships, 2019).

[54] See International Organization of Securities Commissions (www.iosco.org, 2019).

With respect to fintech, we are very involved in current initiatives that track trends, set standards, and explore ICOs, trading platforms and crypto-assets. How we approach novel fintech issues domestically is important since we co-ordinate and share information, ideas, and experiences in a global forum with international regulators who are facing many of the same issues.

Our international participation has resulted in the publication of guidance through the CSA on the applicability of securities laws to crypto-asset offerings,[55, 56] investment funds, and trading platforms. By providing greater clarity on regulations and by ensuring this guidance is aligned with international standards, we hope to improve the outcomes and experiences of market participants and investors doing business in Ontario.

For more information on OSC LaunchPad guidance, developments and events, visit www.osc.gov.on.ca/en/osclaunchpad.htm.

WHAT ARE YOUR THOUGHTS ON THE DISRUPTION OF TECHNOLOGY TO THE CAPITAL MARKETS?

PAT CHAUKOS: Where blockchain and DLT will be a huge benefit, I think, to all of us, is in terms of how we execute trades; how we buy investment products. Think about back office, middle office, exchanges, all the intermediaries involved. I think the technology will help collapse some of those steps. I think that's where we as individuals, hopefully, will see some of those cost savings.

HOW ABOUT ON IDENTITY AND INCLUSION?

PAT CHAUKOS: When the Ontario Securities Commission started OSC Launchpad a couple of years ago, we actually did a hackathon called OSC RegHackTO.[57] One of the challenges to participants was around "client identity and knowing your clients." Think about how many times you fill out a form whether you're opening a bank account, applying for a loan, etc., so many instances where we fill out our name, address, etc. What if we didn't have to fill out those forms? What if retailers, institutions, etc. could verify our identity in an automated way, and we could give selective consent for them to do so? It would save a lot of time and energy. I think that's a good example of how blockchain would be able to help, which spans many services in Canada.

[55] Canadian Securities Administrators, *CSA Staff Notice 46-307 Cryptocurrency Offerings* (www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm, August 24, 2017).

[56] Canadian Securities Administrators, *CSA Staff Notice 46-308: Securities Law Implications for Offerings of Tokens* (www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm, June 11, 2018).

[57] Ontario Securities Commission, OSC RegHackTO: Insights from Canada's First Regulatory Hackathon (www.osc.gov.on.ca/documents/en/launchpad_20170306_white-paper-insights-from-canadas-first-hackathon.pdf, March 6, 2017).

Accounting and Auditing in a Blockchain-Enabled World: Audit Regulation on the New Frontier

By Carol Paradine, CEO, Canadian Public Accountability Board (CPAB)

Introduction

As I reflected on this presentation and on the types of technological innovation I have seen in accounting and auditing during my time in the profession, I thought about things like the Internet, smart phones, and computer-assisted audit techniques. I would broadly classify these types of innovation as *enablers*, useful tools that have assisted us as accounting and auditing professionals, but which did not fundamentally change what we do.

However, with blockchain technology and some of the other advancements in artificial intelligence (AI) and robotic process automation, we are seeing technological innovations that promise to fundamentally disrupt the accounting and auditing professions in ways that are not yet completely clear.

The blockchain-enabled audit: fact, illusion or something in between?

At CPAB, we see the tremendous potential that blockchain technology has to offer, and we are following developments closely.

Blockchain enthusiasts say that distributed ledger technology will render intermediaries like banks and auditors redundant. Because blockchains are designed to resist modification of stored records, trust appears to be inherent in the blockchain protocols. In other words, trust does not need to be injected from the outside. Blockchain applications in the payments and remittance industry, for instance, are designed to eliminate the need for intermediaries like banks.

As an example, take traditional financial reporting. Auditors inject trust by attesting that the financial statements are fairly stated. Consider how blockchain and other advanced technologies could displace auditors as the agents of that trust:

- Smart contracts built on blockchains could be used to automate virtually all company transactions which, in turn, would be recorded immutably on a distributed ledger. We may see entire finance departments displaced by automation that follows IF/THEN protocols.
- Consider a company involved in distribution. When the distributor receives inventory fitted with electronic tags by the manufacturer, smart contracts could automate the entire accounts payable function.
- If the operating effectiveness of internal controls were inherent in the design of smart contracts, traditionally higher-risk manual controls would become redundant.
- AI systems could then be used to pick up where blockchain technology left off (i.e., by handling accounting accruals and estimates).

We might be tempted to think that, with trust inherent in the programming of the smart contracts and the immutability of the blockchain record, there is not much left for an auditor to do. Although this is all very interesting, I don't think that we are there yet. I strongly believe that a (human) auditor's judgment and professional skepticism will not be replaced by machines any time soon. We are somewhere in between, with auditors collaborating with ever-smarter machines.

Auditors will still be required to verify that smart contracts have been configured to handle legitimate business transactions. If a smart contract is used to pay contract employees based on hours logged, auditors will need to verify that real employees are being paid to carry out real work, and that fraudulent payments are not being made to the smart contract designer. Further, auditors will need to test whether the AI black boxes used to make estimates are operating appropriately.

Cryptocurrencies – a new frontier

While advancements in blockchain technology are of great interest to CPAB, investor protection and the public's trust in the capital markets are its primary concerns. Not all ventures in blockchain technology are worthwhile or even legitimate, and what the future holds for the 2000+ cryptocurrencies currently traded on cryptocurrency exchanges around the world is anybody's guess.

At last count, about 50 public companies in Canada are involved in the cryptocurrency ecosystem. In fact, as CPAB understands it, this is one of the highest numbers of public companies with activities related to cryptocurrencies anywhere in the world. Many are cryptocurrency miners, some hold cryptocurrencies for capital appreciation, and others issue tokens and coins to finance activities ranging from developing new blockchain solutions to exploring for gold.

In an article on cryptocurrencies and cannabis companies, *The Globe and Mail* described Canada's junior equity markets as the "Wild West."[58] Two features make Canada's capital markets optimal for "overnight sensations":

- comparatively easier listing requirements than for exchanges in some other parts of the world
- hundreds of publicly listed shell companies that are targets of reverse takeovers, which are perceived by some to be back-door shortcuts to equity listings

Our junior equity markets have served Canadians well when it comes to financing the economy's growth engine, namely, early-stage-exploration mineral, oil, and gas companies. However, the features listed above now put Canadian investors at risk when it comes to cryptocurrencies.

According to a new investor-education portal created by the Ontario Securities Commission (OSC), called Get Smarter About Crypto,[59] as many as five per cent of Ontarians are invested in cryptocurrencies, but many lack a basic understanding of how they work and how they are regulated. These investors are particularly vulnerable to over-hyped offerings of still unproven cryptocurrency value propositions.

The OSC recently launched a fake coin offering, called TBA Coin,[60] to educate investors about the risks of investing in initial coin offerings (ICOs). Marketed as "the world's most secure cryptocurrency built on next-generation blockchain technology," investors are "guaranteed" a "10% monthly return." Fortunately, crypto investors falling for the TBA Coin will be lucky enough to have only emotional scars to show for their "investment."

In 2018, CPAB established an internal team to examine the audit implications and to drive audit quality on this new frontier by working with blockchain experts, academics, large and small audit firms, professional bodies, and other Canadian and international regulators.

We learned that audit companies had little guidance for treating the emerging cryptocurrency ecosystem. CPAB felt it needed to provide some direction. We recently published our perspectives on audit risks in some challenging areas and our expectations of how auditors should be addressing those risks. This material is available on CPAB's website.[61]

[58] Natalie Obiko Pearson, Kristine Owram, and Danielle Bochove (Bloomberg News), *Bitcoin, marijuana stock crazes take root in Canada's Wild West* (www.theglobeandmail.com/globe-investor/investment-ideas/bitcoin-marijuana-stock-crazes-take-root-in-canadas-wild-west/article37417558, December 22, 2017).

[59] See Ontario Securities Commission, *Get Smarter About Crypto* (https://getsmarteraboutcrypto.ca, 2019).

[60] See TBA Coin Project Ltd., *TBACOIN: The Blockchain for Audiences* (https://tbacoin.ca, 2018).

[61] Canadian Public Accountability Board, *Auditing in the Crypto-Asset Sector* (www.cpab-ccrc.ca/Documents/News%20and%20Publications/Auditing%20in%20the%20Crypto-Asset%20Sector.pdf, n.d.).

Here are three areas that we think are particularly challenging to audit:

1. **Private-key security**
   Access to the private key that controls a cryptocurrency does not necessarily entail ownership. For example, how would an auditor determine that related companies, each with access to the same private key, are not each pointing their auditor to the same crypto-asset?

   Some good management practices are being discussed. For instance, management might adopt key ceremonies to protect their private keys and to demonstrate to their auditors that the private keys were created in a cryptographically secure manner, and that no one could have made unauthorized copies.

   Auditors will be challenged to obtain enough evidence in the absence of a strong control environment established by management of the entity.

2. **Crypto-exchanges and custodians**
   Companies that transact or hold cryptocurrencies often entrust crypto-exchanges and custodians to safeguard their private keys.

   Auditors are accustomed to a world where the identity of the parties to a financial transaction are known and trusted intermediaries, including financial institutions, payment networks, regulatory authorities and auditors, who act together to protect the integrity of those transactions. In that environment, auditors are able to rely on information received from financial intermediaries as part of their audits.

   However, crypto-exchanges and custodians remain largely unregulated, and the effectiveness of their internal control systems has yet to be meaningfully scrutinized. To our knowledge, no service auditors' reports (i.e., SOC 1 reports) are available to date that attest to the effectiveness of internal controls at crypto-exchanges and custodians. The Wall Street Journal reported in 2018 that hacking-related losses from crypto-exchanges since 2011 totalled $1.63 billion USD.[62] Auditors will be challenged to determine whether cryptocurrencies held in custody by a crypto-exchange exist at year end.

3. **Auditing cryptocurrency transactions**
   Auditors not only audit the ending balance, they audit the transactions recorded throughout the year. They ask whether there was a valid business purpose to the transaction, the name of the counterparty and whether the transaction was accurately recorded.

   These are all questions with no easy answers within the context of the pseudonymous world of cryptocurrencies.

[62] Steven Russolillo and Jeong, Eun-Young, "Cryptocurrency Exchanges Are Getting Hacked Because It's Easy," *Wall Street Journal* (www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000, July 16, 2018).

Beyond understanding the technical nuances of a blockchain, including its cryptography and consensus mechanism, auditors should continue to keep their focus on the bigger picture and assess the business purpose of the transactions.

Humans and machines: the joint audit

At CPAB, we are often asked for our perspective on how to train future audit professionals within the context of any digital disruption that will change how we work and interact with each other. Several scenarios can be developed on how this may roll out. CPA Canada's work on the future of the profession is informative in this regard.[63]

DO YOU THINK THAT DLT WILL MAKE FUTURE AUDITORS' JOBS EASIER OR MORE DIFFICULT?

CAROL PARADINE: I think DLT will make audit easier. When auditors go into a company right now and ask for a selection of transactions, and the company can't find them, there's a lot of back and forth that is very inefficient. Having a centralized mechanism of keeping transactions – whether it's smart contracts or the support for what a particular transaction is – will be both efficient and more effective.

What is certain is that human auditors will be collaborating increasingly with ever-smarter machines. This collaboration will require a different skill set. We have already seen a shift at the audit firms in their recruiting practices. In recent years, the bigger audit firms have been hiring proportionately more students with science, technology, engineering and math (STEM) academic backgrounds to complement their recruits who come from traditional accounting programs. Audit teams of the future will have an increasingly eclectic mix of professionals with diverse backgrounds.

My best advice? I think students and seasoned professionals alike need to embrace the fact that change is the only constant and that learning will be a life-long pursuit.

[63] For more information, search "future of the profession" at Chartered Professional Accountants of Canada (www.cpacanada.ca/search-results?#q=%22future%20of%20the%20profession%22).

An Introduction to Tax Issues for Cryptocurrencies and Potential Blockchain Applications

By Laura Gheorghiu, Partner, Gowling WLG

Guidance is far behind

Many people are surprised to hear that bitcoin and other crypto-assets are taxable. People commonly thought that buying bitcoin, for example, took them out of the legal system and the taxation system, and that every trade after the first purchase had nothing to do with tax. There are many issues that complicate the taxation of these transactions. This paper briefly introduces a few of these issues as well as some future blockchain applications for tax compliance.[64]

Characterization of crypto-assets may guide taxation

How crypto-assets are used or created may be driving how they are taxed. In Australia,[65] for example, taxation depends on whether the cryptocurrency was created through mining activities or used for:

- investment
- trading
- carrying on a business
- conducting an exchange

In Canada, the Canada Revenue Agency's (CRA) initial pronouncements in 2014 dealt only with bitcoin and the question of how to tax transfers of bitcoin. At that time, no one, including the CRA, could envision the development of so many different kinds of applications

[64] For more comprehensive information, see Mariam Al-Shikarchy, Steven Baum. and Laura Gheorghiu, *Canada: Canadian Taxation Of Cryptocurrency ... So Far.* (www.mondaq.com/canada/x/648030/fin+tech/Canadian+Taxation+Of+Cryptocurrency+So+Far, November 20, 2017 and https://gowlingwlg.com/en/insights-resources/articles/2017/canadian-taxation-of-cryptocurrency-so-far/?lang=en-CA?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original, November 20, 2017).

[65] Australian Securities & Investments Commission's (ASIC's) *Moneysmart*, "Cryptocurrencies" (www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies, 2018).

of blockchain, nor the creation of so many different types of crypto-assets. The CRA has recently released compliance guidelines on cryptocurrency[66] but has limited types of discussion to two aspects of digital currencies:

- Payment method: Where it is used to pay for goods and services, the transaction is considered to be a barter because digital currency is not legal tender.
- Commodity: Whether it is bought, sold, or traded on an exchange, the currency is treated as a commodity.

Little guidance has been provided for other kinds of blockchain applications.

WHAT ARE YOUR THOUGHTS ON THE DISRUPTION OF TECHNOLOGY TO THE CAPITAL MARKETS?

LAURA GHEORGHIU: From the legal side, the perception, at first, was that if people used blockchain technology, they could avoid regulation. The result was that they didn't. **Many times we forget how important the intermediaries are to protecting us, not just from ourselves, but from others we cannot control.** A good example in Québec was the Plexicoin ICO. It raised $5 million based on a hoax: there was nothing behind it at all. It was up to the SEC (U.S. Securities and Exchange Commission), the AMF (Québec securities commission) and the police to go after the founders of the company and seize some of the crypto.

Then what happened, when the individual wanted to pay bail, the judge said, "Here's a laptop, there's the bailiff. You will transfer your coin from your wallet into the court's wallet, and then you can go." That's really what happened: a very practical answer to the difficult question of "how do we seize someone's property when there is no central authority to assist?"

Initial coin offerings (ICOs)

Consider, for example, the money raised by ICOs. The cryptocurrency issued often acts like a share rather than a payment token. So, an ICO may be more like a security (i.e., an investment in some sort of future business with the hope the tokens held will increase in value as the underlining business grows).

[66] Canada Revenue Agency (CRA). *Virtual Currency.* (www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency.html, June 26, 2019).

But ICOs may differ from the normal issuance of shares because there is no corporation recognized under corporate law that is actually issuing the shares. Instead, software may be issuing a token whose value may go up and down based on what people trading it on a secondary market think it is worth.

Utility and hybrid tokens

Canada's first securities-compliant ICO issuance was the impak coin. The coin accesses a platform that allows consumers to purchase goods and services offered by certain companies that fit into the definition of impacting the economy (i.e., those that are environmentally friendly, do good, have a positive social impact, etc.).[67] Purchases are rewarded with impak coins that can be spent at these same businesses. Not so much with impak coin – because its issuers call it a stable coin – but with others like it, the hybrid function comes from its being used (i.e., having utility) to buy something, but also because it can be held to trade and accrue in value, more like an investment.

Determining tax treatment can be complicated

Income tax

How should crypto-asset transactions be valued? What if transactions involve more than one exchange? Which of the exchange values should be used to determine the tax? Since earning the profits might have required thousands of trades, must the fair market value of every trade be determined? What would that cost? These are the sorts of question for which there is currently little guidance.

If every crypto-token is a commodity, and every disposition is considered a barter by the CRA, then a business that issues a token and raises, say, $50 million for that token, has revenue that should be taxed. If the business had issued shares, it would have raised tax-free dollars, but with an ICO or initial token offering (ITO), it has taxable income of $50 million. This has been a surprise to many. While the tax authorities may not have answered these questions yet, the CRA and Revenu Québec have assembled audit teams for 2019.

Sales tax

A huge number of issues exist around the application of sales taxes to blockchain solutions, and many have not yet begun to be addressed by the tax authorities. Some examples of this follow.

[67] For more information, see impak Finance. *Cryptocurrency : Coded to support the impact economy development* (www.impak.eco/en/impak-coin, 2019).

Normally, a sales tax is an end-consumer tax, and everybody else in the process gets a credit. To get a credit, entities must be registered for tax and have the right supporting documentation. In Canada, intermediaries collect sales tax as agents of the government; every business involved in commercial activity must collect sales tax on all goods and services they supply in Canada. An exception applies when sales are made to foreign buyers or the goods or services are sourced outside Canada. The entity must, however, prove the goods or services are not subject to sales tax.[68]

In this context, are dispositions of cryptocurrencies in the course of commercial activities subject to tax? If so, which factors should be taken into consideration when determining whether the supply[69] is made inside or outside Canada? How can foreign vendors be identified? Who should collect the tax: exchanges or their users? How can adequate supporting documentation be provided? Et cetera.

Revenu Québec took the more aggressive position that supplies of cryptocurrencies are subject to sales tax. However, presumably realizing the many unsolved questions, it withdrew its written interpretation. Uncertainty, therefore, remains.

Most importantly, this uncertainty puts Canadian sellers of cryptocurrencies at a distinct disadvantage. If their supplies are subject to sales tax, with no provable exceptions, and no way for buyers to claim back their taxes, the costs of cryptocurrencies sold by Canadians are effectively made higher than those sold by others.

Using blockchain for tax compliance

Sales tax

If a smart contract on a blockchain could calculate and automatically remit tax, forms and compliance issues would be things of the past. The needed level of trust in the technology and in government agents who have access to that information would be quite significant, however.

More likely, in the short-to-medium term, tax authorities will look to replacing tax-collecting intermediaries with blockchain applications, for good reason:

- Most intermediaries do not want to collect and remit tax.
- Intermediaries can often be the source of lost tax revenue through improperly collecting the tax, failing to remit the tax collected, or claiming credits for which they do not qualify.
- Intermediaries are the most easily replaceable part of the tax-collection process.

[68] Editor’s note: Under Canada’s *Excise Tax Act* (ETA; see https://laws-lois.justice.gc.ca/eng/acts/e-15), a person is not considered a non-resident if living in Canada.

[69] Editor’s note: *Supplies* is the term for all things subject to sales tax in Canada. Supplies other than sales (e.g., leases) are taxed.

Instead of the seller having to register for, collect, and remit sales tax, for example, a blockchain function, perhaps in a smart contract, would withhold a percentage of the business's proceeds and remit it on behalf of the purchaser (i.e., the party actually required to pay the sales tax).

When and how such solutions will be implemented remains to be seen. One thing is certain, however: the intersection of blockchain technology and tax is forcing us to reconsider how and when we should collect taxes in ways even more varied than occurred when e-business was first emerging.

Social Innovation and the Blockchain

By Marc Lijour, Co-Founder of ColliderX and Founder of the Metamesh Group

The paper printed here is a condensed version of his full article, which can be found in the online ideas platform, Medium.[70]

What is social innovation?

"Social innovation is the process of developing and deploying effective solutions to challenging and often systemic social and environmental issues in support of social progress."[71]

Social innovation is a process that pushes out beyond the boundaries of any single sector or organization. It happens when stakeholders collaborate to co-create a better system, and when they empower actors to implement it.

Social innovation focuses on social and environmental, not just financial improvement (i.e., the triple bottom line). The "triple bottom line (TBL) is a sustainability framework that examines a company's social, environment, and economic impact,"[72] emphasizing that firms have a duty to care about the people, regions, and environment they work with and within to maintain livable conditions for their customers and employees alike. TBL influenced sustainability reporting standards (e.g., the GRI standards[73]), environmental, social, and governance (ESG) performance measures, and more, but now, 25 years after coining the term, John Elkington is worried that it is just another accounting tool and has lost the force of the original idea, which was to "[encourage] businesses to track and manage economic (not just financial), social, and environmental value added – or destroyed."[74]

I think Elkington would be encouraged by people driving social innovation, including individuals, communities (groups and associations), and leaders of private and not-for-profit organizations. Organizations can make commitments and drive social innovation, but they are ultimately driven by individuals (one or many) who give them a purpose.

[70] Lijour, Marc, *Social Innovation and the Blockchain* (https://medium.com/@marclijour/social-innovation-and-the-blockchain-ed862ba75823, June 10, 2019).

[71] Stanford Graduate School of Business, Center for Social Innovation, *Defining Social Innovation* (www.gsb.stanford.edu/faculty-research/centers-initiatives/csi/defining-social-innovation, n.d.).

[72] John Elkinton, *25 Years Ago I Coined the Phrase "Triple Bottom Line." Here's Why It's Time to Rethink It* (https://hbr.org/2018/06/25-years-ago-i-coined-the-phrase-triple-bottom-line-heres-why-im-giving-up-on-it, June 25, 2018).

[73] The GRI standards were the "first global standards for sustainability reporting." See GRI Standards (www.globalreporting.org/standards, n.d.).

[74] John Elkington, *ibid.*

The major problem I observed in my public sector and not-for-profit career was the centralization of decisions in time and space. All the decision makers for an issue need to agree on the same thing at the same time. If that sounds hard, that is because it is. In the public sector, getting more than five decision-makers in a room at the same time was already a serious challenge and became exponentially more difficult as more stakeholders were involved and issues became polarizing. Under these conditions, only the simplest and smallest steps forward could ever be taken.

What if we could democratize decision-making by pushing it to the level of individuals?

Enter blockchain

Blockchain is a technical solution that shines for:

- managing and implementing decision-making through automated consensus
- creating incentive structures that can nudge participants into behaving constructively
- creating trust and transparency by securing access, enabling mechanisms of proof, and making records tamper-resistant[75]

The ethos of much of the blockchain community is against the Establishment, the "too big to fail" corporations, and the oppression of common folk who have become the "product" rather than the beneficiaries of the digital world. Many in this community believe in equal rights, in collaboration, in transparency, and in equity. It is no surprise that social innovation has been one of the first areas of intense progress in the blockchain space.

Social innovations using blockchain technology have emerged in financial services, social good works, environmental protection, and many other areas. A few examples not covered by previous speakers are covered here.

Wealth and financial services

My first use of Bitcoin was to send money almost instantaneously to my family abroad, but commissions charged were close to 15% (too high in my opinion) and could be as high as 30% in the poorer countries (where transfer options were more limited: a perverse effect of the law of supply and demand). Over the last few years, challengers have launched services at much lower commission rates: Abra, TransferWise, Xoom (a PayPal service), and many others. At the time of writing (April 2019), the World Bank reports that the average cost of sending remittances is now just under 7% of the amount sent.[76] Bitcoin still works for

[75] For more information on how blockchain properties work almost magically to create a layer of trust in business and social activities, see Paul Vigna and Michael Casey, *The Truth Machine: The Blockchain and the Future of Everything* (New York: St Martin's Press, 2018), for history, main characters, and increased understanding of the blockchain community.

[76] The World Bank, *Remittance Prices Worldwide: Making Markets More Transparent* (https://remittanceprices.worldbank.org/en, [2019 data]).

transfers and is now easier to use with the popularization of Bitcoin ATMs (nearly 700 in Canada alone).[77] However, the newer applications, using fiat currencies, are easier to use than Bitcoin, because users do not need to understand, manage, or deal with crypto-assets or their taxes. In keeping with social innovation, one of the challengers, TransferWise, was founded "with the vision of making international money transfers cheap, fair, and simple."[78]

According to the International Monetary Fund, "[on] average, the world's debt now exceeds $86,000 in per capita terms, which is more than 2½ times the average income per-capita."[79] Yet, while debt levels remain high, wealth is increasingly concentrated in fewer hands. The number of billionaires has doubled since the last financial crisis [2008], according to Oxfam.[80]

Many in the cryptocurrency community believe that blockchain will democratize investment and allow regular people to earn the otherwise inaccessible economic rent flowing from capital. Initial Coin Offerings (ICOs) and Security Token Offerings (STOs) could be the poor person's IPO. New financial instruments, like cryptocurrency-backed debt and derivatives, could contribute to democratizing this field and disrupting traditional banking. The Celsius Network,[81] for instance, facilitates fiat conversion of crypto-assets and facilitates peer-to-peer borrowing and lending on blockchain.

Social good works

Some blockchain applications improve the human condition across the globe.

Beyond financial literacy and financial inclusion, for those who do not have a lot of capital (i.e., more debt than savings), blockchain may help them get a better return on their work. For example, many creators, particularly artists, have difficulty capturing the value of their labours. Many intermediaries (galleries, studios, publishers, managers, etc.) feed on their margin, but the digital revolution, through free viewing of their work, has further limited their ability to even get paid. Access Copyright, a Canadian not-for-profit organization, helps writers, visual artists and publishers "remix and share published content

[77] Coin ATM Radar, *Bitcoin ATMs in Canada* (https://coinatmradar.com/country/38/bitcoin-atm-canada. 2019).

[78] TransferWise, *The TransferWise Story* (https://transferwise.com/ca/about/our-story, 2019).

[79] Samba Mbaye and Marialuz Moreno Badia, *New Data on Global Debt* (https://blogs.imf.org/2019/01/02/new-data-on-global-debt, January 2, 2019).

[80] Oxfam, *Public Good or Private Wealth?* [Oxfam Briefing Paper] (www.oxfam.org.nz/sites/default/files/reports/Public%20Good%20or%20Private%20Wealth%20-%20Oxfam%202019%20-%20Summary.pdf, January 2019).

[81] See Celsius Network Inc. (https://celsius.network, 2019).

while ensuring appropriate rewards."[82] It works with the "creator-focused innovation lab Prescient,[83] which has launched Attribution Ledger[84] that keeps track of the relationship between creators and their works of art by using blockchain and machine learning.

What if singers and musicians could self-publish and avoid both traditional intermediaries and newer ones, recently revealed to pay little to artists?[85] A few years ago, ConsenSys[86] funded Ujo-Music,[87] which uses Ethereum to connect artists and fans directly.

Hala Systems[88] is a U.S. (for-profit) social enterprise aiming to protect populations living in war zones. The team uses blockchain and several emerging technologies to give early warning of threats and to provide immutable evidence for assets and for events that take place, so that people can eventually be held accountable.

NeedsList[89] is developing a registry for humanitarian aid by using blockchain to maintain a decentralized list of much needed resources such as food, clothing, and volunteers required for disaster response. **NeedsList** was a finalist in the Social & Culture Impact category at the 2019 SXSW Interactive Innovation Awards.[90]

Millennials are setting new standards through their consumption and relationship with brands. WhatRocks, with its motto, "Have fun, do good,"[91] aims to disrupt the advertising industry by becoming the leading label for social impact advertising. Consumers earn Rocks (i.e., coins on blockchain) when they view ads showing the WhatRocks label. They can use these Rocks to make donation and to get free or discounted event tickets. Blockchain makes the use of the Rocks cryptocurrency secure and efficient.

[82] Access Copyright, *Access Copyright's Affiliates: Canada's Storytellers, Chroniclers and Educators* (www.accesscopyright.ca/creators, 2019).

[83] See Prescient, *Who We Are* (https://prescientinnovations.com, 2018).

[84] Prescient, *Project Information: Attribution Ledger* (https://prescientinnovations.com/attribution-ledger, 2018).

[85] Kabir Sehgal, *Spotify and Apple Music Should Become Record Labels So Musicians Can Make a Fair Living* (www.cnbc.com/2018/01/26/how-spotify-apple-music-can-pay-musicians-more-commentary.html, January 26, 2018).

[86] ConsenSys (https://consensys.net, 2019).

[87] See Ujo (https://ujomusic.com, 2019).

[88] See Hala Systems Inc. (https://halasystems.com, 2018).

[89] See Needslist (https://needslist.co, 2019).

[90] Ari Roth, *2019 SXSW Interactive Innovation Awards Finalists & Hall of Fame Inductee Kimberly Bryant* (www.sxsw.com/interactive/2019/announcing-the-2019-sxsw-interactive-innovation-awards-finalists-and-hall-of-fame-inductee-kimberly-bryant, January 22, 2019).

[91] See WhatRocks, *About WhatRocks Foundation* (www.whatrocks.co/en/about-whatrocks-foundation, n.d.).

The environment

Many blockchain projects aim to improve the environment. During my work at ConsenSys, I encountered a growing number of projects on carbon pricing across several continents. Blockchain allows the measurement and tracking of carbon units that can be sold on peer-to-peer market places. It allows price discovery and near immediate settlement. Blockchain is ideal to enable those market places.

In December 2018, the Bounties Network, ConsenSys Social Impact, and Coins.ph partnered to launch a pilot project called *Bounties for the Oceans* to incentivize people to clean up Manila Bay in the Philippines.[92] Participants received the equivalent of US$10 in cryptocurrency for picking up trash. The Bounties Network has a mechanism to manage the proof of (human) work so that people get paid fairly, but the small number of smart phones, poor Internet connections, unreliable or expensive data plans were eye-opening hurdles to the experiment. The project was important because it provided lessons about those hurdles for future projects.

To protect the fish population, World Wildlife Fund has worked with Viant,[93] a custom-blockchain builder, on an initiative to demonstrate food provenance, because, unfortunately, much fish labelled tuna is not really tuna. The *Bait to Plate* project[94] helps consumers understand what they are eating.[95] Again, blockchain creates an ideal record of the facts, such as what was caught, when it was caught, how and where it was processed.

WHAT ARE YOUR THOUGHTS ON SOCIAL INNOVATION AROUND IDENTITY AND INCLUSION?

MARC LIJOUR: There's a concept of **self-sovereign identity where people own their own data and can decide to share that data with people they want on a need-to-know basis.** People might authorize organizations to use their data and even sell it but may want remuneration in return. That is possible with blockchain. Several large organizations, including some telecommunications companies (telcos) are thinking about providing this remuneration.

[92] Mark Beylin, *Bounties For The Oceans: Incentives to Change the World* (https://medium.com/bounties-network/bounties-for-the-oceans-incentives-to-change-the-world-8f3429fd01e9, December 10, 2018).

[93] See Viant (https://viant.io, 2018).

[94] World Wildlife Fund, *From Bait to Plate: Preventing Illegally Caught Seafood from Entering Our Food Chain* (www.worldwildlife.org/pages/bait-to-plate, 2019).

[95] CNN, *What is Blockchain?* [Video] (www.cnn.com/videos/cnnmoney/2018/05/11/blockchain-database-cryptocurrency-viant-pangea-sebastian.cnn, [2019]).

Doing more

I have mentioned only a few examples of social innovation projects leveraging blockchain. They are only the beginning. There are 2,000 applications (DApps) on the public Ethereum network today (the largest concentration, as far as I know). There will be many more. Looking to the future, this is what I see and hope for:

- **Social innovation:** Social innovation is becoming an inseparable part of how business leaders and people in general envision work, live, and play in the future.
- **Blockchain:** The ethos of the blockchain community is aligned with the spirit and methods of social innovation. Blockchain draws the best technical and social practices from the open-source community and post-2008 social activists.
- **We are all in:** Social innovation requires everyone to participate. Blockchain, pushing decision-making and ownership to the edge of the network, empowers every one of us to take control.
- **Barriers to innovation are low:** Technology has given everyone a voice through social media, and the ability to create an app from a dorm room and to deploy it in the cloud with lunch money. Grants are available from not-for-profit organizations such as the Ethereum Foundation[96] and the AION network[97] to improve blockchain technologies. The big IT organizations continue to offer grants for social innovation projects. More importantly, investment in social ventures is rising.

[96] Ethereum Foundation, *Ethereum Foundation Grants Program Wave 5* (https://blog.ethereum.org/2019/02/21/ethereum-foundation-grants-program-wave-5, February 21, 2019).

[97] AION, *Bounties & Grants* (https://aion.network/bounty, [2019]).

Blockchain as a Tool to Advance Sustainability

By Michael Torrance, Chief Sustainability Officer, Associate General Counsel, BMO Financial Group

This article, which first appeared in its original form in the September 2018 edition of the Canadian Mining Journal*, has been augmented here with material from Michael Torrance's presentation. It is included with permission from the* Canadian Mining Journal*.*

Introduction

Blockchain has been hailed as a technology as revolutionary as the Internet. Does it have any application in the sustainability space? The answer is "yes," though exploration of potential applications is only just beginning.

Blockchain is most widely associated with cryptocurrencies like bitcoin or platforms like Ethereum, but these represent only a small part of the technology. Blockchain is an (essentially) incorruptible and highly decentralized ledger. Whereas formerly a record of transactions would be stored on a single proprietary information system or computer, a blockchain system is stored across many. Each record or block on a blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data. The record is permanent and is resistant to modification of the data, in part because the modifications would have to happen across multiple distributed ledgers all at once. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks.

In essence, the blockchain provides a permanent, permissionless, public and transparent record of transactions or other activities.

Blockchain devotees see the technology as socially revolutionary because it allows for the disintermediation and decentralization of formerly highly centralized processes.

Whereas a transaction or contract would formerly need to be administered by banks, lawyers, governments or other intermediaries, blockchain has the potential to create a disintermediated economy where users can leverage technology to transact autonomously.

Blockchain and sustainability

In 1970, New York Times Magazine published an article entitled, *The Social Responsibility of Business Is to Increase Its Profits*, by economist Milton Friedman. Unfortunately, the title is often used as a dictum but misquotes Friedman. Within the article, Friedman qualifies the title's message by saying that business executives have responsibilities to the owners of a business, and

"[t]hat responsibility is to conduct the business in accordance with [the owners'] desires, which generally will be to make as much money as possible while ***conforming to the basic rules of the society, both those embodied in law and those embodied in ethical custom.****" [Emphasis added.]*

Stakeholders have emerging expectations around corporate sustainability that embody Friedman's qualifications, and may go beyond them, yet sustainability is not easily proven. If a company is viewed as sustainable, what does that mean? Companies put information about their sustainability practices into the marketplace but not through any central authority. Stakeholders must trust this decentralized information in order to evaluate it. The combination of decentralized information and trust is similar to the characteristics of a blockchain. So, while blockchain may not disrupt the field of sustainability, there might be synergy between them.

The application of blockchain to advance sustainability is the subject of much interest in the blockchain community. For example, the Blockchain for Social Impact Coalition (BSIC) [98] is an initiative of ConsenSys,[99] a "venture production studio" based in Brooklyn. BSIC incubates, develops, and implements blockchain products and solutions that can address social and environmental challenges across the United Nation's Sustainable Development Goals.[100]

The Bounties Network,[101] part of BSIC, aspires to be "a decentralized social impact contribution network," and sees charities becoming the administrators of *bounties* (i.e., rewards for accomplishing tasks) rather than funds. Bounties are operated as social contracts on a blockchain. They reduce the blind trust donors put in single organizations like charities and reduce misuse of donations by rewarding organizations for completing work (i.e., proof of action) and allowing donors "to contribute directly to a cause, rather than funneling money through a third party."[102] Social impact bounties through the Bounties Network, will focus on things like:

- financial inclusion
- supply chain

[98] Blockchain for Social Impact Coalition (BSIC) (https://blockchainforsocialimpact.com, n.d.).

[99] ConsenSys (https://consensys.net, 2019).

[100] United Nations. *Sustainable Development Goals* (https://sustainabledevelopment.un.org/?menu=1300, n.d.).

[101] Simona Pop, *How Blockchain-Based Bounties Can Reinvent Our Social Impact Systems and Incentivize Action* (https://medium.com/bounties-network/how-blockchain-based-bounties-can-reinvent-our-social-impact-systems-and-incentivize-action-e60d7f571e6, April 12, 2018).

[102] *Ibid.*

- identity and vulnerable populations
- energy and environment

Even before its work with the BSIC, ConsenSys actively supported projects like Viant's[103] "partnership with the World Wildlife Fund to prototype [an] asset-tracking and supply chain modelling platform"[104] to track and trace fish caught in the South Pacific. The initial effort resulted in a "fully-traceable [fish] product, geo-located, tracked, and digitally signed for at every juncture on its journey from the oceans of Fiji"[105] to dinner plates at a New York conference on blockchain.

The potential for supply chain track-and-trace on a public, transparent, and highly secure public ledger has application far beyond the fishing industry. In the mining sector, for example, such technology could facilitate local procurement initiatives or facilitate the tracing and tracking of potential conflict minerals, which is already being done for raw-cut diamonds by a start-up called EverLedger.[106] The possibilities are immense and only beginning to be explored.

Perhaps blockchain-based executable contracts, like those being developed by the start-up OpenLaw,[107] a free legal repository, could be developed alongside community engagement initiatives and impact benefits agreements. Blockchain characteristics would be valuable in promoting transparency and providing accountability where trust and integrity are essential in the implementation of such agreements.

Yet another application of blockchain is in the development and tracking of "reputation," including corporate reputation regarding sustainability. A multi-million dollar industry already exists around environmental, social and governance (ESG) ratings, which are used by asset managers and investors in assessing the sustainability of their investment companies. Blockchain could improve and make such ratings processes more transparent and decentralized. For example, "token curated registries" built on blockchain can curate lists of just about anything. An example already in operation is the adChain Registry,[108] which is "a community-curated list of ad-supported websites (domains)," compiled through the use of an Ethereum-based cryptocurrency called adToken (ADT). AdChain participants are incentivized to rationally include or reject websites from the registry based on the merits of ad performance and inventory quality by using purchased ADT to vote for proposed sites considered for inclusion on the registry. Applied in the sustainability context, this technology

[103] Viant, a ConsenSys "spoke" is a technology-based advertising company. See Viant (www.viantinc.com, 2018).

[104] ConsenSys, *Watch How Treum Tracks Sustainable Fish from Bait-to-Plate with Blockchain Tech* (https://media.consensys.net/watch-how-viant-tracks-sustainable-fish-from-bait-to-plate-with-blockchain-tech-99ff46e4f43e , July 6, 2018).

[105] *Ibid.*

[106] See Everledger (www.everledger.io, 2018).

[107] See OpenLaw (https://openlaw.io, 2019).

[108] See adChain, *The adChain Registry* (https://adchain.com, 2019).

could develop lists of the world's most sustainable companies (i.e., companies that can be trusted in the context of stakeholder or community engagement, that provide acceptable sustainability disclosure or that list quality green or social bonds). Unlike preceding approaches to developing such lists, blockchain processes would not be centralized, proprietary and opaque, but rather could be open, transparent, and populated with the wisdom of a wide market of experts.

Blockchain-based prediction market technology (e.g., the prediction market tool Gnosis[109]) could be applied in the ESG-ratings space to develop real-time, company-specific ESG ratings usable by investors, through market mechanisms. Such a mechanism would increase:

- ability of investors who use such data to participate in the generation of the rating
- collaboration across the marketplace
- transparency of the process

Companies could use the real-time data to build key risk indicators or to identify instantaneously how events or news are impacting their reputation for sustainability.

TO WHAT DEGREE DO YOU BELIEVE THE TRANSPARENCY INTRODUCED BY BLOCKCHAIN WILL IMPACT THE NEED FOR REGULATION, AND WHAT DO YOU THINK ITS IMPACT ON SUSTAINABILITY REPORTING WILL BE?

JUST IN GENERAL, DO YOU THINK BLOCKCHAIN WILL BOLSTER THE GENERAL PUBLIC'S TRUST IN CORPORATIONS?

MICHAEL TORRANCE: I think regulators are struggling with how to regulate sustainability reporting, if at all. There is a proliferation of standards now, and there's a thing called survey fatigue: [organizations] must review many different disclosure frameworks and disclose in many different ways about the same information.

If used the right way, blockchain could be used to create ways to disclose that are simpler than the current ways. I think regulators would like that, because they want more transparency, but they just don't always know how to do it.

Would blockchain increase trust? I think greenwashing, for example, was a problem where disclosure was done, at first, because it was good PR. Now, sustainability disclosure is moving to something much more codified, with clearer expectations about what it should look like. There's an emphasis on metrics, and there's interest in tying it to financial materiality. All of that would be facilitated by collecting information better and putting it on a very transparent system that cannot be manipulated by intervention. I think blockchain could *increase trust* if that were to happen.

[109] See Gnosis (https://gnosis.io, 2019).

Technologies are even being developed around blockchain to facilitate dispute resolution. One day company grievance mechanisms might be managed without cost through decentralized blockchain-based staking and arbitration protocols. This technology could be built on top of blockchain-based audit protocols (modelled after current methodologies for human rights, labour standards or environmental and social sustainability audit frameworks) to allow for claims of compliance to be publicly and transparently recorded and subject to challenge from interested stakeholders.

These potential uses of blockchain are merely the tip of the iceberg and depend for their development only on how creative developers and sustainability professionals can be in finding potential uses.

About the Authors, Speakers and Panel Moderators

Technology pillar

Dr. Garrick Hileman, PhD

Head of Research at Blockchain.com and Researcher at the London School of Economics

Keynote Speech: Blockchain Technology – Past, Present and Future

Dr. Garrick Hileman completed his PhD in economic history at the London School of Economics. He is best known for his research on monetary and distributed systems innovation, particularly cryptocurrencies and blockchain technology.

Dr. Hileman has been ranked as one of the 100 most influential economists in the U.K. & Ireland. He is regularly invited to share his research and perspective with public sector institutions, including the CIA, U.S. Army and Naval War Colleges, Federal Reserve, Bank of England, and the Financial Stability Board, as well as media, including the BBC, CNBC, FT, WSJ and NPR. Garrick is frequently sought as a speaker.

Notable cryptocurrency and blockchain research publications include the co-authored 2017 *Global Cryptocurrency Benchmarking Study* (University of Cambridge) and the co-authored 2017 *Global Blockchain Benchmarking Study* (University of Cambridge). He also created and published the CoinDesk *State of Bitcoin* and *State of Blockchain* reports from 2013-2016. Garrick's other research interests include sovereign debt, financial crises, financial repression and prudential regulation, black markets and systemic risk.

Andreas Veneris, PhD

Professor, Computer Engineering Electronics, Department of Electrical and Computer Engineering, University of Toronto

Challenges in the Era of Crypto-Decentralization: Where Do We Go from Here?

Dr. Andreas Veneris is a Connaught Scholar and Professor at the Department of Electrical and Computer Engineering, cross-appointed with the Department of Computer Science at the University of Toronto. He is an alumnus of the Japanese Society for the Promotion of Science, hosted as visiting professor by the University of Tokyo (2010-11). In 2006-2016, he held a joint faculty position at Athens University of Economics and Business (Department of Informatics). He holds a PhD from the University of Illinois, Urbana-Champaign, where he was also visiting faculty in 1998-99 before joining University of Toronto. His research is in formal methods for verification of smart contracts and systems, algorithms and crypto-economics, and ledger-based technologies.

He has published more than 130 papers in premier IEEE/ACM conferences and journals; he received a 10-year Best Paper Retrospective Award (IEEE/ACM Asian South Pacific Design Automation Conference, 2014); he holds multiple patents, and he was nominated for the Franklin Institute Bower Award and Prize for Achievement in Science in verification by Turing Award recipient Professor Stephen Cook. Andreas has been involved with the vision and deployment of Ethereum along with its founding team since 2013. He also founded the Blockchain Research Seminar Series at the Fields Institute of Mathematics in 2017.
In 2006, he led Vennsa Technologies in Series A funding to commercialize research in formal methods serving the Tier 1 semiconductor industry. At an earlier stage of his life, he worked on the development of Mosaic (Netscape) and later he was member of the team that performed the first-ever webcast (37th Grammy Awards, March 1, 1995), an event acknowledged in the American Congress.

Peter J. Patterson

IBM Blockchain – Canada Market Leader

An Introduction to IBM's Blockchain for Business

Peter Patterson is the Blockchain Market Leader for IBM, responsible for strategy and growth in Canada. Since 2015, Peter has worked on dozens of projects spanning start-ups and enterprises alike, aligning business value, governance, and operational models.

Peter is passionate about developing blockchain-enabled business networks and new forms of cross-industry value exchange in both the private and public sectors. Prior to joining the blockchain team, Peter led the IBM Cloud team in the financial services industry.

Governance pillar

Pat Chaukos

Deputy Director, Ontario Securities Commission (OSC)

OSC LaunchPad and Innovation

Pat Chaukos is leading the Ontario Securities Commission's initiative, the OSC LaunchPad. This initiative is committed to modernizing regulation to support fintech innovation.

Pat has extensive experience with novel fintech businesses. Before leading OSC LaunchPad, Pat managed a team that focused on the exempt market, working with many new business models including online trading platforms, lending platforms, and crowdfunding portals.

Pat holds a Doctor of Laws (JD) from Osgoode Hall Law School and is a Chartered Professional Accountant (CPA). Before joining the OSC, Pat was Vice-President, Risk Management & Compliance at Royal Mutual Funds and RBC Investments, and has practised as both a lawyer and a chartered accountant on Bay Street.

Carol Paradine

CEO, Canadian Public Accountability Board (CPAB)

Accounting and Auditing in a Blockchain-Enabled World: Audit Regulation on the New Frontier

Carol is the Chief Executive Officer of the Canadian Public Accountability Board. Prior to assuming the leadership role at CPAB, Carol was a partner in a major international firm. She specialized in assurance and advisory services for public companies as well as complex accounting and financial transactions. Carol served on the firm's board of directors and executive committee with roles that included Managing Partner – Leadership Development and Succession, Managing Partner – Prairie Region, and Acting Chief Financial Officer.

Community service is equally important to Carol, with roles that have included Chair, Manitoba Chambers of Commerce; President, Alzheimer Society of Manitoba; board and audit committee member, Alzheimer Society of Canada; board and audit committee member, Centreport Canada; board and finance committee member, YMCA-YWCA National Capital Region; board member, Innovate Manitoba; board member, Harmony House; and advisory board member, Carleton University School of Business. She also coached youth soccer for a number of years and was a lecturer and coach at Carleton University.

Carol has a Bachelor of Commerce degree, along with her Chartered Professional Accountant and Certified Public Accountant designations from Canada and the United States. She speaks both official languages.

Laura Gheorghiu

Partner, Gowling WLG

An Introduction to Tax Issues for Cryptocurrencies, and Potential Blockchain Applications

Laura is a tax partner in the Montréal office of Gowling WLG, and a member of the Tech and Blockchain & Smart Contracts Groups. Laura's practice focuses on cross-border (inbound and outbound) investment structures, corporate reorganizations and advising domestic and multinational private equity funds. She is also developing expertise in the application of taxation rules to the technology space, in particular, to providers of e-business and blockchain technology solutions.

Laura has also advised on issues with respect to employer payroll and pension obligations; Federal and Québec value-added taxes (GST/HST and QST); and Québec commodity taxes (in particular, with respect to fuel and alcohol). Her dispute resolution practice includes representing clients in their dealings with the Canada Revenue Agency and the Québec Revenue Agency at the audit and notice of objection stages, and preparing voluntary disclosures on income tax and sales tax issues.

Laura has been recognized as a Women in Tax Leader 2017 by the International Tax Review.

A frequent writer and speaker at the Canadian Tax Foundation (in particular, on subjects of international financing and the impact of bilateral tax treaties), she serves as an editor of the Taxation of Executive Compensation and Retirement Journal and is a co-author of the Taxation Chapter of the Business Guide to Environmental Law. She is also a member of the Canadian Tax Foundation Montréal Young Practitioners Steering Committee.

Laura holds a degree from HEC Montréal (LLM – fisc.) where she also received the CFT Awards for highest average in the LLM (Tax) program and two scholarships (the PSB Biosjoli merit scholarship and the board of graduate studies diplomas' merit scholarship). She also earned a degree from the McGill University (LLB and BCL) where she was distinguished with the Stikeman Elliott/Carswell National Tax Award.

Social innovation pillar

Marc Lijour

Co-founder of ColliderX and founder of the Metamesh Group

Social Innovation and the Blockchain

Marc Lijour helps people and organizations realize their full potential by leveraging technology and freedom to innovate. In 2018, he joined ConsenSys, the largest Blockchain company, with 800 employees in 30 countries, to bring Ethereum to the enterprise market. He believes Ethereum, with its ability to manage private and public blockchains, is best positioned to fulfill the promise of an Internet of value that is globally inclusive and fair to firms and individuals alike.

Marc holds degrees in Mathematics and Computer Science, as well as an MBA (in the Management of Technology and Innovation) and certifications in Education. His active free-software evangelism of the last 20 years has led him to work on research projects with Linux publishers and system integrators. He has more than 10 years' experience in senior roles, helping large institutions, particularly in the public sector, develop and implement innovative solutions, policies, and programs.

Marc serves on a number of not-for-profit boards, including the Information and Communications Technology Council (ICTC), the Toronto French Business Network (TFBN), TechConnex, and last, but not least, ColliderX, the world's first Open Source R&D Hub focusing on Blockchain and related technologies, such as AI and VR, which he co-founded in 2017. He has recently launched Metamesh Consulting, a new practice focusing on making business, life, and society more purposeful and impactful by leveraging new technologies such as blockchain.

Michael Torrance

Chief Sustainability Officer, Associate General Counsel, BMO Financial Group

Blockchain as a Tool to Advance Sustainability

Michael Torrance is Chief Sustainability Officer and Associate General Counsel of BMO Financial Group. Michael joined the bank from Norton Rose Fulbright LLP where he was a Partner in their Toronto office. His experience includes risk advisory on international standards of environmental and social risk management and human rights due diligence. Michael has authored guides on international environmental and social governance frameworks, including the Equator Principles and IFC Performance Standards on Environmental and Social Sustainability. A focus of his work has been the application of these standards in the banking and finance context. As Chief Sustainability Officer, Michael leads strategy and implementation of sustainability governance at the enterprise level of BMO Financial Group, including ESG reporting and stakeholder relations. Michael sits in the Corporate Affairs group and reports to the corporate secretary and general counsel of BMO.

Panel moderators and conference organizers

Yue LI, PhD

Associate Professor of Accounting, University of Toronto

Yue Li is an Associate Professor at the University of Toronto with cross-appointments at the Institute for Management & Innovation and Joseph L. Rotman School of Management. He received his MBA from the University of Toronto and his PhD from Queen's University. Yue is a CPA, CMA. His research focuses on the disclosure and valuation relevance of corporate environmental performance, corporate social responsibility and sustainability practice. Yue has served as Ad Hoc Editor for Contemporary Accounting Research, as Associate Editor for the Asia-Pacific Journal of Accounting and Economics, Managerial Auditing Journal, and Accounting Forum, and as Guest Editor for the Journal of Management Accounting Research and Asia Review of Accounting. He has published his research in the leading accounting research journals, including *The Accounting Review*, *Contemporary Accounting Research*, *Accounting, Organizations and Society*, *Journal of Accounting and Public Policy*, *European Accounting Review*, *Journal of Accounting, Auditing and Finance*, among others.

Soo Min Toh, PhD

Associate Professor of Organizational Behaviour and HR Management, Director of the Institute for Management & Innovation, University of Toronto

Soo Min is an Associate Professor at the University of Toronto and is cross-appointed to the Institute for Management & Innovation and the Joseph L. Rotman School of Management, and is Professorial Fellow at the University of Edinburgh Business School. She received her PhD from Texas A&M University. Soo Min sits on several editorial review boards of significant international journals and was the Chair of the International Affairs Committee at the Society of Industrial & Organizational Psychology. At the University of Toronto, she teaches undergraduate and graduate students about leadership, bias, maximizing human potential, and conducting research. University. Her research interests include cross-cultural management, leadership, and cooperation. She has published in the *Academy of Management Journal, the Academy of Management Review, the Journal of Applied Psychology, and Psychological Science*, and serves on the editorial board of the *Journal of International Business Studies*. In addition, her work on leadership, women leaders, and cross-cultural intergroup cooperation has been featured in international news and business media, including the *Financial Times*, *Fortune*, the *Globe & Mail*, and *Harvard Business Review*.

Irene M. Wiecek

Professor of Accounting, Teaching Stream, Director of the Master of Management & Professional Accounting Program and Director, BIGDataHUB, University of Toronto

Irene is a Professor at the University of Toronto where she is cross-appointed to the Institute for Management & Innovation and Joseph L. Rotman School of Management. Irene has been involved in professional accounting education for over twenty-five years, sitting on various university and provincial / national professional accounting organization committees as well as developing and directing the CPA Canada IFRS Immersion Programs for practising accountants and founding and co-directing the CPA/Rotman Centre for Innovation in Accounting Education. In the area of standard setting, she is currently a member of the Accounting Standards Board IFRS Discussion Group.

Irene has co-authored numerous books and publications including seven editions of the text *Intermediate Accounting* (by Kieso et al) for which she is one of two Canadian co-authors on the Canadian edition. Irene's interests lie in the area of International Financial Reporting Standards, integration in accounting education and most currently, big data, artificial intelligence and emerging technologies including blockchain. Irene is a member of the CPA Canada Foresight Working Group on Reimaging the Profession as well as the group's Data Governance Workstream. She is an FCPA, FCA and is the Director and founder of the BIGDataHUB at the University.

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA