TIM Technology Innovation Management Review

October 2017
Volume 7 Issue 10
http://doi.org/10.22215/timreview/1107

Image Credit: XoMEoX (CC-BY)

Blockchain

Welcome to the October issue of the *Technology Innovation Management Review*. We welcome your comments on the articles in this issue as well as suggestions for future article topics and issue themes.

Carleton UNIVERSITY

www.timreview.ca

Publisher

The *Technology Innovation Management Review* is a monthly publication of the Talent First Network.

ISSN

1927-0321

Editor-in-Chief

Chris McPhee

www.timreview.ca

The PDF version is created with Scribus, an open source desktop publishing program.

Overview

The *Technology Innovation Management Review* (TIM Review) provides insights about the issues and emerging trends relevant to launching and growing technology businesses. The TIM Review focuses on the theories, strategies, and tools that help small and large technology companies succeed.

Our readers are looking for practical ideas they can apply within their own organizations. The TIM Review brings together diverse viewpoints – from academics, entrepreneurs, companies of all sizes, the public sector, the community sector, and others – to bridge the gap between theory and practice. In particular, we focus on the topics of technology and global entrepreneurship in small and large companies.

We welcome input from readers into upcoming themes. Please visit timreview.ca to suggest themes and nominate authors and guest editors.

Contribute

Contribute to the TIM Review in the following ways:

- Read and comment on articles.
- Review the upcoming themes and tell us what topics you would like to see covered.
- Write an article for a future issue; see the author guidelines and editorial process for details.
- Recommend colleagues as authors or guest editors.
- Give feedback on the website or any other aspect of this publication.
- Sponsor or advertise in the TIM Review.
- Tell a friend or colleague about the TIM Review.

Please contact the Editor if you have any questions or comments: timreview.ca/contact

About TIM

The TIM Review has international contributors and readers, and it is published in association with the Technology Innovation Management program (TIM; timprogram.ca), an international graduate program at Carleton University in Ottawa, Canada.

Editorial: Blockchain

Chris McPhee, Editor-in-Chief

Anton Ljutic, Guest Editor

From the Editor-in-Chief

Welcome to the October 2017 issue of the *Technology Innovation Management Review*. This month's editorial theme is **Blockchain**, and it is my pleasure to introduce our Guest Editor, **Anton Ljutic**, a training and development specialist in the domains of IT security and former Professor at Champlain Regional College in Saint-Lambert, Canada.

For special issues scheduled for publication in 2018, we are currently seeking contributions for the themes of Entrepreneurship in India, Inclusive Innovation, Frugal Innovation, and Cybersecurity. We welcome suggestions of themes for future special issues in addition to queries from potential guest editors.

For upcoming regular issues, we are accepting general submissions of articles on technology entrepreneurship, innovation management, and other topics relevant to launching and growing technology companies and solving practical problems in emerging domains. Please contact us (timreview.ca/contact) with potential article topics and submissions.

Chris McPhee
Editor-in-Chief

From the Guest Editor

Great inventions lead to unexpected consequences. Consider how the invention of electricity triggered rapid innovation and transformation in telecommunications – first came the telegraph and the telephone, then radio, television, and finally, digital convergence over the Internet. These innovations transformed war, politics, education, shopping, and countless other aspects of modern life. But it is often the social, economic, and even cultural effects of electricity that truly help inventions go far beyond what could have been expected by their inventors. The music industry exploded with the gramophone, health was transformed with radiology and imaging, the airline industry owes its existence to cheaper aluminum, while urban landscapes were transformed by elevators and subways. Each of these examples shows the importance of electricity as a "general purpose technology" – a technology "that can lead to the creation of many sub-inventions" (Gordon, 2017).

And that is precisely what blockchain is: a general purpose technology.

As its name suggests, blockchain is a chain of blocks of information, usually called digital ledgers. These ledgers are chronologically linked and replicated in a distributed database. Information can be added, but never removed; any change is witnessed and validated by the chain and is always available for verification. Each block is protected by cryptography, and only those authorized can access the information in the ledger. Although private blockchains exist, a typical blockchain is public, has no central authority, and is said to be "decentralized". Thus, the introduction of blockchain is resulting in a move from highly centralized, single-point-of-failure systems to those that are closer to being user-controlled and that provide an auditable trail for moving things of value.

The Internet is about information exchange. Blockchain adds a totally new dimension: the exchange of value between potential strangers in the absence of trusted relationships. Replacing the dependency on

Editorial: Blockchain

Chris McPhee and Anton Ljutic

trust with cryptography means that most verification, identification, authentication, and similar forms of assurance, accreditation, certification, and legalization of identity, origin, competence, or authority of persons or assets can now be guaranteed by mathematics. And once trust is replaced by reliable cryptography, there can be disintermediation of all the layers of "middlemen".

The contributors to this issue of the TIM Review show that blockchain technology has already permeated many areas of human endeavour. None of them claims to know where the impacts will end, but they give us a convincing picture of a revolution in the making. The reason is that blockchain incorporates a number of characteristics that are useful, unique, and unavailable elsewhere.

In the first article, **Melanie Swan**, a technology theorist from Purdue University in the United States and author of the best-selling book *Blockchain: Blueprint for a New Economy* (Swan, 2015), introduces, defines, and elaborates on the key concepts of the new blockchain technology. Swan highlights both the potential economic benefits and major challenges facing the future of blockchains.

Next, **Philippa Ryan**, Barrister and Lecturer in the Faculty of Law at the University of Technology Sydney, Australia, examines "smart contracts" and the legal implications of their proliferation on the blockchain. Ryan systematically examines some of the legal and practical problems that smart contracts could raise and proceeds by showing how to avoid or bridge them. Her overall conclusion is that smart contracts lead to key improvements in online transactions thanks to the nature of blockchain technology.

In the third article, **Mark Engelhardt**, a partner at Ovodenovo Intellectual Property Consulting in Ottawa, Canada, relies on a number of participant interviews to identify research and development directions in the healthcare sector. Indeed, one of the areas where blockchain is likely to cause significant changes is healthcare and healthcare services – from the way medical records are kept to the administration of medication and the delivery of dental care. The decentralized nature of blockchains "puts the patient at the centre" and in control of, or at least an equal participant in, the healing process. Another relies on the blockchain's anonymity and encryption of records to provide greater control of access to information by the patient, which paradoxically might lead to more data being available to researchers. As well as preserving confidentiality, blockchain also guarantees the integrity of records given that any tampering is detectable. Lastly, blockchain might eliminate waste and therefore reduce cost in a sector sorely burdened with expensive overhead that absorbs a large share of national resources.

In the fourth article, **Greg Wolfond**, CEO of SecureKey in Toronto, Canada, argues that blockchain-based solutions have the potential to make government operations more efficient and improve the delivery of services in the public and private sectors. Drawing on SecureKey's efforts to develop digital identity technologies and through its collaboration with the Digital ID & Authentication Council of Canada (DIACC; diacc.ca), Wolfond's contribution emphasizes the importance of an ecosystem-based approach within the Canadian context.

Finally, **Hugh Rooney**, **Brian Aiken**, and **Megan Rooney** answer the question "Is Internal Audit Ready for Blockchain?" Hugh Rooney is a member of the Tendermint/COSMOS team who are building blockchain infrastructure, Brian Aiken is an External Board Member of the Audit Committee to the Auditor General of Canada, and Megan Rooney is law student at Osgoode Hall in Toronto, Canada. Thus combining their audit/legal/blockchain expertise, the team offers practical advice to help organizations prepare their internal audit teams to be "blockchain ready". They argue that blockchain technology is coming rapidly and many levels of government in Canada are already on board. Internal auditors must prepare to deal with new data formats, acquire proficiency with big data analytics to reduce business risk, improve performance and maximize value, work more collaboratively across organizations, and understand that some current work will become redundant. The authors briefly describe six steps that must be taken by internal audit practitioners, and they conclude that blockchain has the potential "to enable numerous new digital solutions to many of the challenges governments and other large organizations face".

The articles in this special issue offer only a high-level introduction to what has been described as the greatest invention since the Internet (e.g., Naughton, 2016; Torpey, 2016). There are far too many application cases for anybody to list and far too much technical detail to cram into a review such as this. A recent Juniper Research study revealed that over half of large corporations are studying the use of blockchain (Holden & Moar, 2017). Two-thirds of the same companies said that they expected the technology to be integrated into their systems by the end of 2018. Our contributors have, instead, covered a fairly wide area of developments, describing leading-edge cases from healthcare, a transformative identity verification and control for Canadians, and preparation required of internal auditors for working with blockchain. Questions were raised, definitions advanced and legal and economic effects of blockchain examined. We thank you for your interest. We hope that you will follow some of the leads on your own.

This story has only just begun.

Anton Ljutic
Guest Editor

References

Gordon, R. J. 2017. *The Rise and Fall of American Growth: The U.S. Standard of Living Since the Civil War.* Princeton, NJ: Princeton University Press.

Holden, W., & Moar, J. 2017. *Blockchain Enterprise Survey: Deployments, Benefits & Attitudes.* Basingstoke, UK: Juniper Research.

Naughton, J. 2016. Is Blockchain the Most Important IT Invention of Our Age? *The Guardian,* January 24, 2016. Accessed October 1, 2017: https://www.theguardian.com/commentisfree/2016/jan/24/blockchain-bitcoin-technology-most-important-tech-invention-of-our-age-sir-mark-walport

Swan, M. 2015. *Blockchain: Blueprint for a New Economy.* Sebastopol: O'Reilly Media.

Torpey, K. 2016. Why the Bitcoin Blockchain Is the Biggest Thing Since the Internet. *Nasdaq,com,* April 19, 2016. Accessed October 1, 2017: http://www.nasdaq.com/article/why-the-bitcoin-blockchain-is-the-biggest-thing-since-the-internet-cm608228

About the Editors

Chris McPhee is Editor-in-Chief of the *Technology Innovation Management Review.* He holds an MASc degree in Technology Innovation Management from Carleton University in Ottawa, Canada, and BScH and MSc degrees in Biology from Queen's University in Kingston, Canada. Chris has nearly 20 years of management, design, and content-development experience in Canada and Scotland, primarily in the science, health, and education sectors. As an advisor and editor, he helps entrepreneurs, executives, and researchers develop and express their ideas.

Anton Ljutic is a futurologist with many interests, having been a professional musician in Germany, a programmer at IBM Rome, a professor of Economics and an early Internet telecommunications enthusiast and consultant in Montreal, a Head of the Government of Canada's IT Security Learning Centre, and the founder and chair of the government's Interdepartmental Committee on Security Training. He was founder and editor in the early 1990s of one of the earliest Internet ezines, *Glosas News.* He is a member of Blockchain Association of Canada (BAC) and a believer in political and economic decentralization through blockchain. He holds a Master of Arts degree from Carleton University in Ottawa, Canada, and a Diploma in Economics from the University of Zagreb, Croatia.

Citation: McPhee, C., & Ljutic, A. 2017. Editorial: Blockchain. *Technology Innovation Management Review,* 7(10) 3–5. http://doi.org/10.22215/timreview/1108

Keywords: blockchain, bitcoin, cryptography, trust, economics, smart contracts, healthcare, digital identity, authentication, services, transactions, internal audit

Anticipating the Economic Benefits of Blockchain

Melanie Swan

> “ *In the future, it might seem just as strange to say that I am trusting a third-party institution with my interests as to say that I'm using an abacus today.* ”
>
> Gavin Wood
> Ethereum Co-Founder

In this general overview article intended for non-experts, I define blockchain technology and some of the key concepts, and then I elaborate four specific applications that highlight the potential economic benefits of digital ledgers. These applications are digital asset registries, blockchains as leapfrog technology for global financial inclusion, long-tail personalized economic services, and net settlement payment channels. I also highlight key challenges that offset the potential economic benefits of blockchain distributed ledgers, while arguing that the benefits would outweigh the potential risks. The overarching theme is that an increasing amount of everyday operations involving money, assets, and documents could start to be conducted via blockchain-based distributed network ledgers with cryptographic security, and at more granular levels of detail. One economic implication of widespread blockchain adoption is that the institutional structure of society could shift to one that is computationally-based and thus has a diminished need for human-operated brick-and-mortar institutions.

Introduction

Blockchain (distributed ledger technology) is a network software protocol that enables the secure transfer of money, assets, and information via the Internet, without the need for a third-party intermediary such as a bank (Swan, 2015). Transactions are validated, executed, and recorded chronologically in an append-only tamper-resistant database, where they remain available on the Internet for on-demand lookup and verification. A digital money system such as Bitcoin is the first and perhaps the most obvious application of blockchain technology. Money can be transferred immediately in real-time from one continent to another, at very low costs, and in a matter of seconds or minutes, instead of waiting days or weeks, and paying high commissions, as is the case with current international money transfer and remittance solutions. Just as the simple mail transfer protocol (SMTP) constitutes the underlying protocol by which Internet users can send an email to each other in a seamless and interoperable way, regardless of their email provider, likewise, the Bitcoin protocol allows people to seamlessly transfer money to one another, regardless of their bank. However, digital currency is but one application enabled by blockchain technology. The four main kinds of applications in development are real-time money transfer and payments, property registries, contractual agreements, and identity confirmation.

The terms blockchain and distributed ledger technology are often used interchangeably. Distributed ledger is the general form of the technology, and blockchain is a specific form with an additional technical detail. Both refer to the concept of a ledger– a file that keeps track of who owns what. A distributed ledger has four salient features: i) a transaction database shared among network members that is ii) updated by consensus, with iii) records timestamped with a unique cryptographic signature, maintained in a iv) tamper-proof auditable history of all transactions. Blockchain adds the additional feature of sequential updating of database records per chained cryptographic hash-linked blocks (each block calls a hash of the previous block, effectively linking transaction blocks into an immutable chain, hence the term "blockchain"). There are two kinds of blockchains: public and private. Anyone may use public blockchains such as Bitcoin (bitcoin.org) and Ethereum (ethereum.org), and identity is not known. Private blockchains are analogous to a corporate intranet, used by industry consortia and governments, where users are known and credentialled.

Cybersecurity could be one of the biggest drivers of blockchain adoption. Recent breaches – the private data of an estimated 145.5 million Americans was exposed by the Equifax credit attack (Cowley, 2017) and, in another major attack, the names, emails, and passwords of all 3 billion Yahoo user accounts were stolen (Larson, 2017) – underline the urgent need for better cybersecurity solutions. Centralized databases provide an attractive target for hackers, whereas it is possible that decentralized storage records protected by cryptographic signatures on blockchains might dramatically improve network cybersecurity. Greater user control and permissioning of personal data is an expected feature of decentralized solutions. Blockchains are called "trustless" in that they eliminate having to trust any third party institution such as Equifax or Yahoo in the middle of transactions with personal data. Blockchains are *smart networks* that confirm and transfer value directly, without third-party intermediaries. Intelligence is built directly into the network's operations through a sophisticated protocol that automatically identifies, validates, confirms, and routes transactions within the network. The result is a trustless system in that the human counterparties and institutions involved do not need to be known and trusted. Instead, trust is placed in the computational smart network system, which could help to create next-generation cybersecurity solutions.

Application 1. Digital Asset Registries

Following digital currencies and money transfer, one of the biggest blockchain applications in development is digital asset registries. The same distributed ledger technology provides the means to record and transmit digital goods over the Internet, while ensuring that these goods cannot be copied or multiplied (thereby addressing the double-spending problem that has been an issue with digital currencies previously). A digital asset registry is a listing of smart assets (also referred to as smart property). A smart asset is an asset that is registered to a blockchain and thus can be easily verified and transferred because of this digital registration (Swan & de Filippi, 2017). Digital asset registries might use blockchains extensively as a system to record, transfer, and verify asset ownership. This could include titles for automobiles, homes, and land.

Land titling systems are a "low hanging fruit" application to demonstrate blockchains in practical use. Some countries have pilot programs underway, notably Georgia, Ukraine, Sweden, and Ghana (Reese, 2017). In Sweden, the government estimates that the project could save taxpayers over $106 million USD a year by eliminating paperwork, reducing fraud, and speeding up transactions (Lantmäteriet, 2016; Wong, 2017). The money at stake suggests resistance to new solutions, for example, the United States title insurance industry earns $18 billion USD a year for a product that some have evaluated as outdated and largely unneeded, even before the concept of blockchain-based registries (Woolley, 2006). There are property transfer issues and also legal implications. A blockchain can be used as a digital registry to record, transfer, and verify asset ownership (home, auto, stocks, bonds, mortgages, and insurance), and also to preserve the integrity and authenticity of sensitive documents or records (e.g., passports, visas, driver's licenses, birth and death certificates, voter registration, contracts, wills, patents, and medical records). An exemplar implementation of digital asset registries for identity services is the State of Illinois's blockchain-based birth registry project (Illinois Blockchain Initiative, 2017).

Application 2. Leapfrog Technology

One of the highest-impact applications of blockchains could be as a leapfrog technology for global financial inclusion. It does not make sense to build out brick-and-mortar bank branches to every last mile in a world of digital services. Instead, eWallet banking apps might be an effective means of reaching the two billion "unbanked" people in the world (PwC, 2016). Even without phone-based banking, low-cost debit cards might effectively service the unbanked (Rogoff, 2016). These kinds of "FinTech "solutions (i.e., financial technology: financial services delivered by technology) could have the benefit of opening up new markets to service providers who did not have a cost-effective method of addressing these customers previously (Swan, 2017). The leapfrog impact could be significant as banking services are bundled together with identity services and land registries. The United Nations estimates that 1.1 billion people, one sixth of the world's population, live without an officially recognized identity (2017). Similarly, the World Bank estimates that 70% of the world's population lacks access to land titling (Heider & Connelly, 2016). Land titling and property transfer systems have been identified as a crucial step for economic development (de Soto, 2003). The adoption challenges are perhaps not always technical as much political given that solutions are only possible to the extent that power elites are willing to implement them (Chua, 2004).

A demonstration case of digital financial services as a leapfrog technology is the mobile payments market in China. In 2016, Chinese people and organizations spent the equivalent of $5.5 trillion USD through mobile payment platforms, about 50 times the amount spent in the United States (Kuhn, 2017). Nearly half (42.4%) of in-store purchases in China are via non-cash payments (Chen, 2017). Debit cards and credit cards were not offered and adopted in China to the same extent as in other countries, and thus an alternative to cash such as mobile payment has been widely adopted. More broadly, credit is in some sense a “luxury service” only extended to a small percentage of people worldwide. In an era of blockchain-based digital finance, credit could be a consumer service that is much more transparent, widely available, and synchronized across country boundaries. For example, there could be open-source FICO scores, blockchain-based credit bureaus, and blockchains as the backbone of the first international credit agency (Swan, 2016). Just as blockchain-based electronic medical records can be accessed securely anywhere in the world, so too could credit scores. The impact could be opening up credit markets to retail customers on a global basis. There could be advantages such as individuals not having to build credit histories from scratch when living in a different country. But there could also be drawbacks, as not everyone might want to join a global credit system (although one that is more transparent and user-controlled might be more welcome).

Application 3. Long-Tail Personalized Economic Services

The long-tail argument is that, in digital marketplaces, it is possible to sell lower quantities of more items (Anderson, 2008). The 80/20 rule – the classic logic that 80% of sales come from the top-selling 20% of items – does not hold in digital marketplaces. Researchers confirm long-tail economics in digital marketplaces, finding that niche books account for 36.7% of Amazon’s sales (Brynjolfsson et al., 2010). They argue that power laws as opposed to Pareto distributions are a better model for digital marketplace sales for books, music, and software downloads. For the blockchain economy, the key point is that not only are long-tail markets economically viable, but also that there is demand for *personalized* products and services that cater to individual needs. Previously, one size had to fit all in financial and government services due to economies of scale and other barriers. However, in a network economy with blockchain-based asset transfer, personalized financial and government services might be better tailored to individual needs and wants. An example of personalized economic services where one size does not fit all is that, instead of a standard 30-year mortgage, a borrower might prefer a 22-year mortgage that better corresponds to personal life events such as a planned home downsizing once children are grown.

Amazon, eBay, and Craigslist are digital marketplaces that allow the long tail of economics to meet in the sense of the buyer of a particular rare item being able to find a seller of that item in a way that would not be possible in a mass-market retail store. The point is that, in digital marketplaces, buyers and sellers can transact more granular personalized business than is economically feasible in the brick-and-mortar format. Likewise, with blockchains, the long tail of personalized financial services might be able to meet in “eBay for money” type websites, where the buyer of a specific financial service could find a provider. The implication of algorithmic trust, and funds locked or escrowed with smart contracts, is that any two long-tail parties can meet and transact in a secure blockchain-based environment, without having to know each other. Personalized banking, credit, and financial services could become routine, and also personalized governance services, for example, a closer link between the public services funded and consumed by individuals. Early evidence of long-tail markets for blockchain services is a September 2017 transaction that purports to be the first real asset transfer with a blockchain. US-based TechCrunch founder Mike Arrington purchased a Ukraine-based residence using Propy, a global decentralized property store on the Ethereum blockchain (Masse, 2017). This notable transaction strikes a parallel with Meg Whitman’s automobile purchase on the eBay Motors website in the early 2000s, which helped to legitimize digital marketplaces for large-size transactions.

Application 4. Payment Channels and Peer Banking Services

One of the most intriguing ideas being developed in the blockchain industry is payment channels. A payment channel is a financial contract executed over time in three steps: i) one party opens up a payment channel with one or more parties and posts a pre-payment escrow balance on file, ii) the party consumes against this credit over time, until iii) the closing transaction in which aggregate activity is booked in one net transaction to close the contract. The idea arose for micropayments, such as video bandwidth consumption, where piecemeal transactions do not make sense and an automated contractual arrangement can support aggregate consumption. Payment channels are similarly conceived for regular consumption such as opening up a Starbucks payment channel for $50 each month. The daily coffee consumed is tracked and booked against the $50 channel and netted at the end of the month. Contracts close and roll over at regular intervals. Either party may elect to close the payment channel early, in which case the net settlement would be booked and the contract would end. Another benefit of payment channels is easing blockchain scalability by only booking the opening contract and the final amount as opposed to interim transactions, while being contractually obligated and protected all along the way.

Payment channels are a speculative concept that is under discussion, but the conceptual implications are provocative. First, the radical implication of peer-to-peer networks is that any node can deliver services to other nodes, for a small transaction fee. This is already how the Bitcoin network operates, with 9,352 worldwide peer nodes (bitnodes.21.co) hosting the transaction ledger. The mining operation to confirm and log transactions is another network peer-based activity. Storage and news hosting are newer network services, and the implication is that payment channels have the requisite functionality to allow peer nodes to offer banking services (Dryja, 2016). We start to see what the claim that cryptocurrencies are “programmable money” might actually mean in implementation. Recognizable feature sets from other financial contracts (for example prepayment risk and European/American-style option execution) can be enabled easily in blockchain-based contracts such as payment channels. The question arises as to how to treat payment channels from an accounting and legal standpoint. For accounting purposes, is a payment channel a deferred payment or an installment sale? When during the contract is revenue to be recognized, and what are the balance sheet liability obligations? Legally, do payment channels constitute assignments of claims or forward-looking IOUs? A contingent three-part financial contract over time is a new instrument, especially when considering that transfers might exist across multiple hops (parties) in a directed graph structure of layered contingencies that is based on distributed computing network architectures as opposed to traditional modes of financial exchange.

Other conceptual implications are similarly striking. The idea of economic activity based on net settlement versus gross settlement is intriguing. Despite the current limit of roughly $175 (4% of the value of one Bitcoin) placed on the total payment channel transfer amount of any one channel by the existing solution provider, the Lightning Network (lightning.network), other payment channel solutions could have different parameters. What if many more operations in the economy were to transition to a net payments basis? Central banks clear amongst themselves with real-time gross settlement (RTGS) systems, as does Ripple (ripple.com). Industry consortia such as interbank daily settlements are tabulated on a net basis. However, what about opening up net clearing functionality to individuals? The idea is essentially an enhanced version of paycheque direct deposit plus auto-pay bills, just formalized into a multi-party payment contract. Personal monthly inflows and outflows could be orchestrated by a payment contract that nets salary against expenses and builds in a savings remainder. With money and payments digitized, and activity being securely forward-committed by payment contracts, the implication is that net flows instead of gross flows might be transferred. An economy based on net clearings or contracts for difference is quite different than the current system, and the risks and benefits would need to be evaluated.

A further implication of digitized money and payments is that the standard amounts at which we do business could be much more granular. This granularity could possibly allow progress in reconceiving the debt juggernaut impacting individuals and institutions alike. Streaming money could be disgorged in much smaller chunks that are more closely tied to costs and repayment possibilities (Antonopoulos, 2017). We could similarly reconceive economic modes of consumption and the related financing options. There could be a reconstitution of mechanisms for pre-paid consumption (a small part of current overall economic activity) against the much larger portion of activity that is post-paid and based on credit and terms. Digitized streaming money and payment channels could be techniques to quicken the 30–60–90 day terms and uncollectible debt problem in supply chain finance, and facilitate a just-in-time economy for money.

Key Challenges

The potential economic benefits of blockchain distributed ledgers are offset with several key challenges. The first challenge is that the technology is complicated. Even the basics are difficult to understand, both conceptually and technically, and this is a barrier to effective decision making and the ongoing implementation and use of the technology. Second, a variety of challenges have to do with the technical aspects of the technology. Bitcoin is the largest open blockchain in a field where private blockchains are also starting to be in use. As the biggest demonstration case, one concern specific to Bitcoin is that 70% of the mining operation (data centres that validate and confirm transactions) is concentrated in China (Coleman, 2016). Others counter that this is not a long-term risk as the mining operation would likely become more globally diversified as the use of the currency grows. Another concern is that there seem to be a variety of unresolved technical issues. However, it is important to note that Bitcoin is an open source software project, and that it is helpful, not detrimental, that all of the issues are publicly debated by worldwide developers. So far, changes to the software have been proceeding democratically, with all network participants involved in decision making (the five big constituencies are developers, miners, exchanges, wallets, and merchants). A recent example of this is the hard fork for the Bitcoin blockchain to incorporate SegWit2x, a new standard increasing scalability, with the decision made in August 2017 for implementation in November 2017 (Higgins, 2017). Others worry about hacking scandals, and these would likely persist in the ongoing development of blockchain ledger systems, while cybersecurity responses will also continue to develop in lockstep.

The third challenge is scalability – creating distributed financial networks that can scale to Visa-class processing levels and beyond – given that the networks may be used for a wider variety of transaction types. By comparison, Visa processes an average volume of 1,667 transactions per second, and Bitcoin processes 7 per second (Vermeulen, 2017). Visa transfers $18 billion per day, and Bitcoin transfers $300 million per day. At the heart of the issue is coordinating the operation of distributed computing networks. Visa is a closed proprietary network. Other computing networks that are more similar to distributed ledgers are those such as Google's PageRank. This system is distributed, but has an overall control mechanism (a locking service called Chubby in Google's case) that coordinates how network nodes are updated.

Public blockchains are different in that they are truly open distributed networks which any new peer may join. The computer science problem is getting 1 million distributed clients to agree, including when there could be malicious nodes on the network, because it is open (Williams, 2016). The mechanism by which distributed systems come to agreement about new truth states of the network is called consensus (and relatedly Byzantine agreement). The concept is that of a "world computer" that is securely and efficiently coordinated by algorithms as to how the network reaches consensus on new truth states of the database (ledger) and nodes update their copy. The kinds of consensus algorithms currently in use by blockchain systems are "proof of work" and "proof of stake". However, these algorithms may not be scalable solutions for the longer term. Proof of work, while secure, is inefficient. One estimate is that the Bitcoin network could consume as much electricity as Denmark by 2020 (Deetman, 2016) due to the proof-of-work requirement. Even though private blockchains have known and credentialled users, their scalability, too, is gated by the ability to update nodes in very large distributed networks. Thus, the development of consensus algorithms that are scalable, efficient, and secure is a challenge for the long-term viability of blockchain technology.

The fourth challenge is effective government regulation to support the development of the industry. Because blockchains deal with money (a sensitive area with incentive for corruption), they are likely to continue to be under the purview of national regulation. Although the technology allows anyone to download software and set themselves up as a bank, offering financial services on a payment gateway, it is not legal to do so. Even the most basic exchange between cryptocurrencies and fiat currency is deemed a money transmitter service and must be appropriately licensed by state agencies in order to be legal in the United States (Lujan, 2017). The onus is on entrepreneurs to determine the relevant regulatory aspects that apply to their businesses and then either comply or face non-compliance charges.

As with any new technology, the challenge is encouraging honest activity while thwarting nefarious behaviour. With blockchain, the question is how to encourage businesses to explore the new frontier enabled by digital ledgers, while managing an environment that simultaneously invites new kinds of scams and wrongdoing. The most recent example is the "dot-com boom" in initial coin offerings (ICOs), which have raised $2.7 billion USD to date, and how different national governments are regulating them (CoinDesk, 2017). In the United States, ICOs are evaluated on a case-by-case basis, and if they behave like a security, they are deemed as such, and fall under securities regulations (US SEC, 2017). Regarding law enforcement, digital ledgers should be recognized as a new and more complicated digital venue where illegal activities may be taking place alongside honest activities. Regulatory agencies are called upon to become savvy about the risks presented by the new technology and operate within this domain. Regulators need to understand how digital ledger technologies work and can be used for operations such as money laundering, and they need to understand how illegal practices might be detected, tracked, and persecuted in these new transnational cryptographic areas. An example of this was regulators using the tracking features inherent to blockchain transactions to apprehend perpetrators in the Silk Road case (Brandom, 2015). While being cognizant of these and other challenges, overall, the economic benefits of blockchain could outweigh the potential risks.

Conclusion

Blockchain distributed ledgers have the ability to securely digitize many current operations in economics and finance, and legal and government services, such that they might be reengineered for the Internet era. The four main kinds of blockchain applications are money transfer and payments, property registries, contractual agreements, and identity confirmation. Blockchains are able to transfer money and assets, and also preserve the authenticity of sensitive documents and records. The terms blockchains and digital ledgers are generally interchangeable, although blockchains have an additional feature in that transaction blocks are linked together with cryptographic hashes, which provides additional security. Blockchains could be important in cybersecurity solutions because they have decentralized storage records protected by cryptographic signatures as opposed to centralized databases that attract hackers.

In this article, four specific blockchain applications were examined that might have a positive economic benefit. First considering digital asset registries, there are a number of projects underway, particularly for improved efficiency in land titling and birth registration. Second, blockchains are identified as an important leapfrog technology for global financial inclusion with eWallet banking services, identity registration, and land titling. Third, distributed ledgers might allow personalized economic services to be created such as non-standard mortgages to suit individual needs in digital marketplaces that are like an “eBay for money.” Fourth, a speculative technology called payment channels might eventually develop into a digitized payment system for resource consumption that settles based on net payments instead of gross transfers, and enables peer-to-peer banking services. The overarching theme that emerges from this analysis is that many daily operations involving money, assets, and documents could start to be conducted on digital networks with cryptographic security. Given that less friction and human involvement may be needed to transfer goods and services, less physical infrastructure might be needed to make it happen. It is not that the influence and role of institutions would wane, but that their material footprint and how they do business could change substantially in a blockchain economy.

About the Author

Melanie Swan is a technology theorist in the Philosophy Department at Purdue University in West Lafayette, Indiana, United States. She is the author of the best-selling book *Blockchain: Blueprint for a New Economy* (2015), which has been translated into six languages. She is the founder of several startups including the Institute for Blockchain Studies, DIYgenomics, GroupPurchase, and the MS Futures Group. Ms. Swan's educational background includes an MBA in Finance and Accounting from the Wharton School of the University of Pennsylvania, an MA in Contemporary Continental Philosophy from Kingston University London and Université Paris 8, and a BA in French and Economics from Georgetown University. She is a faculty member at Singularity University and the University of the Commons, an Affiliate Scholar at the Institute for Ethics and Emerging Technologies, and an invited contributor to the Edge's Annual Essay Question.

Anticipating the Economic Benefits of Blockchain

Melanie Swan

References

Anderson, C. 2008. *The Long Tail: Why the Future of Business is Selling Less of More.* New York: Hachette Books.

Antonopoulos, A. 2017. *Advanced Bitcoin Scripting.* SF Bitcoin Developers Seminar, April 20, 2017. Accessed October 18, 2017: https://www.youtube.com/watch?v=MiS8-4uIOYo

Brandom, R. 2015. In the Silk Road Trial, Bitcoin is a Cop's Best Friend. *The Verge,* January 14, 2015. Accessed October 18, 2017: https://www.theverge.com/2015/1/14/7546669/silk-road-trial-bitcoin-tracking

Brynjolfsson, E., Hu, Y. J., & Smith, M. D. 2010. The Longer Tail: The Changing Shape of Amazon's Sales Distribution Curve. *SSRN,* September 20, 2010. Accessed October 18, 2017: http://dx.doi.org/10.2139/ssrn.1679991

Chen, T. 2017. China Mobile Payment Report 2017. *WalktheChat,* June 25, 2017. Accessed October 18, 2017: https://walkthechat.com/china-mobile-payment-report-2017/

Chua, A. 2004. *World on Fire: How Exporting Free Market Democracy Breeds Ethnic Hatred and Global Instability.* New York: Anchor Books.

CoinDesk. 2017. CoinDesk ICO Tracker: All-Time Cumulative ICO Funding. *CoinDesk,* October 13, 2017. Accessed October 18, 2017: https://www.coindesk.com/ico-tracker

Coleman, L. 2016. China's Mining Dominance: Good or Bad For Bitcoin? *Cryptocoins News,* September 14, 2016. Accessed October 18, 2017: https://www.cryptocoinsnews.com/chinas-mining-dominance-good-or-bad-for-bitcoin/

Cowley, S. 2017. 2.5 Million More People Potentially Exposed in Equifax Breach. *New York Times,* October 2, 2017. Accessed October 18, 2017: https://www.nytimes.com/2017/10/02/business/equifax-breach.html

Deetman, S. 2016. Bitcoin Could Consume as Much Electricity as Denmark by 2020. *Motherboard,* March 29, 2016. Accessed October 18, 2017: https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

De Soto, H. 2003. *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else.* New York: Basic Books.

Dryja, T. 2016. *Lightning Network as a Directed Graph: Single-Funded Channel Topology.* SF Bitcoin Developers Seminar, April 24, 2016. Accessed October 18, 2017: https://www.youtube.com/watch?v=-lgYYz3y_hY

Heider, C., & Connelly, A. 2016. Why Land Administration Matters for Development. *World Bank,* June 28, 2016. Accessed October 18, 2017: http://ieg.worldbankgroup.org/blog/why-land-administration-matters-development

Higgins, S. 2017. Bitcoin Cash Just Mined Its First Block, Making Blockchain Split Official. *CoinDesk,* August 1, 2017. Accessed October 18, 2017: https://www.coindesk.com/bitcoin-cash-just-mined-first-block-making-blockchain-split-official/

Illinois Blockchain Initiative. 2017. *Illinois Partners with Evernym to Launch Birth Registration Pilot.* The Illinois Blockchain Initiative, Press Release, August 31, 2017. Accessed October 18, 2017: https://illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c

Kuhn, A. 2017. In China, A Cashless Trend Is Taking Hold With Mobile Payments. *NPR,* June 29, 2017. Accessed October 18, 2017: http://www.npr.org/sections/alltechconsidered/2017/06/29/534846403/in-china-a-cashless-trend-is-taking-hold-with-mobile-payments

Lantmäteriet. 2016. *The Land Registry in the Blockchain.* Gävle, Sweden: Lantmäteriet. http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Larson, S. 2017. Every Single Yahoo Account Was Hacked - 3 Billion in All. *CNN,* October 4, 2017. Accessed October 18, 2017: http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

Lujan, S. 2017. U.S. Government Cracks Down on Illegal Bitcoin Money Transmitters. *Bitcoin.com,* May 5, 2017. Accessed October 18, 2017: https://news.bitcoin.com/government-cracks-down-on-illegal-bitcoin-money-transmitters/

Masse, B. 2017. Apartment Purchased with Ethereum Raises Hopes, Questions. *Inman,* September 29, 2017. Accessed October 18, 2017: https://www.inman.com/2017/09/29/apartment-purchased-with-ethereum-raises-hopes-questions/

PwC. 2016. *The Un(der)banked is FinTech's Largest Opportunity. DeNovo Q2 2016 FinTech ReCap and Funding ReView.* New York: PwC Strategy&. https://www.strategyand.pwc.com/media/file/DeNovo-Quarterly-Q2-2016.pdf

Reese, F. 2017. Land Registry: A Big Blockchain Use Case Explored. *CoinDesk,* April 19, 2017. Accessed October 18, 2017: https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem/

Rogoff, K. S. 2016. *The Curse of Cash.* Princeton, NJ: Princeton University Press.

Swan, M. 2015. *Blockchain: Blueprint for a New Economy.* Sebastopol, CA: O'Reilly Media.

Swan, M. 2016. *Decentralized Finance: Blockchains, Prediction, and Valuation.* Paper presented at The Economist: Finance Disrupted, New York, NY, October 13, 2016. http://www.financedisrupted.com/melanie-swan/

Swan, M. 2017. Expectation on Blockchain: Blockchain Economics and Finance. *Chijo (Intelplace),* 121: 17–24. http://melanieswan.com/documents/msj.pdf

Swan, M., & de Filippi, P. 2017. Toward a Philosophy of Blockchain: A Symposium: Introduction. *Metaphilosophy,* 48: 603–609. http://dx.doi.org/10.1111/meta.12270

United Nations. 2017. ID2020 Summit. *United Nations.* Accessed October 18, 2017: http://id2020summit.org

US SEC. 2017. *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities.* United States Securities and Exchange Commission (US SEC), Press Release, July 25, 2017. Accessed October 18, 2017: https://www.sec.gov/news/press-release/2017-131

Vermeulen, J. 2017. Bitcoin and Ethereum vs Visa and PayPal – Transactions Per Second. *My Broadband,* April 22, 2017. Accessed October 18, 2017:
https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html

Williams, D. 2016. DFINITY: Applications of Verifiable Random Function. *Stanford Computer Forum,* November 15, 2016. Accessed October 18, 2017:
https://www.youtube.com/watch?v=hX0DkgQloDE

Woolley, S. 2006. Inside America's Richest Insurance Racket. *Forbes,* October 28, 2016. Accessed October 18, 2017:
https://www.forbes.com/forbes/2006/1113/148.html

Wong, J. I. 2017. Sweden's Blockchain-Powered Land Registry Is Inching towards Reality. *Quartz,* April 3, 2017. Accessed October 18, 2017:
https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/

Citation: Swan, M. 2017. Anticipating the Economic Benefits of Blockchain. *Technology Innovation Management Review,* 7(10): 6–13.
http://doi.org/10.22215/timreview/1109

Keywords: blockchain, economics, payment channels, distributed ledgers, cryptocurrencies, cybersecurity, cryptoeconomics, long tail markets, digital goods, smart assets, smart contracts, streaming money, programmable money, lightning network, digital asset registries, eWallet

Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain

Philippa Ryan

> “*A contract is not sufficient unto itself, but is possible only thanks to a regulation of the contract which is originally social.*”
>
> Émile Durkheim (1858–1917)
> Sociologist and modernist

Much of the discussion around blockchain-based smart contracts has focused on whether or not they operate in the same way as legal contracts. However, it is argued that most contracts are social rather than legal in nature and are entered into because the parties trust each other to perform the agreed exchange. Little has been written to address how the blockchain’s trust protocol can enable the kind of social contracting that characterized the way exchanges were conducted before the Internet. This article aims to fill that gap by exploring blockchain-based smart contracts primarily as non-contractual social exchanges.

Introduction

Stewart Macaulay’s seminal 1963 article “Non-Contractual Relations in Business” explored why merchants and manufacturers often fail to plan their commercial relationships and why they seldom resort to legal sanctions to settle disputes. Macaulay found that, in many business exchanges, detailed planning and legal sanctions play only a small role. His tentative explanation was that businesses prefer to deal with people or organizations they trust based on their prior dealings or their reputation. According to Macaulay, a manifestation of trust might be a brief conversation followed by a handshake. The rationale is that, if parties cannot rely on promises as being made in good faith, and plan for the future accordingly, the cost of uncertainty would make conducting business impossible. However, this approach to contracting frustrates lawyers, who advise their clients to plan for contingencies and formalize their business arrangements.

This article will apply Macaulay’s behavioural analysis of business exchanges to smart contracts. In particular, it will examine the way that blockchain can provide and build trust and reputation while also managing the performance of the exchange. Once the management of performance of a smart contract is explained and understood, it is possible to give expression to the way that blockchain manages good faith in online business exchanges. In this way, blockchain solves a significant problem for anyone wanting to do business online.

Situating Smart Contracts within Contract Theory

Smart contracts enabled by blockchain technology are programmable applications that manage exchanges conducted online. Those exchanges would usually be an asset in exchange for value (but could be an asset in exchange for another asset, or one value for another value that is in a different currency). In the case of blockchain technology, value may be represented by a digital token, such as Bitcoin or another cryptocurrency. Much of the discussion around smart contracts enabled by blockchain technology has focused on whether or not they operate in the same way as legal contracts. However, legal contracts are not usually the focus of discussion when exchanges are conducted offline. This disconnect between the treatment of exchanges managed by smart contracts and exchanges in the analogue world is probably due to a combination of factors including the word “contract” in the term “smart contract”, and also the claim made by many blockchain developers and advocates that this innovative technology can provide and manage trust between the parties. There is a further important factor that considers the nature of contractual relationships: they are often founded on custom and conversation. According to Doddridge, legal principles are derived from logic, natural philosophy, cannon, and finally, from “the customs and conversations of men” (Doddridge, 1630).

In order to distinguish contracts established by custom and conversation from those that are founded on terms and conditions, it is useful to reflect on existing contractual theory. For example, Weber’s (1922) distinction with an analysis of freedom of contract between what he described in the 1920s as the traditional “status contract” and the (then) modern “purposive contract”. The former describes the complex social web of inter-relationships that arise when members of a community contract with each other to meet their economic and personal needs. The contracting members of this ecosystem change organically as they enter into agreements to accommodate the symbiotic relationship with the other members of the network. The latter (that is the “purposive contract”) refers to legal claims made by one against another without necessarily being personally acquainted with each other. This discussion readily applies to the consideration of the use and legal implications of smart contracts because so much of the discourse around smart contracts has so far concentrated on their legality and how contracting parties will assert their rights and obligations. However, it is suggested here that their use is more social than legal and that the status of the parties to a smart contract prevails over their legal relationship. Indeed, when most people conduct business over the Internet, they are less interested in the legal consequences of those transactions than the interconnectedness that results from the exchange. This can be seen in the way that people rate their experiences on eBay, Uber, and TripAdvisor. Users of these service providers rate their experience with the vendor based on the quality and timeliness of the delivery of the service or product. These ratings create reputation for the service provider and build relationships of trust in the network or community. Even though the nature of the marketplace means that participants will very likely never meet, their interactions give rise to exchanges where the parties to the transaction are relying on each other’s status established through these conversations, rather than their strict legal rights expressed in terms and conditions.

At the time that Weber was writing about economy and society in 1920s Germany, electricity was powering small-scale domestic appliances, including lights, sewing machines, telephones, recording equipment, and fans. As soon as a premises was connected to electricity, the business or householder could buy and use lights and appliances powered by electricity. To pay for this service, a contract arrangement would be entered into between the customer and the electricity company. Electricity companies employed and trained meter readers to attended to households and to note down exact consumption in order to generate a bill so that the owner or tenant of the premises could pay their usage, usually on a monthly basis. The meter reading, the calculation of consumption, the generation of the bill, and the payment were all conducted manually.

Clearly, smart contracts can manage financial interactions between machines, vehicles, humans, regulators, government, and financial service providers. Indeed, many of these processes are already managed online via processes that are automated. However, at this time, some steps along the path still require human intervention. For example, in order to pay for electricity, a service provider needs to calculate the amount owing by measuring consumption and then applying a formula that generates an invoice. These processes (the register of consumption, the calculation of the amount owing, the generation of the invoice, and its delivery via email) are all currently automated and (as long as there are no disputes) they require no human intervention. The only step along the way that requires a human to do something is when the customer pays the invoice.

If the human steps are to be replaced by automated processes, then it is important to ensure that this step emulates the appropriate human interaction. For example, if the payment of an electricity bill is currently done by authorizing a funds transfer from the customer’s bank account to the electricity company’s bank account and nothing more, then the automated processes should simply emulate this process. A smart contract could manage all of these steps without the need for any intervention. Any requirement to enter a password or in some other way to verify the customer’s authorization of the payment can be readily bypassed by providing pre-authorization for all of these types of payments. The pre-authorization and direct funds transfer of payments to financial organizations and other service providers has been a part of the online banking ecosystem for more than two decades. Including this step in smart contracts is a next logical step in the way that online transactions will be managed.

It is important to note in this description of how we use and pay for electricity that a close reading of the terms and conditions of use of the electricity and the legal implications or obligations that arise from incurring a debt to the electricity company are not usually regarded as a necessary step in making such an arrangement. This is because the human experience of consuming and paying for utilities, products, and services such as water, gas, electricity, garbage collection, sanitation, food, petrol, and public transport is a custom with which most people are familiar.

In the day-to-day workings of developed economies, few disputes arise between consumers and those who deliver and sell these types of goods and services. Legal scholarship that focuses on the contract lawsuit, as opposed to contractual relationships, creates a distortion of most social norms and economic systems (Macaulay, 1977). Since the advent of the Internet, many of the payments and invoices for these transactions are managed online, but the nature of the exchanges remains a social experience. These types of contracts are very different in nature to the purchase of a business or an investment in property. These commercial arrangements require due diligence to be conducted on the target and perhaps legal advice in relation to the terms and conditions upon which the purchase or investment will be made.

Weber’s (1922) understanding of different types of contracts is applicable to an analysis of how smart contracts will fit into our future of online exchanges and it favours the characterization of these relations as conversational and social, rather than strictly legal and purposive.

The question of whether or not a smart contract is also a legal contract is only necessary when considering its use. In most cases, the answer will be more intuitive than deliberate. This reflects the way that contracts are currently conducted both online and offline. It is usually unnecessary because smart contracts are a thoroughly modern extension of Weber’s notion of a conversational or social relationship, and they are an example of the law “in action” as opposed to the law “on the books” (Leib & Eigen, 2017).

The way that contracts are experienced is not so much about the law as it is about human interaction. Contract formation and enforcement are almost entirely about the law of the threat of legal enforcement in case a dispute arises. This is understood in the context of social contracts. The types of contracts that demand close attention to and legal expression of the terms and conditions are those that give rise to enduring relationships that require significant investment or those that expose one or both parties to high levels of risk. The need to reduce terms to a written contract rarely arises in relation to small, low-risk, ongoing transactions.

In the modern age of smart contracts, much of this human interaction is online. Archetypal contracts are contracts derived from an archetypal set of exchange conditions. These conditions include some bilateral, pre-consent negotiation, a general understanding by both parties that an enforceable obligation is being undertaken, a general understanding of the terms, a general understanding of the consequences of breach of those terms, and some direct or indirect relationship between the benefit of the bargain and the contract itself (Kastner, 2010). These foundational components of the collective imagination about “contract” sustain its sociological and normative legitimacy (Eigen, 2008). It is these descriptions of contract that are found in legal textbooks. However, modern online exchanges do not include the traditional behavioural characteristics of contract formation. Whereas traditional offline contracts were sealed with a handshake or a signature, modern online exchanges can be agreed to with a click (Eigen, 2008). Examples of this modern exchange would be the online purchase of digital music or the placement of a bid via online auction sites, which often requires pre-registration with a credit card and then the click of a button during the live auction. There are more sophisticated ways to shop online for physical items that emulate the offline retail shopping experience. For example, purchasing a product from a digital store involves selecting the item and its addition to a “shopping cart”, the option to “continue shopping”, and then the payment for all items in the cart at the virtual “checkout”. Online shopping is not a radical departure from the way that the common law regards the shopping experience. The moment when the contract is entered into happens when the customer makes the offer to purchase at the checkout. As Somervell (1953) noted, when the customer reaches the checkout, they can remove items from the cart and then choose to authorize payment. This analysis applies to both online and in-store (that is, offline) purchases. If an online purchase is one that is available to any shopper, then in most cases, there is no need for the vendor to refuse the customer’s offer to purchase the items and make the payment.

Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain *Philippa Ryan*

This article applies Macaulay's work in the 1960s and 1970s to the modern experience of smart contracts and, by analogy, to the trust mechanisms provided and managed by blockchain technology. In doing so, it is argued that smart contracts enabled by the blockchain are the archetype of contract in action, as opposed to contractual doctrine. The legal implications for blockchain are that its online exchanges will align closely to Macaulay's notion of non-contractual or social relations. Discussion about the nature of online exchanges conducted via smart contracts is better suited to a behavioural analysis of business exchanges than a doctrinal analysis of the law of contract.

Macaulay's Behavioural Analysis of Traditional Business Exchanges

According to Macaulay's behavioural analysis of traditional business exchanges (Macaulay, 1963), most contracts are examples of the law in action. The law in action refers to how people and businesses use contracts to manage their lives; how disputes in the performance of contracts arise and are settled; and how the resolution of disputes affects the parties to the disputes and influences future parties to contracts. The emphasis is on what happens on the ground, empirically, not on what theoretically should or probably would happen if certain assumptions were true (Macaulay & Whitford, 2015). It is argued here that this approach to the discussion of contracts is readily applicable to the way that humans will use most blockchain-based smart contracts. Of course, there will always be exceptions. The law and human experience generally have always managed to articulate exceptions. However, most contracts are social exchanges and most are conducted with little dispute, and most disputes are resolved by the participants without recourse to the law or lawyers.

For any contract system to function well, trust is an essential element (Eigen, 2008). Beale and Dugdale (1975) described similar dynamics in the relationships between engineering firms in Bristol, England. Again, this was research conducted in the mid-1970s pre-Internet era and at least a decade before there was any notion that business exchanges could be conducted online. Beale and Dugdale noted that the manufacturing companies spent minimal timing in contract planning. They surmised that was likely due to the existing familiarity between the companies. Because the parties to the transactions trusted each other, they perceived a low level of risk in their business dealings. Under these circumstances, any extensive negotiations would lead to delay and expense that was disproportionate to the risk of dispute. It was also observed that manufacturers were also concerned that too much negotiation might sour an otherwise peaceful relationship and break down important bonds of trust (Scott, 1997).

Social contracting is usually managed by codes of behaviour that direct the parties as to how they should behave (Scott, 1997). This is in contradistinction to the law, which operates to tell the parties what they must not do and what they must do. The difference is a question of mode/strength of enforcement: social norms are enforced by ostracism; positive law is enforced by sanction as expressed by a court order at the end of a litigious process. Social norms in contracting are important because they may be industry-specific and even contrary to the exact letter of the law. The relationship between the parties and their relative bargaining power will usually dictate whether one of the parties (usually the weaker of the two) will seek legal advice prior to contracting. However, most of the exchanges that happen online between organizations and consumers or customers do not involve large transactions and therefore would not justify the expense of seeking legal advice. The question of how online contracts are formed and the social norms that keep the parties from involving their lawyers is more relevant in the discussion of companies and firms doing business online with other business or industry organizations.

Behavioural Analysis of Business Exchanges as Applied to Smart Contracts

Bitcoin (bitcoin.org) is an electronic payment system employing cryptographic proof, instead of trust, in order to ensure that reversal of a transaction, once entered into, is impossible. Bitcoin was the first application to utilize what has become known as blockchain technology. Blockchain uses peer-to-peer data and certain of Bitcoin's components in order to reduce the need for trusted third parties in mediating bilateral communications. Blockchain technology enables an electronic payment system based on cryptographic proof that hashes and timestamps transactions into an ongoing chain of hash-based proof of work, allowing any two willing parties to transact directly with each other without the need for a trusted third party (Nakamoto, 2009). Smart contracts on blockchain networks are the next logical progression for the Internet. The Internet and globalization disrupted in many ways Macaulay's notion of social contracting. Business conducted online, in different parts of the world, and in different timeframes does not lend itself to brief conversations and handshakes. Establishing trust and reputation in online exchanges has been a challenge for e-commerce.

Blockchain technology can streamline online exchanges and reduce corruption, mistakes, fraud, and tax evasion. This is possible because blockchain technology is at its least the most reliable online tracking system yet developed. With a timestamp server, a chain of timestamps is created that publishes the hash of the transaction and proves the data must have existed at a particular time. The proof-of-work system involves scanning for value and ensuring that it cannot be changed (Nakamoto, 2009).

Blockchain can provide and build trust and reputation

Bitcoin operates on a blockchain network that has been touted since its inception as being “trustless”. In this context, “trustless” does not mean that the participants on the network cannot be trusted. Instead, it means that there is no need for a trusted third party. Without a trusted party, transactions must be publicly announced. This is achieved via a system that allows participants to agree on a single history of the order in which transactions were received. The payee needs proof that, at the time of each transaction, the majority of nodes agreed it was the first received (Nakamoto, 2009).

For exchanges conducted purely online, there is little risk that one of the parties will not fulfil their part of the deal. This is because both the payment and the delivery are executed by the smart contract. The blockchain manages the exchange of the two. This scenario saves time and costs. It means that the parties to a transaction take a much more active role in meeting their respective obligations. The exchanges feel almost cash-like in their immediacy and immutability. Because transactions cannot be reversed, the need for trust is eliminated (Nakamoto, 2009). With these mechanisms in play, the network can advertise to everyone that a transaction has been completed and the reputation of the participants in the completed exchange is enhanced automatically for all to observe.

However, online transactions become a bit more complicated when the exchange is payment for the delivery of a physical item, for example a widget. The delivery of a widget would be managed off-chain and would require human intervention to complete delivery. In this case, one solution is for the smart contract to provide an escrow service until such time that the widget has been successfully delivered. Of course, this may reduce the risk for the party paying for the widget (they will not authorize release of the funds on escrow to the sender until they receive the widget), but it leaves the sender exposed to two obvious risks. The first risk is that the party receiving the widget does not release the funds from escrow. However, this risk is quite low as the terms of the escrow will mean that the funds remain held in suspense until the dispute about delivery of the widget is resolved. The second risk to the sender is that the widget is sent to the wrong recipient, stolen, or not delivered for some other reason. In this case, the sender has parted with the item but has not been paid. This second risk can eventuate as readily off-line and off-chain as it can on-chain. The blockchain does not give rise to the risk of the missing widget and it cannot eliminate it. Equally, the presence of a bank or trusted third party would not have reduced or eliminated that risk. In practical terms, where the transaction value is low, the party at risk is likely (implicitly) to assume (that is, accept) the risk. When the transaction value is high, the risk solution probably lies in an insurance policy.

As we can see, these qualities of blockchain technology as applied to commercial transactions are not absolute, but are dependent on the circumstances.

To appreciate the importance of proving and managing trust in e-commerce, it is important to consider the notion of uncertainty, perceived risk, and unreliability. The more certain the parties are that something will happen, the less they need to consider whether or not they trust it (Christopher, 2017). When business is conducted online, trust becomes even more important. The usual norms associated with personal contact and social interaction are not available. The parties cannot rely on their intuitive judgements about a person’s trustworthiness. This is why credit card companies are enlisted for these transactions – the credit card provider has done the due diligence.

In order to eliminate credit card companies and other trusted (but expensive) third parties from the transaction network, the blockchain has mechanisms to build reputation for its participants.

Trust is built when the blockchain confirms to the entire network that a transaction was completed. Building reputation requires a broader dynamic. The ability to assess the reputation of a member in an online community is an essential need that arose with the launch of the Internet. The reputation gained by sellers and buyers in e-commerce communities like eBay is based on the feedback they provide about each other after the conclusion of a commercial transaction. This reputation rating system is vital for all e-commerce because reputation creates trust, and without trust there can be no commerce (Rietjens, 2006, 55).

Many Bitcoin exchanges have designed trading platforms that provide information about the number of trades undertaken by each trader and the ratings provided by other users. The feedback is represented by colour-coded dots and percentage rankings to reflect each trader's level of recent trading activity and the satisfaction of their customers. However, these apps are not built into the blockchain network and so suffer from a lack of decentralization; they depend upon the trustworthiness of those providing the feedback.

It is an essential ingredient of any e-commerce reputation system to manage the integrity of feedback and to ensure that it is provided only by genuine users (and not, for example, by fake identities created by the person or persons who want to synthesize an improvement in their reputation). Anyone can browse eBay, but in order to join in the business of this community, buyers and sellers must first be registered with the platform. Exchanges are only possible when users are signed into the system with their unique identities. Users do not usually use their real name or identity on eBay. Instead, users have a pseudonym (for example, "carlover" or "allroundaussie"). Although these pseudonyms protect the privacy of the members of the community, they are linked back to genuine pre-validated email addresses and credit cards. This system ensures that real people are the puppet-masters of their avatars and that they must behave according the rules of the marketplace. Under the rating system, the more stars received by a member, the more reliable and trustworthy they are, increasing their popularity with other members, and thereby resulting in significant economic advantages for those users (Kollock, 1999).

In the case of reputation of goods and services and their suppliers, the solutions available to prevent feedback abuse are generally reliable but centralized under the control of a few large Internet companies. However, by building a decentralized and distributed feedback management system on top of the blockchain, it is possible to provide reliable reputation ratings (Carboni, 2015). A key feature of this system would be to attach more weight to the feedback of an established and trusted user on the network than new identities.

This is important for anyone wanting to conduct business with a particular person or organization for the first time. eBay manages this by allowing new sellers to offer only a small number of items for sale until they reach a certain level of trustworthiness, as established by the feedback ratings from those first-run customers. Reputation is preserved in this way as a reflection of how much the users of a network trust another participant.

The Legal Implications for Blockchain and the Law in Action

There are two approaches for parties to adopt when agreeing to manage their financial and asset exchanges via a smart contract. First, they can let all of the programmable logic and code in the smart contract represent the agreed terms and conditions. The problem with this approach is that it may be difficult for one of the parties to know how to read the code and therefore understand how it will behave. The second approach is for the parties to share an external document that discloses all the legal terms and conditions that will bind the parties and that may in part also reflect the way that the smart contract will behave. This too has its dangers. For example, it would be important to ensure that whatever is said in the external document accords with the way that the code will behave. Relying on the established doctrine of mistake, the parties would by mutual agreement or upon receipt of a court order modify the code of a smart contract to reflect their actual intention. This should be sufficient to ameliorate any concerns arising from the very real possibility of mistake.

If trust has already been established between the parties, there will be little cause for concern as to what the code will do or whether or not there is an external document that articulates in plain English (for example) the way that the code will behave. There are certain behaviours in the physical world that are undesirable and obstructive in business, but which are circumvented by smart contracts. For example, oppression, delay, or hold up. Hold up occurs when one contracting party threatens another with economic harm unless they grant a concession of some sort to the threatening party. When a smart contract is managing the exchange between the parties, the obligations on both sides of the transaction are effected simultaneously and subject to the agreed terms that have been coded into the application. The nature of smart contracts confines their use to certain types of online transactions or transactions where payment will be automated upon the tracking of a certain event. This makes it difficult for one of the parties to cause delay in delivery or payment.

Because contracts are social tools as well as legal instruments, expectations and relationships are as important in contracting as legal obligations (Levy, 2017). In an online business environment, it may be easier to communicate to the rest of the community (for example via social media) if there is an untrustworthy participant, but the system is not immune to malicious attacks. Because reputation is built on feedback, the effect of this phenomenon makes it more problematic for business to suffer a bad review than to be sued for failing to meet a certain obligation under a contract. Any self-correcting mechanism could enhance the trust protocols that underpin the technology. This issue supports the case for a decentralized and possibly incentivized feedback-based reputation system to be built into blockchain technology.

What is missing from this discussion are the obvious problems that may arise when a smart contract fails to deliver on its promise or does not behave in a way that was expected by the parties. The legal consequences of these circumstances give rise to their own peculiar problems. For example, identifying pseudonymous parties, deciding jurisdiction, and options for the non-litigious resolution of the dispute. These problems vary in magnitude and volume depending upon the types of blockchain networks and environments that underpin the smart contracting. For example, the public Bitcoin blockchain is permissionless and operates as a financial transaction network. These smart contracts have very different features to those that may arise in private chains, where users are known to the system.

The problems arising where the users are known only by their pseudonyms and where jurisdiction is in dispute are more relevant to and prevalent in a public chain environment. However, these problems are not insuperable and nearly always arise in large public blockchain environments (such as Bitcoin). If the parties know each other and could have resolved these matters in an analogue transaction, there is no impediment to them resolving or prosecuting a dispute in the usual way.

Conclusion

In summary, this analysis has focused on the way that blockchain's trust and reputation protocols have restored to online business some of the features of social contracting that were lost with the advent of the Internet. Blockchain-enabled smart contracts bring more certainty and reliability to online transactions than has been available to e-commerce environments for the past twenty years.

It is clear that smart contracts will serve an important function in the automation of transactions as more of our business and social exchanges migrate to programmed applications and platforms that manage our online relationships. To ensure this smooth transition and to support the network of social contracts that sit within this ecosystem, it is important to keep in mind that not all transactions and exchanges are purposively contractual in a legal sense. Those who program and use smart contracts will benefit from delineating between social exchanges versus commercial contracts, as well as contracts that create enduring relationships from those that manage more casual affairs. Smart contracts can deliver significant benefits to the way that we manage supply chains and regulate variable payments. As research continues into the use of smart contracts, it will be useful to look at the way that different types of social exchanges are conducted in the analogue (offline) world, in order to emulate that experience online.

About the Author

Philippa (Pip) Ryan is a Barrister and Lecturer in the Faculty of Law at the University of Technology Sydney (UTS), Australia. Her PhD reclassified the liability of third parties to a breach of trust. Her current research explores contracts and trustless relationships enabled by blockchain technology. Pip designed and coordinates legal technology subjects and in conjunction with the UTS Connected Intelligence Centre, she is developing writing analysis software to improve students' self-assessments. She is on the industry advisory board of the Australian Digital Commerce Association, she is the Deputy Chair of the Australian Computer Society's Blockchain Technical Committee, and she is a member of the Standards Australia Blockchain Technical Committee.

References

Beale, H., & Dugdale, T. 1975. Contracts between Businessmen: Planning and the Use of Contractual Remedies. *British Journal of Law & Society,* 2(1): 45–60.
http://doi.org/10.2307/1409784

Carboni, D. 2015. *Feedback Based Reputation on Top of the Bitcoin Blockchain.* ArXiv.org.
https://arxiv.org/abs/1502.01504v2

Christopher, C. M. 2016. The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain. *Nevada Law Journal,* 17(1): 139–180.

Doddridge, J. 1630. *The English Lawyer.* London.

Eigen, Z. J. 2008. The Devil in the Details: The Interrelationship Among Citizenship, Rule of Law and Form-Adhesive Contracts. *Connecticut Law Review,* 41(2): 389–430.

Kastner, T. 2010. The Persisting Ideal of Agreement in an Age of Boilerplate. *Law & Social Inquiry,* 35: 793–823.
http://dx.doi.org/10.1111/j.1747-4469.2010.01202.x

Leib, E. J., & Eigen, Z. J. 2017. Consumer Form Contracting in the Age of Mechanical Reproduction: The Unread and the Undead. *Illinois Law Review,* 2017(1): 65–109.

Levy, K. E. C. 2017. Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science Technology and Society,* 3: 1–15.
https://doi.org/10.17351/ests2017.107

Kollock, P. 1999. The Production of Trust in Online Markets. In E. J. Lawler, M. Macy, S. Thyne, & H. A. Walker (Eds.), *Advances in Group Processes:* 99–123. Greenwich, CT: JAI Press.

Macaulay, S. 1963. Non-Contractual Relations in Business: A Preliminary Study. *American Sociological Review,* 28(1): 55–67.
http://dx.doi.org/10.2307/2090458

Macaulay, S. 1977. Elegant Models, Empirical Pictures, and the Complexities of Contract. *Law & Society Review,* 11(3): 507–528.
http://doi.org/10.2307/3053130

Macaulay, S. & Whitford, W. C. 2015. The Development of Contracts: The Law in Action. *Temple Law Review,* 87: 793–806.

Nakamoto, S. 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin.org.
https://bitcoin.org/bitcoin.pdf

Rietjens, B. 20016. Trust and Reputation on eBay: Towards a Legal Framework for Feedback Intermediaries. *Information & Communications Technology Law,* 15(1): 55–78.
http://dx.doi.org/10.1080/13600830600557935

Scott, J. 2009. Empirical Studies Strike Back against the Force of Contract Theory. *UCL Jurisprudence Review,* 4: 256–257.

Somervell, L. J. 1953. *Pharmaceutical Society of Great Britain and Boots.* [1953] 1 QB 401; [1953] EWCA Civ 6; [1953] 1 All ER 482, [1953] 2 WLR 427.

Weber, M. 1968. *Economy and Society.* G. Roth & C. Wittich (Eds). Oakland, CA: University of California Press.

Citation: Ryan, P. 2017. Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain. *Technology Innovation Management Review,* 7(10): 14–21.
http://doi.org/10.22215/timreview/1110

Keywords: blockchain, legal, law, smart contracts, trust, reputation, online transactions

Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector

Mark A. Engelhardt

> “*Blockchain is a way for people to solve problems by sharing things.*”
>
> Diego Espinosa
> Founder and CEO, Healthcoin

Health services must balance patient care with information privacy, access, and completeness. The massive scale of the healthcare industry also amplifies the importance of cost control. The promise of blockchain technology in health services, combined with application layers built atop it, is to be a mechanism that provides utmost privacy while ensuring that appropriate users can easily add to and access a permanent record of information. Blockchains, also called distributed ledgers, enable a combination of cost reduction and increased accessibility to information by connecting stakeholders directly without requirements for third-party brokers, potentially giving better results at lower costs. New ventures are looking to apply blockchain technology to solve real-world problems, including efforts to track public health, centralize research data, monitor and fulfill prescriptions, lower administrative overheads, and organize patient data from an increasing number of inputs. Here, concrete examples of the application of blockchain technology in the health sector are described, touching on near-term promise and challenges.

Introduction

Health is the foundation of an engaged and happy life, and modern humans have been the fortunate beneficiaries of great advances in medical technology (Collins, 2015). With each new technology, more clues become available to decipher the problems that plague our well-being. The advent of individualized information from cheaper genome sequencing, the Internet of Things, and widespread collection of health data may enable researchers to solve formerly inaccessible health problems. However, when this massive quantity of data is spread out with limited access, is in forms not conducive to sharing, cannot be easily packaged for computational methods, or does not exist as a complete record, it is impossible to perform the complex data analysis required to arrive at solutions.

To address these fundamental challenges in health data management, innovators are focusing on four main areas:

1. *Putting the patient at the centre.* For most patients, sustaining health involves many interactions with a variety of healthcare providers and data collection tools, all of which generate information critical to making informed and appropriate healthcare decisions. There is increasing agreement that information should be available to patients such that they can be active agents in their own care, and patient participation and involvement has become a cornerstone of modern medical practice (Kitson et al., 2013; Stewart, 2001). Caretakers also require access to medical information, however, patients increasingly want to be in control of what information caretakers receive, and under what circumstances.

2. *Privacy and access.* Equally important to consider is the intimate and highly personal nature of health information. Health information must be private and accessible only by appropriate parties, for appropriate reasons, at appropriate times. Some jurisdictions have legislation in place to protect personal

information, (e.g., Canada: Minister of Justice, 2015; United States: Department of Health and Human Services, 2013), which new technologies must take into consideration. Despite the complexity of the problem (de Lusignan et al., 2014; Mold et al., 2012, 2015; Tieu et al., 2016; Woodman et al., 2015), there are efforts underway to enable each adult to have full access to their own medical records (Hankewitz, 2016; Kelsey & Cavendish, 2014; Suberg, 2017).

3. *Completeness of information.* Currently, medical information is frequently held by individual providers or private data collectors without full patient access (Das, 2017). This limits the ability of patients to explore options, contribute and correct errors in their own data, and share their information with new practitioners to fully define a medical history. Patient-centred information sharing should enable the patient increased control and better outcomes by ensuring that complete health information is available to the right people at the right time. Lack of information interoperability is detrimental to using new data-based diagnostic technologies.

4. *Cost.* There is a crisis in the cost of healthcare, and expense looms large behind every discussion of changes to its delivery. Health expenditure per capita has increased 60% over the past 10 years (The World Bank, 2015). In countries such as Australia, the United Kingdom, and Canada, health expenditures represent about 10% of GDP; in the United States, this number is closer to 17% (The World Bank, 2015). Paradoxically, outcomes in the United States are worse than elsewhere (Avendano & Kawachi, 2014), a clear indicator that there is waste in the system. A recent study showed that older people with diagnosed chronic diseases face catastrophic health expenditure even in some of the wealthiest countries in Europe (Arsenijevic et al., 2016). It is of note that the population in developed countries is, on average, aging, and therefore this situation can reasonably be expected to worsen in the future.

Technology can be part of the solution. A study by McKinsey & Company estimated that more than $300 billion could be recovered per year by using health data creatively and effectively, with two-thirds of that in the form of reductions to national health care expenditure – about 8 percent of estimated healthcare spending at 2010 levels (McKinsey & Company, 2011). In particular, blockchain technology has the potential to hold and control access to massive amounts of anonymized health data, enabling new research and new insights, while at the same time protecting the privacy of patients. Importantly, blockchain technology serves as a protocol to connect important stakeholders to data without requiring an expensive layer of data mediators and escrow services to broker trust, removing middle management and its associated cost from the data-sharing equation. Better data sharing between stakeholders should also reduce waste, for example, that due to duplicate testing that occurs when healthcare providers are not aware of each other's actions.

Don Tapscott, a leader in the industry, has said "though there are many culprits, the root of the problem is our industrial-age thinking about delivering healthcare, where data is hoarded, patients are assumed to be ignorant, and where healthcare is only available when you’re in the system. This leads to costly and ineffective care. Blockchain promises to change that. We can fix healthcare by basing it on a set of new principles — collaboration, openness, and integrity, and where the patient co-creates their own data with full transparency into it." (Schumacher, 2017). Blockchain technology is being applied increasingly in the finance sector, but as Mo Tayeb of Medicalchain points out, "your body is more important than your bank account" (personal communication, August 25, 2017). It is now time to take what has been learned and apply it to something even more important: health.

Blockchains are Decentralized, Immutable, Private, and Agents of Trust

At its core, blockchain technology consists of a few straightforward ideas with interesting properties that align significantly with important healthcare challenges.

Blockchains are distributed ledgers – sequential lists of transactions with identical copies shared and maintained by multiple parties. There is no single source that claims authority over the true data, which is instead declared by consensus amongst the multiple parties holding the data (Figure 1). Because of this, blockchains are referred to as *decentralized.* This arrangement protects the data from tampering not just by individual keepers of the blockchain, but also external attempts at damage. In one example, the decentralization of blockchain solutions would offer intrinsic protection against assaults such as the recent WannaCry ransomware attacks because the blockchain would only be affected if simultaneously attacked at many sites (Mattei, 2017).

An Introduction to Blockchain Technology in the Healthcare Sector

Mark A. Engelhardt

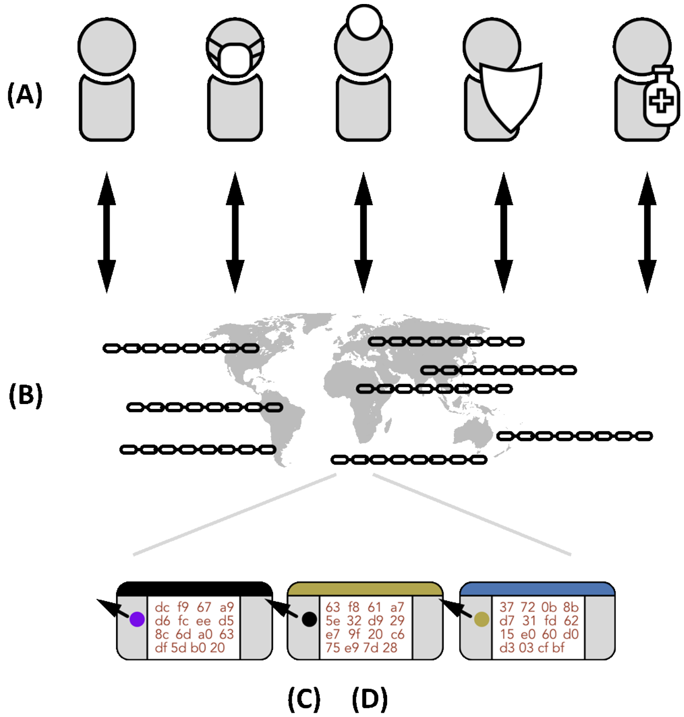

Figure 1. Stakeholders (A) have selective and controlled access to data elements stored in a set of identical verified blockchains held at multiple locations (B), wherein each block contains auditable information about creation and sequencing (C) and encrypted private information (D). Information about sequencing could be in the form of a hash that acts as a signature to uniquely describe one or more previous blocks in the chain. Although all arrows between (A) and (B) are shown as double-headed, read and write access to the blockchain would be stakeholder-dependent as defined in smart contracts.

Each record in the chain includes precise information about when it was created and the cryptographic signature of the preceding record in the chain, along with additional arbitrary information. The signature – or hash – consists of a cryptographically generated sequence of letters and numbers of a defined length that uniquely identifies any digital entity. Changing any record would change its signature, and would therefore create an easily detectable break in the chain. Records can only be added, never removed, and only by consensus of the maintainers of the distributed copies. Blockchains are thus *immutable.*

Information in each block can be encrypted such that only the holders of the correct cryptographic keys can access the information in it. Blockchains are thus *private.*

An emergent property of this structured and shared data is that it eliminates the need for trust brokers between parties who require access to data. Even if not all data in a blockchain can be accessed due to privacy constraints, each stakeholder can prove with mathematical certainty that they are in possession of an exact and unmodified copy of the historical data stream. Everyone has equal information, and well-constructed blockchains ensure that all stakeholders can see all the data required to audit the transactions on the chain. The decentralized and immutable nature of blockchain implementations combined with this transparency means that they convey *trust.*

Additional rules, often referred to as smart contracts, can be built into these decentralized, immutable, private, and trusted ledgers to regulate how the data can be used. Smart contracts are not a core feature of every blockchain, but are often central to their use in the complex world of healthcare. These contracts benefit from the properties of the blockchain: once set, a smart contract built into a blockchain is immutable and can be trusted to operate the same way, using trusted information shared equally between all parties, indefinitely. Kristin Lauter, Principal Research Manager at Microsoft, has said "you can propose any crazy encryption you want and say it's secure. Why should anyone believe you?" (Molteni, 2017). Blockchain technology answers: bitcoin, a high-value implementation of blockchain, has been open for years to hackers with a lot to gain but remains secure. This cannot be construed as a guarantee of future performance, but it does provide some measure of confidence.

It seems important to add, given the frenzy in the press regarding blockchain technologies (Panetta, 2017), that blockchains are tools with useful properties that may be applicable in many areas, but cannot by themselves solve the panoply of issues endemic to our institutions. Even with perfect technology, the information being put onto a blockchain can still contain faults, and any rules for accessing and adding new information to blockchains must first be created and agreed to by the holders of the consensus. The benefits of applying blockchain technology can be fully realised only after investment in careful technical and administrative planning that includes all stakeholders.

Examples of Blockchain Technology Applications to Healthcare

In general, blockchain technology is best suited to projects where:

1. There multiple stakeholders contributing.

2. More trust is required between parties than currently exists.

3. There an intermediary that could be removed or omitted to increase trust or efficiency.

4. There is a need for reliable tracking of activity.

5. There is a need for data to be reliable over time.

An examination of some real applications may give a better understanding of how blockchain technology works in healthcare, what it offers, and the current state of the industry. The following specific examples have been chosen to clarify concepts, and do not indicate the importance of one approach versus another. A full exploration of blockchain technology companies throughout the health sector is beyond the scope of this review, but an attempt has been made to identify a collection of international and noteworthy examples.

Busting prescription drug fraud

Prescription drug fraud is a well-defined challenge to which blockchain technology can be applied. In one example, the blockchain company Nuco attempts to address three common exploits employed to execute prescription fraud: modifying numbers to change the prescription itself, duplication of prescriptions (e.g., photocopying), and so-called "doctor shopping" whereby fraudsters visit many doctors to collect as many original prescriptions as possible (Kesem Frank, personal communication, August 24, 2017). To address these problems, experts have called for monitoring programs to be installed that improve access and response time, scan prescription data to flag suspicious purchasing patterns, and can alert physicians and pharmacists (McDonald & Carlson, 2013). Nuco identifies the problem as an "open-ended loop", meaning that there is incomplete feedback between the prescription writers (physicians) and the prescription fillers (pharmacists). This fragmented communication is the kind of problem blockchain can solve (Figure 2).

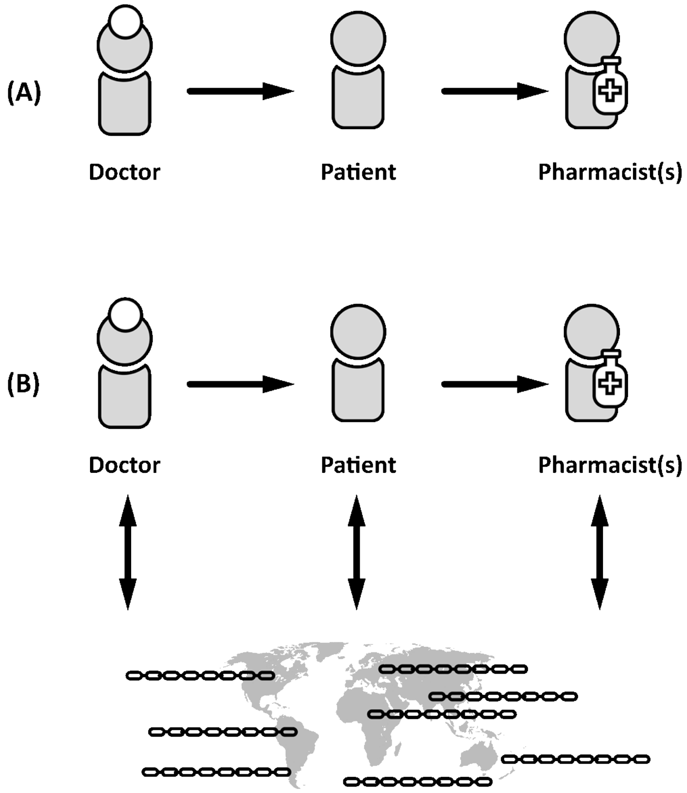

Figure 2. (A) An example of an open-ended loop, where a patient is given a prescription by a doctor, who then delivers it to one (or more) pharmacist(s). A pharmacist has no knowledge of whether the prescription is original, accurate, or previously filled. (B) To close the loop, transactions are stored on blockchains. Each stakeholder can access and add to the blockchains as appropriate. For example, a doctor can add record the original prescription and a pharmacist can check that the prescription is unaltered; a pharmacist can record actions on a prescription, and the doctor or another pharmacist can check its status.

Nuco's blockchain-based solution to the prescription fraud problem works as follows: when a prescription is produced by a doctor, a machine-readable code is attached that serves as a unique identifier. This unique identifier is then associated with a block of information including the name of the drug, the quantity, the anonymized identity of the patient, and a timestamp. When the prescription is filled by a pharmacist, the symbol is scanned, the attempt to fulfill the prescription is recorded on and compared against the blockchain, and the pharmacist is quickly informed whether the prescription is eligible to be filled and given information to verify its accuracy.

Copies of the blockchain, or distributed ledger, are held by multiple stakeholders in a *decentralized* network. These stakeholders might include pharmacy chains, insurance providers, auditors, or hospitals, each of whom has a vested interest in solving prescription drug fraud and is large enough to dedicate resources to the computing infrastructure required. Due to the encryption of the blockchain information, *privacy* is maintained when it is passed between stakeholders, and each of the stakeholders can only access information to which they are specifically entitled through the possession of the correct cryptographic keys. Each of the stakeholders can *trust* that the information they have is accurate because each has an unbroken chain that is identical to the other chains and that they can audit to ensure its integrity.

This solution illustrates an example of a *permissioned blockchain,* in which only specified parties can read information and transact. It is one of two common broad implementations of blockchain technology; the other is public chains, of which an example is given below.

The Nuco solution integrates on top of existing patterns of usage and uses existing technologies (e.g., the pharmacist only requires a smartphone or similar device to read the unique identifier), providing *interoperability* with existing protocols. Interoperability will be an important consideration as new blockchain projects interface with both current and new technology for information storage.

HealthChainRx and Scalamed are also working on blockchain solutions to combat prescription fraud and are close to releasing solutions. Both have expressed a strong desire and emphasis on giving patients control over their data, including the ability to authorize who can use it and how (Dave Evans and Tal Rapke, personal communications, August 2017).

Scalamed plans to adopt a public blockchain rather than a permissioned chain (see Nuco, above), which presents an opportunity to differentiate between these two approaches (Tal Rapke, personal communication, August 27, 2017). In public blockchains, storage and maintenance of the blockchain is not restricted to trusted stakeholders. Instead, anyone who participates is remunerated for handling the encrypted data structure. The blockchain is *decentralized* across many public nodes that work together to verify and process transactions, resulting in *trust* that the chain is accurate. They do this without the ability to decrypt private data. The choice of one of these different models, permissioned *versus* public, is a fundamental decision made early in any blockchain project.

Patient-centred medical records

If there is a common undercurrent that runs through almost all blockchain technology companies working in the health sector, it is the desire to enable people to exercise more personal control over the data collected about them. Physicians are already inundated with more information than they can deal with, and much, much more is coming. A blockchain solution can lighten this burden on the doctor by creating a higher level of organization, accessibility, and amenability to time-saving digital tools while also further engaging the patient in their own care.

As an initial project, Medicalchain has tackled hospital discharge summaries, which include a summary of treatment and necessary follow-up care. Hospitals have incentive to both ensure these documents are free of liability-creating errors and process them quickly to free up beds for the next patient in the queue. Currently, information is siloed: transferring records over municipal boundaries can require written requests, and problems with duplication of data, fraud, and inaccessible data are rampant (Mo Tayeb, personal communication, August 25, 2017). Medicalchain has introduced a digitized solution that leads doctors through a structured discharge process that reduces errors and omissions and speeds up review by senior staff. They are currently moving this system to a blockchain, which will enable efficient *decentralized* sharing of data between stakeholders (e.g., hospitals in different networks and health insurance providers) who will be able to *trust* that the patient data is private due to encryption and historically accurate due to the immutable nature of the blockchain.

More ambitiously, Medicalchain is currently also developing a permissioned blockchain shared across a network of trusted international healthcare institutions to help patients receive care internationally without complicated collection and transfer of medical records (Mo Tayeb, personal communication, August 25, 2017). Their proposed solution for enabling international blockchains is an opportunity to discuss another important concept: on-chain *versus* off-chain storage of information. Some jurisdictions do not allow private healthcare data to be stored externally. How then can one construct an international shared data structure? The answer may lie in the same type of cryptographic signature that enables each block of the blockchain to uniquely identify the block that it follows. Similarly, each block can contain cryptographic signatures of remotely stored documents that can be used to prove that a document has not been changed in any way. Data can be kept in each patient's home jurisdiction, and then, when transferred by the patient, proven through signatures recorded and shared through the blockchain to be the complete and accurate record of the patient's medical history. In this scenario, only proof that the document is genuine is stored internationally on the blockchain; the actual documents can sit (in encrypted form) in home jurisdictions until the owner of the data (the patient) decides to share them. Storing cryptographic signatures in this way is known as "off-chain storage" and is a common theme in blockchain technology for the health sector, both to deal with regulatory hurdles and due to the prevalence of large data files such as imaging data, the inclusion and sharing of which on the blockchain precludes a streamlined solution.

Healthcoin, an initiative that first developed a blockchain-based solution for helping people work together to improve diabetes symptoms has since expanded their vision towards building a system to construct a global electronic health record system. They identify a value proposition for patient-centred information control that consists of three principles: 1) give the complete data to the user, 2) allow the user to channel their data to its best use, and 3) allow users to broadcast outcomes with mechanisms in place to certify the broadcasted information (Diego Espinosa, personal communication, August 28, 2017). Healthcoin sees themselves as not being in the healthcare business so much as the data sharing business, with the patient sitting at the control panel.

This is a busy space, and analogous projects to connect patient information between stakeholders are being attempted by numerous other players, including BurstIQ, Factom, GemOS, HealthCombix, MedRec, Patientory, and SimplyVital. Even IBM's Watson is getting into the game (Byers, 2017). Patientory, with a solution that attempts to bridge existing electronic medical record systems in the United States, appears to be the closest to having a real product in the hands of patients (Patientory, 2017).

BurstIQ presents a vision of what can be done once blockchain technology becomes the major medium to store patients' data. They see the future of care at the junction of precision medicine, delivering treatments specific to a particular patient's needs, and machine learning, where artificial intelligence is used to learn from health trends and particular patients' histories (Frank Ricotta, personal communication, August 25, 2017). BurstIQ aims to integrate data streams to gain new insights into individual best health outcomes and help people realize them.

The overt shift to patient responsibility over their own data in these blockchain-based solutions represents a significant change. HealthCombix, in collaboration with PointNurse, is attempting to address this by introducing a nurse-mediated layer to make sure that the data that ends up in the immutable blockchain record is accurate, that it has been transferred correctly to the patient, and that the patient understands how to curate, update, and control access to their records (Cyrus Maaghul, personal communication, August 25 2017.) Another differentiating feature of HealthCombix is their plan to tie their system into a specialized hardware component that can be used to reliably monitor patients and introduce quality records to the blockchain. Bowhead is another initiative interested in using a hardware component to feed trusted information to a blockchain.

Given that these solutions are developed in parallel and in the absence of standards, a new interoperability problem emerges. QBRICS and Nuco (Aion) have initiated projects to develop blockchain-based technologies to translate and consolidate information from multiple sources to reconstruct patient data fragmented across platforms.

Connecting the dental industry

The dental industry is a highly fragmented market consisting of many independent practitioners. Dentacoin is an initiative that aims to use blockchain technology to connect dentists, patients, and suppliers (manufacturers and laboratories) globally. Phase I of their project was the implementation of a review platform that relies on the immutability and decentralization of blockchains and the transparency and reliability of blockchain-bound smart contracts to create trust in the review process. Desirable actions, such as writing a review, are rewarded by transferring cryptocurrency to the patient, which can then be used to purchase dental services from participating practitioners. Dentists are rewarded for participating through access to market research and cryptocurrency accepted by manufacturers. Dentacoin is banking on the trust and decentralization inherent in blockchains to enable an economy of scale to develop between the participating parties, without requiring additional brokers to manage the interactions between each individual piece of the network. Of note is that this blockchain technology endeavour is dipping its toes into real waters: they already have two proof-of-concept clinics that accept payments in the Dentacoin currency, and several dozen real practices registered for their review platform (Donika Kraeva, personal communication, August 28, 2017). Future phases of the Dentacoin project plan to use their incentive strategy to encourage patients to educate themselves about dental care, set up insurance contracts between patients and dentists that reward patients who perform a minimum of dental maintenance, and to serve as a patient health record, analogous to the patient records covered in the previous section.

The creators of Dentacoin chose to implement a public blockchain because they felt that a more centralized private blockchain would be less trustworthy due to the more limited number of verifiers ensuring transaction fidelity. As with most initiatives mentioned in this article, they favour the storing of private information off chain (see Medicalchain, above).

Key Additional Areas That May Benefit From Blockchain Technology Integration

Blockchain technology may revolutionize medical research and individual care

The storage and sharing of health information presents an enormous challenge, including some important risks to privacy, and fantastic opportunities, including the potential to develop a practical understanding the health of unique individuals instead of generic humanity. Blockchain technology companies are diving into this space and promising a new era of research and discovery propelled by analysis of aggregated longitudinal health information from individuals in the context of that from the population at large, and by a new ability for researchers to access data they need to gain new insights.

As the decreasing cost of whole genome sequencing approaches $1000 USD, and still meaningful but somewhat less complete analysis even cheaper, the collection of this data has become increasingly common. As an example of the scale of experiment possible in the past couple of years, one recent study employed whole genome sequences of over a thousand participants (Lippert et al., 2017); in another, two hundred thousand participants contributed genome-wide markers (Lo et al., 2016). The application of this scale of data is potentially revolutionary. The Lo study, for example, found genetic correlations with psychiatric data that may have been impossible to locate with fewer markers. Currently, finding large data sets to better the understanding of interactions between disease and other traits and aspects of human lives is a difficult process filled with many obstacles and much paperwork and bureaucracy. Future understanding of human health may benefit enormously if the data now being accumulated by humans around the world can be made easily accessible to researchers. This must be done while adhering to ethical standards and with maintenance of privacy through effective anonymization and ownership of the data by the individual whom it describes, including the ability to grant and revoke access to it. There is evidence that people want this control, and also that many want their data to be useful: a study of research participants receiving whole genome sequence results expressed a strong desire to receive all results, including the raw data, and to maintain the privacy of the data; also, about a third of them consented to sharing their data (Sanderson et al., 2016). Although there is evidence that some incentives may be required (Pevnick et al., 2016), perhaps with the right communication and protections in place, even more people would be willing to contribute their data to the common good.

As with many aspects of this nascent industry, it will be important to get things right: if privacy and ownership concerns cannot be addressed, the willingness of people to contribute their information may evaporate. Operators in this space are aware of the challenge and they are attempting to grapple with it (Jagadeesh et al., 2017). Encryption and keyed access are a first level of protection, but more work is necessary before solutions are ready to be rolled out widely. It is not a simple problem to store private information into a public space, maintain control of who can access it and how it is applied, and at the same time deal with real-world problems such as key loss and changes in an individual's ability to manage their own data, not to mention navigate the process of carefully defining who should have access to what information and under what circumstances (Tanner, 2013).

Why is blockchain technology an interesting tool for this kind of sharing? In addition to the baseline level of anonymization afforded by the encryption of data (but which non-blockchain solutions could also employ), there are several reasons. The first is the immutability of the data: once stored, data for research can be trusted not to change. Second, storage would be transparent: it would be clear to participants what data was and was not available, and replication of studies to verify results would be more straightforward, and there is good evidence that closer monitoring of studies is warranted (Chan et al., 2004; Dwan et al., 2013). Third, with tested and tried smart contracts in place, owners of the data could have confidence that they control their own data and could both grant and revoke access to it in anonymized form to enable research. The immutability of smart contracts due to their inclusion in the blockchain is no small thing: it provides confidence that once a relationship is established it will not be altered, and, as it continues to work as promised, that any contract is secure versus malfeasance.

The focus here has been on the collection of genetic information from our personal genomes, but this is not the only new stream of information that could contribute vast amounts of data to understanding our individual human health. An increasing body of evidence suggests that our microbiome contains information about our personal health, and sequencing efforts are already collecting mountains of bacteriological data (Lynch & Pedersen, 2016; Zhernakova et al., 2016). Also, with the advent of the Internet of Things, an explosion of devices is collecting longitudinal data about all aspects of our lives, such as heart rate, step cadence, exercise frequency, vocabulary complexity, diet – almost anything that can be imagined. Clearly, there are privacy issues here that must be considered, but this data, too, could be verified, or at least assigned confidence levels, and used to assess current health and help to inform life decisions for health maintenance and improvement.

Government
Governments are eager to determine whether the cost-saving promises of blockchain technology can be realized, and at the same time to encourage patient empowerment and advance medical research and care. In Canada, a Nuco-Deloitte collaboration has engaged with a publically-funded research institute to provide a solution that enables individuals to participate in genetic research, due to be announced in late 2017 (Kesem Frank, personal communication, August 24, 2017). In the United States, The Illinois Department of Financial and Professional Regulation is partnering with healthcare firm Hashed Health to build solutions that take advantage of blockchain and distributed ledger technologies to improve the efficiency and accuracy of cross-state medical licensure (Hashed Health, 2017). The United Arab Emirates and Estonia have also made investments in storing medical health records using blockchain technology (Anderson, 2016; Hankewitz, 2016). These are just a few examples of recent announcements, and the momentum is growing.

Blockchain technology is a fledgling endeavour and still must be aligned with current policies and procedures, especially in the healthcare industry. Recognizing that working within the strictures of government is a significant hurdle all on its own, the National Research Council Canada's Industrial Research Assistance Program (NRC-IRAP) has embarked on an experiment that uses blockchain technology (with its attendant immutability, decentralization and transparency) to organize and disseminate public data about its activities and the companies it serves (National Research Council of Canada, 2017). This is viewed as an achievable program that will demonstrate that a public blockchain can be used to hold government data, with a view to learning about, confronting, and addressing administrative hurdles to the framework, and ultimately lay down a path for more complicated data projects (e.g., health data) in the future (David Lisk, personal communication, August 29, 2017). Projects like this one may help to establish blockchain technology as an effective method to record and share government data and serve as an important building block for more sensitive initiatives in the future.

Auditing
As Brian Behlendorf, Executive Director of the Hyperledger project, on meeting the sustainable development goals of the World Economic Forum, put it on a recent Hashed Health (2017) podcast:

> *"Every [goal] involves a metric; every metric, in order to actually know if we are making progress against it or not, needs to come out of an accounting system of some sort, and the best way we know today to build an accounting system that is trustworthy, that is decentralizable ... is with blockchain technology."*

Effective and trusted tracking of transactional information at each step of a process in a transparent and immutable way is an over-arching trait of blockchain implementations. Therefore, the idea of auditing intersects much of what has already been discussed. One can imagine many instances where clear auditing of records in healthcare would be advantageous, including such examples as checking medical practitioner credentials, tracking and reconciling errors or ambiguities in patient data, and verifying insurance claims. One example of an initiative that tries to address some of these issues is Pokitdok, which has partnered with Intel to build a blockchain-based solution that provides identity management to validate every partner in a transaction (Miller, 2017). Two examples of what Pokitdok hopes this might enable are near-instant billing and insurance claim resolution, and instant auditing of pharmaceutical supply chains and provenance. iSolve is another company working in this space, and among other projects is working on end-to-end blockchain solutions to track medication distribution.

There are situations where the importance of careful tracking becomes painfully clear. Counterfeit and fraudulent medication is a growing problem, especially in parts of the world where regulation and cooperation between governments is lacking (McLaughlin, 2012). Detailed and trustworthy pharmaceutical provenance and chain-of-custody information could be built into a blockchain solution, such that local distributors and consumers could audit their own supply and combat fraudulent practices such as relabelling of expiration dates and counterfeiting (Buckley & Gostin, 2013; Khan & Khar, 2015; McLaughlin, 2012; Sprink et al., 2016). Pharmaceuticals are part of a much more general case: everything we consume affects our health, and recently major retailers and food companies have announced a collaboration to identify major areas in the global food supply chain that could benefit from tracking through blockchain technology (Aitken, 2017). It is worth bearing in mind that blockchain is not a magical auditing solution that addresses every challenge. It is a tool that can be used for trusted information storage and sharing, but these initiatives will also require systems to enter accurate and complete information in the first place.

Considerations For Future Blockchain Technology Development

Standards

Ultimately, standards will be important to guarantee interoperability between blockchains and to establish rules for the safe storage and transfer of information. Currently, development is dominated by prototypes and initial phases of projects with the primary concerns of functionality and proof of concept. A representative of Dentacoin expressed the general sentiment: "at the moment everyone should focus on the progress of existing solutions as well as new ideas and concepts that might not follow any standardization yet" (personal communication, August 28, 2017). That said, it is important to begin thinking about standards, and a standards group (ISO/TC 307) has been set up for blockchain (ISO, 2016). For those who wish to have a voice in the future of blockchain, this may be an important avenue for contribution.

Intellectual property protection and freedom to operate must be a key consideration for any blockchain technology initiative

These are early days for the use of blockchain technology in health applications, and exciting new ideas are everywhere. At the same time, fast-moving companies and individuals are taking the opportunity to claim broad swaths of the intellectual property space. A quick patent search reveals that the company EITC Holdings, for example, has 63 granted or pending patents in the United Kingdom with priority dates in early-2016 or later; if EITC has been as aggressive in the United States, they will own a significant portion of claims in the blockchain space. Patent applications do not publish for 18 months after the earliest filing date, so the extent of EITC's filing in the United States will not be known for some time. A report by Reuters suggests that EITC plans to file many more (Wagstaff & Kaye, 2017). Companies including IBM, Mastercard, Fidelity, and Bank of America have also been very active at claiming intellectual property in this area. The extent to which these early patents will be allowed in patent offices and upheld when challenged has yet to be tested. What is clear is that patents are being awarded in the blockchain sector in many worldwide jurisdictions and that forward-looking companies who wish to protect their intellectual property should develop a plan early on, at least to secure their freedom to operate. The effect that the current apparent centralization of control of intellectual property might have on the industry as a whole is unclear, but should be monitored.

Risks

Blockchain technology is only as good as its users; if low quality or incorrect information is put onto the chain, then what can be trusted through immutability and decentralization is that low quality and incorrect information will remain on the chain. Blockchain and supporting technologies offer many new opportunities, but care must be taken to evaluate the entire implementation, including what happens to information before and after it is on a blockchain. Interoperability solutions will have to be diligent about information that is stored, and include solutions for resolution of discrepancies and assigning confidence to different kinds of information.

Also, the movement to transfer information and control to the patient is laudable, but must be accompanied by education. As stated by Nicole Tay, a researcher in public health (personal communication), if "the whole point was to empower the patient and address the failures of our current system, which rely exclusively on the patient's trust, [and if we create a new system where patients are empowered to control their data but do not know what to do with it and end up engaging others to manage it for them], are we really moving away from a 'trust-based' management system?"

Hopefully, the industry will take advantage of the current hype to establish itself, but not stop asking difficult questions. There is a risk that consumers will be drawn in by the golden promise of longer and happier lives care of big data, which may be difficult to turn down even if there are risks. A poor outcome is expected for the blockchain industry if it moves too quickly in the early days and products are pushed out that are not ready. Although there are aspects of blockchain technology that protect against unauthorized access, a large breach of private data through a technical oversight could result in fear of what should instead have held only promise.

One interesting problem is that the ability to access data in the blockchain is through a "key", which is a unique sequence of characters and digits. If a key is lost, then the data it accesses becomes irretrievable. Losing access to a lifetime of health information through the loss of one of these keys is unacceptable, and solutions will have to be implemented to reconnect users with their data. Current solutions to this introduce back doors to accessing the private data on the blockchain, replacing one problem with another.

Another challenge is that, if the decentralization of a blockchain is broken, for example, if one company acquires access to most servers (more than two-thirds with current enterprise methods), then one agent can become the only agent of consensus and can modify the blockchain, contravening the immutability property. New technology for consensus and government regulation surrounding blockchain monopolisation may be necessary to protect against this eventuality.

Finally, a spectre on the horizon is the emergence of quantum computing and its predicted ability to break current encryption methods (Bernstein et al., 2017). It is not clear exactly when this will occur, but within the next decade seems possible (Kobie, 2016). We will have many problems if quantum computing resistant encryption is not solved by then, but if the entirety of one's health data is sitting in blockchains on publically accessible servers, then the privacy of that information will be at risk.

Conclusions

The application of blockchain technology to healthcare is in its infancy, and there are important challenges to face and big decisions to make going forward. Our societal concept of privacy has evolved in the face of challenges over the past decade and blockchain technology may continue to push at these boundaries, but also promises to deliver great rewards if embraced. If people are enabled to choose for themselves whether to adopt blockchain-based solutions, many may deem the risks of information loss minimal compared to the promise of an overall gain in privacy and control of one's data (assuming no major data breaches). They may be willing to risk even more for the promise of longer and healthier lives by releasing their own data into massive new collections of anonymized population health data, which could then be processed by artificial intelligence to develop personalized healthcare strategies.

The promise of blockchain technology is to enable the efficient sharing of information with stakeholders while ensuring data integrity and protecting patient privacy. Proponents hope that it will bring power to the people and enable them to make positive decisions that improve their health and that of others around the world. They see a world where data is safer than ever before. Skeptics are concerned about the complications beyond the hype; what is envisioned is a massive disruption of the health sector, and there are many installed and invested parties who will act against that change, not to mention ethical, regulatory, and technical details still to figure out.

If the challenges of interoperability continue to be overcome, dependable privacy established, good anonymization protocols developed, and consensus achieved around the kinds of contracts needed to control information, then a new age of healthcare may be around the corner. These are significant challenges, but as described above, companies have already made significant inroads into addressing them even at this early stage. This century's technology giants have already shown us that they are good at using artificial intelligence to learn from data; the same kind of technology is poised to produce disruptive new insights with the kind of data now being produced around health, with privacy and patient control as an important central tenet. Some see this as an important step towards the "health singularity": a transformative event where individualized healthcare is delivered based on a deep understanding of the personal biology of each individual.

The potential of blockchain technology is currently being explored across many healthcare sector implementations. A close watch on the companies mentioned in this review, many of which expect to make major announcements in coming months, would be a good first step to keep apace of developments. The technology (and its marketing) is booming, and care should be taken to look beyond "white papers" and press announcements. Academic literature seems to be lagging, which leaves sources such as the press and critical discussions in online forums such as Reddit as primary options to seek sober second thought. It is an exciting time, with many new applications and implementations being discovered and developed, and full of much promise.

About the Author

Mark Engelhardt, holds a PhD from Stanford University in the United States and is a partner at Ovodenovo Intellectual Property Consulting, a full-service patent agency in Ottawa, Canada, where he combines multidisciplinary experience in biological and computational science with experience in intellectual property to help small- and medium-sized companies succeed and to help investors understand technology. He has a passion for non-profit work, and is currently supporting the Ottawa Youth Orchestra Academy as president of their board of directors. Connect through LinkedIn to chat about blockchain technology, intellectual property, non-profit work, and the interesting places they might intersect in the future.

References

Aitken, R. 2017. IBM Forges Blockchain Collaboration With Nestlé & Walmart In Global Food Safety. *Forbes,* August 22, 2017. Accessed October 1, 2017:
https://www.forbes.com/sites/rogeraitken/2017/08/22/ibm-forges-blockchain-collaboration-with-nestle-walmart-for-global-food-safety/

Anderson, R. 2016. Dubai to Use Blockchain Technology for All Government Documents by 2020. *Gulf Business,* October 5, 2016. Accessed October 1, 2017:
http://gulfbusiness.com/dubai-use-bitcoin-database-technology-government-documents-2020/

Arsenijevic, J., Pavlova, M., Rechel, B., & Groot, W. 2016. Catastrophic Health Care Expenditure among Older People with Chronic Diseases in 15 European Countries. *PLoS ONE,* 11(7): e0157765.
https://doi.org/10.1371/journal.pone.0157765

Avendano, M., & Kawachi, I. 2014. Why Do Americans Have Shorter Life Expectancy and Worse Health Than Do People in Other High-Income Countries? *Annual Review of Public Health,* 35(1): 307–225.
https://doi.org/10.1146/annurev-publhealth-032013-182411

Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. 2017. *Post-Quantum RSA.* International Workshop on Post-Quantum Cryptography: 311–329.
http://dx.doi.org/10.1007/978-3-319-59879-6_18

Buckley, G. J., & Gostin, L. O. (Eds.). 2013. *Countering the Problem of Falsified and Substandard Drugs.* Washington, DC: National Academies Press.
https://www.ncbi.nlm.nih.gov/books/NBK202527/

Byers, J. 2017. IBM Watson, FDA Aim to Tackle, Tame Blockchain for Data Exchange. *Healthcare Dive,* January 11, 2017. Accessed October 1, 2017:
http://www.healthcaredive.com/news/ibm-watson-fda-aim-to-tackle-tame-blockchain-for-data-exchange/433833/

Canada: Minister of Justice. 2015. *Personal Information Protection and Electronic Documents Act.* Ottawa: Minister of Justice (Canada).
http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html

Chan, A. W., Hróbjartsson, A., Haahr, M. T., Gøtzsche, P. C., & Altman, D. G. 2004. Empirical Evidence for Selective Reporting of Outcomes in Randomized Trials. *JAMA,* 291(20): 2457–2465.
https://doi.org/10.1001/jama.291.20.2457

Collins, F. S. 2015. Exceptional Opportunities in Medical Science: A View from the National Institutes of Health. *JAMA,* 313(2): 131–132.
https://doi.org/10.1001/jama.2014.16736

Das, R. 2017. Top 5 Reasons Why Every Healthcare Company Should Invest in Blockchain. *Forbes,* August 8, 2017. Accessed October 1, 2017:
https://www.forbes.com/sites/reenitadas/2017/08/08/top-5-reasons-why-every-healthcare-company-should-invest-in-blockchain/

de Lusignan, S., Mold, F., Sheikh, A., Majeed, A., Wyatt, J. C., Quinn, T., Cavill, M., Gronlund, T. A., Franco, C., Chauhan, U., Blakey, H., Kataria, N., Barker, F., Ellis, B., Koczan, P., Arvanitis, T. N., McCarthy, M., Jones, S., & Rafi, I. 2014. Patients' Online Access to Their Electronic Health Records and Linked Online Services: A Systematic Interpretative Review. *BMJ Open,* 4(9): e006021–e006021.
http://dx.doi.org/10.1136/bmjopen-2014-006021

Dwan, K., Gamble, C., Williamson, P. R., & Kirkham, J. J. 2013. Systematic Review of the Empirical Evidence of Study Publication Bias and Outcome Reporting Bias – An Updated Review. *PLoS ONE,* 8(7): e66844.
https://doi.org/10.1371/journal.pone.0066844

Hankewitz, S. 2016. Estonia to Protect Patient Records with Blockchain Technology. *Estonian World,* March 4, 2016. Accessed October 1, 2017.
http://estonianworld.com/technology/estonia-to-protect-patient-records-with-guardtime-blockchain-technology/

Hashed Health. 2017. *Illinois Opens Healthcare Blockchain Development Partnership with Hashed Health.* Hashed Health, Press Release, August 8, 2017. Accessed October 1, 2017:
https://hashedhealth.com/illinois-opens-healthcare-blockchain-development-partnership-with-hashed-health/

ISO. 2016. *ISO/TC 307: Blockchain and Electronic Distributed Ledger Technologies.* Geneva: International Organization for Standardization (ISO).
https://www.iso.org/committee/6266604.html

An Introduction to Blockchain Technology in the Healthcare Sector

Mark A. Engelhardt

Spink, J., Moyer, D. C., & Rip, M. R. 2016. Addressing the Risk of Product Fraud: A Case Study of the Nigerian Combating Counterfeiting and Sub-Standard Medicines Initiatives. *Journal of Forensic Science & Criminology,* 4(2): 1–13. https://doi.org/10.15744/2348-9804.4.201

Jagadeesh, K. A., Wu, D. J., Birgmeier, J. A., Boneh, D., & Bejerano, G. 2017. Deriving Genomic Diagnoses without Revealing Patient Genomes. *Science,* 357(6352): 692–695. http://dx.doi.org/10.1126/science.aam9710

Kelsey, T., & Cavendish, W. 2014. *Personalised Health and Care 2020: Using Data and Technology to Transform Outcomes for Patients and Citizens: A Framework for Action.* London: National Information Board, Department of Health, HM Government. https://www.gov.uk/government/publications/personalised-health-and-care-2020

Khan, A. N., & Khar, R. K. 2015. Current Scenario of Spurious and Substandard Medicines in India: A Systematic Review. *Indian Journal of Pharmaceutical Sciences,* 77(1): 2–7.

Kitson, A., Marshall, A., Bassett, K., & Zeitz, K. 2013. What Are the Core Elements of Patient-Centred Care? A Narrative Review and Synthesis of the Literature from Health Policy, Medicine and Nursing. *Journal of Advanced Nursing,* 69: 4–15. http://doi.org/10.1111/j.1365-2648.2012.06064.x

Kobie, N. 2016. Quantum Computing and Its Threat on Encryption and Our Data. *Wired UK,* October 4, 2016. October 1, 2017: http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption

Lippert, C., Sabatini, R., Maher, M. C., Kang, E. Y., Lee, S., Arikan, O., Harley, A., Bernal, A., Garst, B., Lavrenko, V., Yocum, K., Wong, T., Zhu, M., Yan., W.-Y., Chang, C., Lu, T., Lee, C. W. H., Hicks, B., Ramakrishnan, S., Tang, H., Xie, C., Piper, J., Brewerton, S., Turpaz, Y., Telenti, A., Roby, R. K., Och, F. J., & Venter, J. C. 2017. Identification of Individuals by Trait Prediction Using Whole-Genome Sequencing Data. *Proceedings of the National Academy of Sciences,* 114(38): 10166–10171. http://doi.org/10.1073/pnas.1711125114

Lo, M.-T., Hinds, D. A., Tung, J. Y., Franz, C., Fan, C.-C., Wang, Y., Smeland, O. B., Schork, A., Holland, D., Kauppi, K., Sanyal, N., Escott-Price, V., Smith, D. J., O'Donovan, M., Stefansson, H., Bjornsdottir, G., Thorgeirsson, T. E., Stefansson, K., McEvoy, L. K., Dale, A. M., Andreassen, O. E., & Chen, C.-H. 2016. Genome-Wide Analyses for Personality Traits Identify Six Genomic Loci and Show Correlations with Psychiatric Disorders. *Nature Genetics,* 49(1): 152–156. https://dx.doi.org/10.1038%2Fng.3736

Lynch, S. V, & Pedersen, O. 2016. The Human Intestinal Microbiome in Health and Disease. *New England Journal of Medicine,* 375(24): 2369–2379. http://doi.org/10.1056/NEJMra1600266

Mattei, T. A. 2017. Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World Neurosurgery,* 104: 972–974. https://doi.org/10.1016/j.wneu.2017.06.104

McDonald, D. C., & Carlson, K. E. 2013. Estimating the Prevalence of Opioid Diversion by “Doctor Shoppers” in the United States. *PLOS ONE,* 8(7): e69241. https://doi.org/10.1371/journal.pone.0069241

McKinsey & Company. 2011. *Big Data: The Next Frontier for Innovation, Competition, and Productivity.* New York: McKinsey Global Institute. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation

McLaughlin, E. K. 2012. Counterfeit Medicine from Asia Threatens Lives in Africa. *The Guardian,* December 23, 2012. Accessed October 1, 2017: https://www.theguardian.com/world/2012/dec/23/africa-counterfeit-medicines-trade

Mold, F., De Lusignan, S., Sheikh, A., Majeed, A., Wyatt, J. C., Quinn, T., Cavill M., Franco, C., Chauhan, U., Blakey, H., Kataria, H., Arvanitis, T. N., & Ellis, B. 2015. Patients' Online Access to their Electronic Health Records and Linked Online Services: A Systematic Review in Primary Care. *British Journal of General Practice,* 65(632): e141-e151. https://doi.org/10.3399/bjgp15X683941

Mold, F., Ellis, B., De Lusignan, S., Sheikh, A., Wyatt, J. C., Cavill, M., Michalakidis, G., Barker, F., Majeed, A., Quinn, T., Koczan, P., Avanitis, T., Gronlund, T. A., Franco, C., McCarthy, M., Renton, Z., Chauhan, U., Blakey, H., Kataria, N., Jones, S., & Rafi, I. 2012. The Provision and Impact of Online Patient Access to their Electronic Health Records (EHR) and Transactional Services on the Quality and Safety of Health Care: Systematic Review Protocol. *Informatics in Primary Care,* 20(4): 271–82.

Molteni, M. 2017. To Protect Genetic Privacy, Encrypt Your DNA. *Wired,* August 23, 2017. Accessed October 1, 2017: https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/

National Research Council of Canada. 2017. *“Workin' on the Chain Gang”: Doing Business on the Blockchain.* Ottawa: National Research Council Canada. https://www.nrc-cnrc.gc.ca/eng/stories/2017/blockchain.html

Panetta, K. 2017. Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017. *Gartner,* August 15, 2017. Accessed October 1, 2017: http://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Patientory. 2017. Patientory to Integrate Dash Payments Using BlockCypher Web Services. *Patientory,* August 24, 2017. Accessed October 1, 2017: https://patientory.com/2017/08/24/patientory-integrate-dash-payments-using-blockcypher-web-services/

Pevnick, J. M., Fuller, G., Duncan, R., & Spiegel, B. M. R. 2016. A Large-Scale Initiative Inviting Patients to Share Personal Fitness Tracker Data with their Providers: Initial Results. *PLoS ONE,* 11(11): e0165908. http://dx.doi.org/10.1371/journal.pone.0165908

Miller, R. 2017. PokitDok Teams with Intel on Healthcare Blockchain Solution. *TechCrunch,* May 10, 2017. October, 1, 2017: https://techcrunch.com/2017/05/10/pokitdok-teams-with-intel-on-healthcare-blockchain-solution/

Sanderson, S. C., Linderman, M. D., Suckiel, S. A., Diaz, G. A., Zinberg, R. E., Ferryman, K., Wasserstein, M., Kasarskis, A., & Schadt, E. E. 2016. Motivations, Concerns and Preferences of Personal Genome Sequencing Research Participants: Baseline Findings from the HealthSeq Project. *European Journal of Human Genetics,* 24(1): 14–20. http://doi.org/10.1038/ejhg.2015.118

Schumacher, A. 2017. *Blockchain & Healthcare – 2017 Strategy Guide.* Munich: Axel Schumacher.

Stewart, M. 2001. Towards a Global Definition of Patient Centred Care: The Patient Should Be the Judge of Patient Centred Care. *BMJ,* 322(7284): 444–445. https://doi.org/10.1136/bmj.322.7284.444

Suberg, W. 2017. Alibaba Deploys Blockchain to Secure Health Data in Chinese First. *The Cointelegraph,* August 18, 2017. Accessed October 1, 2017: https://cointelegraph.com/news/alibaba-deploys-blockchain-to-secure-health-data-in-chinese-first

Tanner, A. 2013. Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study. *Forbes,* April 25, 2013. Accessed October 1, 2017: http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/

The World Bank. 2015. World Development Indicators: Health Expenditure Per Capita (Current US$). *The World Bank.* Accessed October 1, 2017: https://data.worldbank.org/indicator/SH.XPD.PCAP

Tieu, L., Schillinger, D., Sarkar, U., Hoskote, M., Hahn, K. J., Ratanawongsa, N., Ralston, J. D., & Lyles, C. R. 2016. Online Patient Websites for Electronic Health Record Access among Vulnerable Populations: Portals to Nowhere? *Journal of the American Medical Informatics Association,* 24(e1): e47–e54. https://doi.org/10.1093/jamia/ocw098

United States: Department of Health and Human Services. 2013. *HIPAA Administrative Simplification Regulation Text.* Washington, DC: U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

Wagstaff, J., & Kaye, B. 2017. Exclusive: Company Behind Bitcoin “Creator” Sold to Private Investors. *Reuters,* April 13, 2017. Accessed October 1, 2017: http://www.reuters.com/article/us-bitcoin-wright-fund-exclusive/exclusive-company-behind-bitcoin-creator-sold-to-private-investors-idUSKBN17F26V

Woodman, J., Sohal, A. H., Gilbert, R., & Feder, G. 2015. Online Access to Medical Records: Finding Ways to Minimise Harms. *British Journal of General Practice,* 65(635): 280–281. https://doi.org/10.3399/bjgp15X685129

Zhernakova, A., Kurilshikov, A., Bonder, M. J., Tigchelaar, E. F., Schirmer, M., Vatanen, T., Mujagic, Z., Vila, A. V., Falony, G., Vieira-Silva, S., Wang, J., Imhann, F., Brandsma, E., Jankipersadsing, S. A., Joossens, M., Cenit, M. C., Deelen, P., Swertz, M. A., Weersma, R. K., Feskens, E. J., Netea, M. G., Gevers, D., Jonkers, D., Franke, L., Aulchenko, Y. S., Huttenhower, C., Raes, J., Hofker, M. H., Xavier, R. J., Wijmenga, C., & Fu, J. 2016. Population-Based Metagenomics Analysis Reveals Markers for Gut Microbiome Composition and Diversity. *Science,* 352(6285): 565–569. https://doi.org/10.1126/science.aad3369

Citation: Engelhardt, M. A. 2017. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review,* 7(10): 22–34. http://doi.org/10.22215/timreview/1111

Keywords: blockchain, health, distributed ledger, patient-centred care, trust

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors

Greg Wolfond

> *"Blockchain is more than just ICT innovation, but facilitates new types of economic organization and governance."*
>
> Sinclair Davidson, Primavera De Filippi, and Jason Potts
> In "Economics of Blockchain" (2016)

Blockchain-based solutions have the potential to make government operations more efficient and improve the delivery of services in the public and private sectors. Identity verification and authentication technologies, as one of the applications of blockchain-based solutions – and the focus of our own efforts at SecureKey Technologies – have been critical components in service delivery in both sectors due to their power to increase trust between citizens and the services they access. To convert trust into solid value added, identities must be validated through highly-reliable technologies, such as blockchain, that have the capacity to reduce cost and fraud and to simplify the experience for customers while also keeping out the bad actors. With identities migrating to digital platforms, organizations and citizens need to be able to transact with reduced friction even as more counter-bound services move to online delivery. In this article, drawing on our own experiences with an ecosystem approach to digital identity, we describe the potential value of using blockchain technology to address the present and future challenges of identity verification and authentication within a Canadian context.

Introduction

Identity verification and authentication has long been a critical component in service delivery for both the private and public sectors, but changing citizen demands in the digital age have stressed the need for new approaches to verify that an individual is who they say they are – with surety. At the same time, as more of our lives migrate online, "bad actors" such as hackers and fraudsters are always finding new ways to exploit our sensitive information for their own personal gain at the expense of legitimate users and online service organizations.

Governments, banks, telecommunications companies, healthcare providers, and businesses of all sizes are vocal in their commitment to becoming more digital – and that commitment hinges on digital identity. Digital identity is a critical, but underserved, layer of the digital era for the safety of citizens as they continue to do more online both domestically and globally. Today, every service is an island unto itself. There is no open mechanism for citizens to assert their own digital identities, for ways for citizens to have trusted third parties to add fragments or attributes ("X is a doctor", "Y's reported income from last year is", or "Z's background check has been verified") to those identities or for citizens to subsequently use their identities around the world and safely interact and authenticate themselves with online services they want to access.

Current identity tools do not support this modern approach, relying instead on physical identity documents, processes, and methods that require expensive and tedious counter visits. Username and password combinations are cumbersome and easily forgotten, while patchwork solutions authenticating users with photos of driver's licenses are less secure, are often extremely difficult to validate, and are easy to spoof. The results of today's inefficient identity-verification methods are high registration costs coupled with fraud and breach risks for businesses, together with low-convenience processes for citizens.

In this article, we argue for an approach that combines the benefits of blockchain and digital ecosystems. As Gartner (2017) defines it, "A digital ecosystem is an interdependent group of enterprises, people and/or things that share standardized digital platforms for a mutually beneficial purpose (such as commercial gain, innovation or common interest). Digital ecosystems enable you to interact with customers, partners, adjacent industries – even your competition." We further argue that new digital identity standards and tools that are trusted across the economy are required to allow individuals to prove they are who they are – in a secure and privacy-enhancing way. Businesses, governments, and consumers need help to combat rising rates of cyberfraud and cybercrime, reduce the risk and friction of transacting digitally, and increase trust and safety for citizens. As a potential enabler of such help, we look to an ecosystem approach to digital identity based on blockchain.

Blockchain – The Building Block for Better Digital Identity

A number of public and private sector organizations have implemented various identity management solutions to manage authentication and authorization privileges of their users within or across system and enterprise boundaries. Many of these current solutions rely on federated authentication and identity networks services provided by a centralized broker architecture. These solutions allow end users to authenticate or provide their identity data claims using third-party digital credentials they already have and trust, such as from their banks.

Although currently deployed identity-brokerage systems provide great utility to their participants, it has been noted that the principles upon which they are designed have several security and privacy limitations. Desirable improvements, described by the United States National Institute of Standards and Technology (NIST) (Grassi et al., 2015) and Brandão and colleagues (2015), include an architecture that reduces reliance on single point of trust and failure and prevents any single party from tracking a user's transaction, while maintaining an auditable trail that cannot be altered but also prevents data mining. The identity of the participant should also be protected using state-of-the-art cryptographic technologies and protocols.

To meet these privacy and data integrity goals, what is needed is a decentralized model based on blockchain that leverages well known technology platforms and standards, and that is available to an ecosystem of participants leveraging an easy-to-license open source codebase maintainable by an established group of developers. If designed to promote easy adoption and integration, and to comply with established security, network communication, and design requirements, this system can be implemented quickly while adhering to guiding principles that are designed to improve privacy, security and ease of access to digital services for both citizens and service providers.

These guiding principles, which have been developed in collaboration with the Digital ID & Authentication Council of Canada (DIACC, 2017), are as follows:

1. *No Centralized Authority:* Both users and consortium members interact directly with the marketplace ensuring that there are no middle-man servers acting as a single point of failure or having the ability to tamper with the transactions.

2. *Secured Blinded Infrastructure:* Participants' identities should be guaranteed and protected using state-of-the-art cryptographic technologies and protocols, while all parties involved in a transaction should remain anonymous to one another. Users' data should not be accessible to the central infrastructure at rest or in motion.

3. *Decentralized, Secured, and Private Data Architecture:* Data storage, transaction endorsement, and log and configuration rules should be available only to network participants, while the network owner maintains financial auditing events in a private ledger with the related proofs of existence stored in a distributed ledger shared with all network participants. Each digital asset should be encrypted with a split key, where the data custodian holds part of the key and the user holds the other.

4. *Privacy and Controls:* Users must always be in exclusive control. Data should be encrypted and consent should be signed with keys that are in the users' control, while data at rest must not be linkable. Data in transit must be viewed by the minimum number of

systems to satisfy the transaction endorsement policy (endorsement is where an organization has verified the validity of a transaction), while user transactions (such as consent) should be linkable to a user only during an authorized investigation (but not otherwise). Transactions should be endorsed by multiple organizations to be valid (to ensure that no single organization can create unauthorized transactions).

5. *Book Keeping, Audit, and Billing:* A transaction history must be kept and cannot be altered, and auditable and decentralized architecture where billing can occur without the network being live.

The application of these principles adds value to the Internet as a new, distributed platform that will help reshape the world of business and transform the order of human affairs for the better. As an indication of the potential benefits of this approach, Tapscott and Tapscott (2017) have summarized the views of 40 policymakers, entrepreneurs, and other experts in Canada on their collaborative approach to transform the country into a world leader in digital identity. This work provides valuable insight on the called "second generation of the digital revolution" that, according to the authors, is being powered by blockchain technology.

A Collaborative Approach to Identity

No single organization or industry can solve the identity challenge alone. It takes a village to make identity. This is how the world works in-person already – new service registrations require customers to show up with trusted documents from existing third parties. What is needed to expand in-person registrations so they work online and at the call centre, too. Adding integrity to the current counter processes is also required so that source documents can be verified and matched to the applicant. Expanding the identity ecosystem in this way allows companies to leverage the best and most reliable information available to validate a customer's identity. This technical implementation of the ecosystem architecture leverages blockchain and distributed ledger technology, which provides the ecosystem foundation. Blockchain facilitates the immutable, secure, and privacy-respecting sharing and validation of digital attributes for consumers and businesses.

The strengths of each company converge to create the standards needed to support a world-leading network model enabling privacy, security, and trust in digital identity authentication, verification, and attribute sharing. Standards drive consistent experiences across industries, reinforcing user behaviours, which increases security – in fact, the user experience is the security. Hiding the security model from users simplifies the experience and minimizes the attack surface that needs to be managed.

Collaboration is necessary to keep the user in the centre of their transactions across the economy. This to enable the secure digital identities needed for citizens to access services from governments and businesses alike. Neither authentication nor identity registration are a source of competitive advantage for anyone – in fact, lack of consistency is a source of risk business and a frustration for customers. We only need look at the payment system as proof here – the card-based payment system is standardized across the world, and across the payment brands. Digital identity needs the same capabilities and scope for global reach, universal acceptance, and simplified user experience.

We believe that secure, trusted digital identities will allow citizens to carry out high-value and day-to-day transactions online, in more economically efficient ways without increased risk; will reduce identity theft and improve public safety and confidence by making it more difficult to use identities fraudulently; and will improve healthcare and healthcare outcomes.

In Canada, we believe that secure digital identities will improve access to government services, regardless of a user's location, that would normally require them to appear in person, and are critical to achieving much of the federal government's innovation and economic vision – digital identification is inextricably tied to digital economy transformative innovations.

Identity Ecosystems in Action

Banks, telecommunications companies, sharing economy companies, and many others around the world stand to benefit greatly from a digital identity ecosystem based on blockchain, but in Canada, we have identified two areas that stand to benefit the greatest: government services and healthcare.

Government services

Immediate access to services has always presented a challenge to governments, where the utmost needed for fraud prevention and thorough physical identification verification has been in place. For instance, renewing a driver's license or passport most commonly requires a visit to a physical location, identity documents in hand, and wait times that frustrate citizens in the digital age.

With mass adoption, government services stand to reduce customer service overhead costs associated with physical office space, verification, call centres, and more, resulting in hundreds of millions of tax payer dollars saved each year, better information sharing across the country, with the additional benefit improved customer service and satisfaction.

Healthcare
Many adult Canadians manage healthcare needs for a spouse, children, or aging parents. Although they may undertake many day-to-day activities online, healthcare management often relies on phone and fax for communications with healthcare providers. Phone tag is common, with voicemail effectively unused due to privacy reasons. Appointments are only made and changed on the phone, in direct conversation. Referrals between providers "vanish" from a patient perspective, and all-too-often, a receptionist selects an inconvenient appointment for the patient, starting another round of phone tag.

Access to a patient's test results is cumbersome. Private labs provide online access to some test results because privacy laws prevent sharing results across providers. Hospitals offer online access to results, for only their tests, and not to information in other provider locations. Primary care physicians, generally, do not allow access to anything. In this digital age, fax machines continue as the gold standard for secure messaging between providers in the healthcare system – paper messaging.

With an inclusive, comprehensive, and secure method of identification Canadian healthcare could be transformed – significantly streamlining patient administration, engaging consumers in self-care and management at home, and supporting those who manage the wellness of their family. Patients and providers could securely identify during appointment bookings, access records and authorize a "circle of care" to share their patient history across multiple providers and family members.

Implicit or explicit consent by consumers to authorize access to their personal information is supported by this secure method of identification, including delegation from aging parents to a "child" who is acting as their healthcare manager, or rules delegating access to their children's records. Secure identification is critical for home-based monitoring devices such as glucometers, intelligent weigh scales, or exercise trackers as data streaming from these devices is consumed by medical record and "smart" monitoring systems. Secure digital identification also enables protection of health information for children under the care of social service agencies, or for a spouse under court order.

Although time savings for health providers and convenience for patients are significant, the transformative value to the health system is reducing the demand side of healthcare via patient engagement.

Digital Identity on Blockchain Will Benefit to the Bottom Line

Cost savings regarding password management alone range in the millions. In 2016, the average administrative cost at call centres to manage and administer a lost, forgotten, or stolen password was estimated to be $31 per incident (Martin, 2016). Assuming one incident per year per working Canadian, across 18.454 million working Canadians, $572 million are lost annually to just call centre password management services and lost productive hours (StatsCan, 2017).

But, improved password management is one of many benefits of a standardized ecosystem. With adequate funding to convene participants, the economic impact on Canada is nearly incalculable. Banks, telecommunications companies, and governments stand to save hundreds of millions per year through increased efficiencies. With application to healthcare and patient consent to view and share their records, billions can be saved annually.

There are multiple other examples of the benefits of blockchain. For instance, Tapscott and Tapscott (2016) highlight that blockchain could transform remittances – the largest flow of funds – into the developing world, and it could provide immutable land title registration for the estimated 5 billion people in the world who have only a tenuous right to their land.

Conclusion and Next Steps for Canada

Private and public sector organizations have many challenges to overcome in synchronizing and aligning their digital transformation efforts to enable the network effects to take hold. Canada's policymakers, civil society leaders, senior business leaders, and entrepreneurs, among other actors, are building strong clusters to help the country be the leader of the next era of the Internet as a platform that helps transform human affairs for the benefit of the citizens.

Executives can contribute to the digital ecosystem by creating open and collaborative cultures where knowledge and innovation are shared with the industry for the benefit of the masses and, more so, to establish quality and communication standards. They also can contribute by staying open to change, embracing digital adoption and transformation within their management models and infrastructure.

It is time for institutions to rethink their processes and governance structures to become more agile and innovative players. The success of an harmonious digital identity ecosystem relies on staying ahead of the organization's digital curve.

As a first step to provide better quality in the provision of public services, SecureKey Technologies' blockchain-based ecosystem (securekey.com) allows multiple partners to strengthen authentication and provide identity attribute validation, as a fabric of trust and as a solid foundation to embrace a new digital era.

SecureKey Technologies‘ vision for the future of digital identities redefines the ways both consumers and businesses approach identity verification and the sharing of key personal information. The ecosystem members' commitment to consumer rights and the secure evolution of digital identities has engaged more like-minded organizations to participate and create a standard of privacy and consumer empowerment across organizations and industries. This process continues to involve exceptional collaboration between SecureKey Technologies, the DIACC, Canada's leading financial institutions, government agencies, telecommunications providers and many, many more. It takes a village to make identity work.

Acknowledgements

This article is based on documents produced in collaboration with the Digital ID & Authentication Council of Canada (DIACC; diacc.ca). The DIACC is a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation the global digital economy. DIACC members include representatives from both the federal and provincial levels of government as well as private sector leaders and organizations, including SecureKey Technologies.

About the Author

Greg Wolfond is the Founder of SecureKey Technologies and brings more than 30 years of experience in fintech, security, and mobile solutions to his role as Chief Executive Officer. Greg is a serial entrepreneur whose earlier ventures include Footprint Software Inc., a financial software company he sold to IBM, and 724 Solutions Inc., a wireless infrastructure software provider he took public. He sits on several boards and has been recognized as one of Canada's Top 40 Under 40, Entrepreneur of the Year, and one of the 100 Top Leaders in Identity. Greg holds a Bachelor of Arts in Computer Science from the University of Western Ontario, Canada, and a Bachelor of Science in Biochemistry and Life Sciences from the University of Toronto, Canada.

References

Brandão, L. T. A. N., Christin, N., & Danezis, G. 2015. Toward Mending Two Nation-Scale Brokered Identification Systems. *Proceedings on Privacy Enhancing Technologies,* 2015(2): 135–155. https://doi.org/10.1515/popets-2015-0022

Davidson, S., De Filippi, P., & Potts, J. 2016. Economics of Blockchain. *SSRN,* March 8, 2016. Accessed October 1, 2017: http://dx.doi.org/10.2139/ssrn.2744751

DIACC. 2017. Digital ID & Authentication Council of Canada (DIACC): Digital Identity Ecosystem Principles. *DIACC.ca.* Accessed October 26, 2017: https://diacc.ca/principles/

Gartner. 2017. Digital Ecosystems. *Gartner.com.* Accessed June 6, 2017: https://www.gartner.com/technology/topics/business-ecosystems.jsp

Grassi, P., Lefkovitz, N., & Mangold, K. 2015. *Privacy-Enhanced Identity Brokers.* Gaithersburg, MD: National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

Martin, Z. 2016. Passwords the Bane of Enterprise Security. *SecureIDNews.com,* January 20, 2017. Accessed October 26, 2017: https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/

StatsCan. 2017. Employment By Age, Sex, Type of Work, Class of Worker and Province (Monthly) (Canada). *Statistics Canada.* Accessed October 26, 2017: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr66a-eng.htm

Tapscott, D. & Tapscott, A. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* Toronto: Penguin Canada.

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Greg Wolfond*

Tapscott, D., & Tapscott, A. 2017. *The Blockchain Corridor: Building an Innovation Economy in the 2nd Era of the Internet.* Toronto: The Tapscott Group. http://dontapscott.com/BlockchainCorridorReport.pdf

Citation: Wolfond, G. 2017. A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review*, 7(10): 35–40. http://doi.org/10.22215/timreview/1112

Keywords: digital identity, online security, digital assets, identity verification, identity fraud, digital attributes, online privacy, consumer privacy, blockchain, cybersecurity

Q&A

Hugh Rooney, Brian Aiken, and Megan Rooney

Q. Is Internal Audit Ready for Blockchain?

A. Blockchain technology offers the promise of "a safe, transparent, rapid and affordable digital solution to many government challenges" (Policy Horizons, 2016). However, this same technology also poses challenges and opportunities to internal auditors wishing to provide maximum value to their organizations, whether governmental or otherwise. In order to rise to the challenges and capitalize on the opportunities, internal audit departments must be able to place auditors – well trained on both blockchain technology and on all blockchain projects right from their inception.

To assess its readiness for blockchain, first consider the function of internal auditing. Internal auditing "is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations" (IIA, 2017). Internal auditors accomplish this activity through the use of a systematic, disciplined approach to evaluate and improve effectiveness and efficiency. To deliver this value to organizations, there are three major areas of focus for internal auditors:

1. *Governance* is "the combination of processes and structures implemented ... to inform, direct, manage, and monitor the activities of the organization toward the achievement of objectives" (IIA, 2017). The governance framework includes ethics and values, organizational performance, and accountability – as well as the communication of risk and control activities within the organization and information technology strategy.

2. *Risk management* refers to the assessment of risks that directly relate to, and impact the achievement of, an organization's mission and objectives. This process includes understanding an organization's appetite for risk, the analysis of fraud risks, and a focus on technology risks as they apply to the achievement of an organization's mission and objectives. Risk management also involves an assessment of the processes involved in the assessment and communications of risk.

3. *Controls* are implemented to help mitigate risk and are the processes for assuring achievement of an organization's objectives in operational effectiveness and efficiency; reliable financial reporting; and compliance with laws and regulations.

In order to provide this independent, objective assurance, internal auditors assess the adequacy and effectiveness of the management control framework that has been established by management. This is done to provide boards, audit committees, and senior management with an objective appraisal and assessment of the adequacy and effectiveness of governance, risk management, and control activities.

Furthermore, the methodologies and tools for providing this assurance have been developed and form the professional standards by which internal auditors perform their work. Although blockchain technology is new, this is not the first time a new technology has been developed. Thus, it will require internal auditors to employ new approaches to assessing this new technology using well established professional standards to ensure adequate assurances can continue to be made.

Blockchain technology is coming rapidly and, at least in Canada, many levels of government are already on board. As an example, the Toronto-based Blockchain Research Institute (blockchainresearchinstitute.org) has recently been granted "support from the federal government, the Ontario provincial government, and the City of Toronto, in addition to the University Health Network in Toronto, the Bank of Canada, and the Federal Institute on Governance" (Kovacs, 2017). Indeed, Policy Horizons Canada (2016), in a brief on blockchain technology, stated that it "could facilitate payments, benefits distribution, identification, record keeping and certification to name a few."

Although blockchain is the technology that allowed the creation of cryptocurrencies (such as Bitcoin or Ether), it is not itself a cryptocurrency. Rather, blockchain technology is used to enable the existence of these cryptocurrencies in the same way that TCP/IP (transmission control protocol/internet protocol) is used to enable the existence of online shopping sites such as Amazon (Iansiti & Lakhani, 2017). In the case of both technologies, the full range of possible applications is exceptionally diverse. In simpler terms: blockchain technology enabled the creation of cryptocurrencies in the same way that steel girders enabled the creation of skyscrapers. Skyscrapers could not exist without steel girders but these same girders can be used to build longer bridges and other structures previously not possible.

So, what is revolutionary about blockchain-based applications (blockchains) from the internal audit point of view? They quite simply require a change in the way organizations and individuals think about where we find the "truth" about transactions and information. Up until the advent of blockchains, the only way to establish one version of the truth was to designate a system of record for specific ledgers. A system of record was thought of as "the place where there is a definitive value for some unit of data" (Inmon, 2003). Just as someone with one watch always knows what time it is and someone with two watches is never quite sure, a system or record ensures you always have one truth. Systems of record live on one system, within a specific organizational structure, and are subject to one governance and control structure.

Iansiti and Lakhani (2017) explain how blockchain is different as follows:

> *"In a blockchain system, the ledger is replicated in a large number of identical databases, each hosted and maintained by an interested party. When changes are entered in one copy, all the other copies are simultaneously updated. So as transactions occur, records of the value and assets exchanged are permanently entered in all ledgers."*

In a blockchain, there is no longer one specific system, within one specific organizational structure, where the "truth" resides. Instead, there is a permanent shared ledger that provides all interested parties or stakeholders with exactly the same "truth" simultaneously. Now the governance, risk management, and control mechanisms are sometimes associated with the blockchain, not with a specific system or organization. Think of it this way: in your private home, you get to set the rules for building and using a pool but when you move to a condominium, the condominium association holds that power.

The full impact of this change – from all applications having a system of record to some applications using blockchains – are still being discovered, but one can identify several obvious implications for internal audit. First of all, internal auditors will need to access information in new formats. Essentially, there will be a new technical environment where critical information is created and stored and internal auditors must be able to access information contained in this environment. Internal auditors will also need to maximize the value of "real-time" information; the value of sampling will have to be re-evaluated when the use of data analytics, on continuous information, is technically feasible. Another consideration is that internal auditors will sometimes need to work collaboratively across organizations. There are public blockchains, such as Ethereum (ethereum.org), that applications may be run on and that have preexisting governance structures, but there are also private/consortium blockchains that are only open to identified stakeholders. Each of these blockchains will have their own governance structure, one that may involve a number of stakeholders across multiple organizations. Internal auditors from these multiple stakeholders will need to work together to ensure all their requirements are met. Finally, internal auditors will need to understand that some work being routinely performed today will become redundant. For example, with a shared ledger there will no longer be any requirement to reconcile differences between systems of record. Instead, there will be one version of the truth and all stakeholders will have access to it.

This background leads us to examine some of the issues regarding what internal audit departments need to consider in preparing themselves for this new technology. In order for internal auditors to provide objective assurance and insight on the adequacy and effectiveness of governance, risk management, and internal control processes in environments utilizing blockchains, the internal auditors must fully understand what they are being asked to deal with.

In support of this objective, internal auditors should consider the following:

1. Internal auditors must possess "the knowledge, skills, and other competencies" needed to perform their individual duties. (IIA, 2017) Therefore, before adopting blockchain, internal audit departments should start training some of their people on blockchain. Internal auditors today are quite familiar with systems of record and their governance, risk management,

and controls. In order to effectively deal with blockchain-based applications, they must first understand the basics of the technology and, in particular, the evolving area of governance.

2. Internal auditors must be involved at the planning stage of blockchain-based applications. All systems must have adequate governance, risk management, and controls, and it is much easier to build these in right from the start than to retrofit them after a problem has been identified.

3. Internal audit departments must include continuous auditing as part of their standard audit methodology, if they have not done so already. Blockchain-based applications provide real-time access to information; continuous auditing will allow internal auditors to use this real-time access to transactions to increase the value they bring to their organizations.

4. As a profession, internal auditors are prudent. This prudence has served the profession well and is relied upon by clients. Unfortunately, there are times when this trait can result in a slow approach in adopting new technologies. It is important that internal auditors prepare themselves such that they can meet the demands of their clients while maintaining their professional standards.

5. The relevant standards bodies will need to cooperate in determining the optimum approach to ensuring that blockchain-based applications not only deliver the business value promised but also do such in a manner consistent with prudent and effective governance. Although there is a growing consensus that blockchains can offer significant value to large organizations, due diligence must still be performed to ensure that such applications are the best choice for a specific objective.

6. One of the key strategic advantages that internal auditors have is their knowledge of the business and organization they support. This knowledge will be critical when it comes to supporting the implementation of blockchain for, without this knowledge, adequate assessment of the governance, risk, and control environment will be difficult to provide.

Blockchain certainly has the potential to enable numerous new digital solutions to many of the challenges governments and other large organizations face. We must, however, take the necessary steps today to ensure that the blockchains of tomorrow are subject to the same high standards as all other business systems and processes. Otherwise, we risk that potential being unrealized.

About the Authors

Hugh Rooney is a member of the Tendermint/COSMOS team who are building blockchain infrastructure that will provide unparalleled scalability, security, and interoperability to the next generation of blockchain-based applications. Hugh holds an MBA from the Richard Ivey School of Business in London, Canada, and has extensive experience in the application of leading-edge technologies to a wide range of business problems in both the public and private sectors.

Brian Aiken is an External Board Member of the Audit Committee to the Auditor General of Canada. He has held a variety of management positions at the Bank of Canada, including oversight for financial systems, strategic planning, corporate security, and internal audit. He later joined the Royal Canadian Mounted Police as a Chief Audit Executive, with responsibility for internal audit, program evaluation, and quality assurance and management review. He completed his career as the Assistant Comptroller General, Internal Audit, at the Treasury Board Secretariat of Canada. He holds a Bachelor's degree in business administration from the University of Ottawa and is a Certified Internal Auditor and Certified Fraud Examiner.

Megan Rooney is a law student at Osgoode Hall Law School in Toronto, Canada, with an interest in the practical implications of technology on governance. A graduate of the Theatre Production and Management program at York Universities Fine Arts Department (Cum Laude and Dean's List). Megan was a Senior Editor at the *Osgoode Hall Law Journal* and has worked as a research assistant to several professors as well as the International Institute of Business Analysis (IIBA).

Q&A. Is Internal Audit Ready for Blockchain?

Hugh Rooney, Brian Aiken, and Megan Rooney

References

Iansiti, M., & Lakhani, K. R. 2017. The Truth About Blockchain. *Harvard Business Review,* 95(1): 118–127.
https://hbr.org/2017/01/the-truth-about-blockchain

IIA. 2017. *International Standards for the Professional Practice of Internal Auditing.* Lake Mary, FL: The Institute of Internal Auditors (IIA).
https://na.theiia.org/standards-guidance/

Inmon, B. 2003. The System of Record in the Global Data Warehouse. *Information Management,* May 1, 2003. Accessed August 23, 2017:
https://www.information-management.com/news/the-system-of-record-in-the-global-data-warehouse

Kovacs, M. 2017. Blockchain Research Institute Gains Support from Three Levels of Government and Private Sector. *IT World Canada,* June 12, 2017. Accessed August 23, 2017:
http://www.itworldcanada.com/article/blockchain-research-institute-gains-support-from-three-levels-of-government-and-private-sector/393907

Policy Horizons. 2016. *Blockchain Technology: Brief.* Ottawa: Policy Horizons Canada, Government of Canada.
http://publications.gc.ca/site/eng/9.828823/publication.html

Citation: Rooney, H., Aiken, B., & Rooney, M. 2017. Q&A. Is Internal Audit Ready for Blockchain? *Technology Innovation Management Review,* 7(10): 41–44.
http://doi.org/10.22215/timreview/1113

Keywords: internal audit, blockchain, governance, risk management, controls

Author Guidelines

These guidelines should assist in the process of translating your expertise into a focused article that adds to the knowledge resources available through the *Technology Innovation Management Review*. Prior to writing an article, we recommend that you contact the Editor to discuss your article topic, the author guidelines, upcoming editorial themes, and the submission process: timreview.ca/contact

Topic

Start by asking yourself:

- Does my research or experience provide any new insights or perspectives?
- Do I often find myself having to explain this topic when I meet people as they are unaware of its relevance?
- Do I believe that I could have saved myself time, money, and frustration if someone had explained to me the issues surrounding this topic?
- Am I constantly correcting misconceptions regarding this topic?
- Am I considered to be an expert in this field? For example, do I present my research or experience at conferences?

If your answer is "yes" to any of these questions, your topic is likely of interest to readers of the TIM Review.

When writing your article, keep the following points in mind:

- Emphasize the practical application of your insights or research.
- Thoroughly examine the topic; don't leave the reader wishing for more.
- Know your central theme and stick to it.
- Demonstrate your depth of understanding for the topic, and that you have considered its benefits, possible outcomes, and applicability.
- Write in a formal, analytical style. Third-person voice is recommended; first-person voice may also be acceptable depending on the perspective of your article.

Format

1. Use an article template: .doc .odt

2. Indicate if your submission has been previously published elsewhere. This is to ensure that we don’t infringe upon another publisher's copyright policy.

3. Do not send articles shorter than 2000 words or longer than 5000 words.

4. Begin with a thought-provoking quotation that matches the spirit of the article. Research the source of your quotation in order to provide proper attribution.

5. Include a 2-3 paragraph abstract that provides the key messages you will be presenting in the article.

6. Provide a 2-3 paragraph conclusion that summarizes the article's main points and leaves the reader with the most important messages.

7. Include a 75-150 word biography.

8. List the references at the end of the article.

9. If there are any texts that would be of particular interest to readers, include their full title and URL in a "Recommended Reading" section.

10. Include 5 keywords for the article's metadata to assist search engines in finding your article.

11. Include any figures at the appropriate locations in the article, but also send separate graphic files at maximum resolution available for each figure.

Issue Sponsor

Technology Innovation Management Review

timreview.ca

Academic Affiliations and Funding Acknowledgements

Technology Innovation Management (TIM; timprogram.ca) is an international master's level program at Carleton University in Ottawa, Canada. It leads to a Master of Applied Science (M.A.Sc.) degree, a Master of Engineering (M.Eng.) degree, or a Master of Entrepreneurship (M.Ent.) degree. The objective of this program is to train aspiring entrepreneurs on creating wealth at the early stages of company or opportunity lifecycles.

- *The TIM Review is published in association with and receives partial funding from the TIM program.*

The Federal Economic Development Agency for Southern Ontario (FedDev Ontario; feddevontario.gc.ca) is part of the Innovation, Science and Economic Development portfolio and one of six regional development agencies, each of which helps to address key economic challenges by providing regionally-tailored programs, services, knowledge and expertise.

- *The TIM Review receives partial funding from FedDev Ontario's Investing in Regional Diversification initiative.*