Blockchain Technology for Recordkeeping

Help or Hype?

SSHRC Knowledge Synthesis Grant Competition on "How can emerging technologies be leveraged to benefit Canadians?"

Principal Investigator: Victoria L. Lemieux

The University of British Columbia, Vancouver, BC, V6T 1Z1
E-Mail: vlemieux@mail.ubc.ca

Volume 1: Report

Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
Canada

This research was supported by the Social Sciences and Humanities Research Council of Canada

Acknowledgements

This project was supported by funding from Social Sciences and Humanities Research Council of Canada. Completion of this project would not have been possible without the contributions of the student research assistants of the University of British Columbia—I am very grateful to each and every one of them.

I would like to thank Darra Hofman, doctoral student in archival science, who conducted reviews of literature and other sources; contributed to the development of a thematic synthesis to identify the recurring themes or issues from the literature review; assisted in the drafting of this report, and travelled to Ottawa to represent our team at the meeting of the Knowledge Synthesis Grant holders.

I would also like to thank Mark Penney, graduate student in archival science; Jessica Tung and Victor Liang, graduate students in the archival science and library and information science dual programme; Steve Thompson, graduate student in library and information science, who contributed in various ways to the research and drafting of this report, as well as assisting with dissemination; and Vikas Singh, graduate student in management information systems at UBC's Sauder Business School.

Finally, I would like to acknowledge the valuable input received from Canadian and international experts during the consultation phase of this study: Kuldar Aas; Jason Baron; Nicolas Connizzo; Luciana Duranti; Barbara Endicott-Popovsky; David Fricker; Natasha Khramtsovsky; Richard Marciano; John McDonald; Chris Prom; Hrvoje Stancic; Mats Stengärd; Peter van Garderen; Ethan Wilding; Angela Walch. Their collective intelligence strengthened this report immeasurably. Any errors or omissions, of course, remain the sole responsibility of the principal investigator.

Table of Contents – Volume 1

Key Messages

1. Blockchain technology, often described as providing a distributed and continuously growing immutable ledger of transactions, is a recordkeeping technology, in the archival science sense of the term[1], as much as it is a value transfer technology.

2. Many current and proposed applications of blockchain technology aim to address recordkeeping challenges; they offer a new form of generation use, storage and/or control of records. For example, the blockchain aims to change the way that the authenticity of records is established from reliance on a trusted third party to a system-based mode of establishing authenticity.

3. Claims associated with use of blockchain technology for recordkeeping are, in a number of cases, overhyped. As an example, blockchain solutions that claim to provide "archival" solutions do not actually preserve or provide for long-term accessibility of records.

4. There appears to be little awareness in the blockchain community of archival science (the science of recordkeeping) theory, principles and practice, or of recordkeeping requirements and standards derived from them. More interaction between the archival/records management and the blockchain communities would promote greater awareness.

5. Despite the fact that blockchain technology is fundamentally a recordkeeping technology and there are many new start-ups that focus on using the technology in recordkeeping applications, there is relatively little research focused on the recordkeeping implications of this technology. Academia-industry collaborations in the application of blockchain technology for recordkeeping are mostly absent.

6. As it is a recordkeeping technology, the blockchain's future development will benefit from the theoretical and practical knowledge of archival science.

7. Blockchain technology is giving rise to new forms of records[2] that must be managed as legal evidence alongside other records in order to meet business and societal purposes. This includes determining how blockchain records will be dealt with under Canada's law of evidence as well as how best to preserve their long-term authenticity and accessibility as evidence.

8. Considerations of the impact of blockchain technology on financial stability should explore whether its widespread use for recordkeeping could be a contagion channel.

9. There is growing support for the introduction of technical standards relating to blockchain technology. Standards focused on use of the blockchain for recordkeeping may help assure that blockchain technologies embed existing recordkeeping solutions and requirements.

Therefore, this report recommends that interdisciplinary research be conducted that integrates the expertise of legal, economics, archival, diplomatic, forensic, and computer and information academic researchers with blockchain start-ups and solution providers. Specifically, such research could begin by using existing archival science theory, principles and practice to identify, and help mitigate, risks to the long-term preservation and accessibility of trusted records generated or stored using blockchain technology.

Executive Summary

Blockchain technology, often understood as a distributed ledger that maintains a continually growing list of publicly accessible records cryptographically secured from tampering and revision[3], is perhaps best known as the value transfer technology underlying cryptocurrencies such as Bitcoin and Ether. However, many new blockchain innovations seek to capitalize, not on value transfer, but on the technology's *recordkeeping* capacity; that is, they offer a new form of records storage, use, maintenance or control of records. Socially signification application areas include identity management, registration of title to property and other assets, certification of educational achievements, and protection of personal privacy. The blockchain, when ideally operating, creates a persistent, immutable, and ever-growing, public ledger that can be updated (i.e., by appending information using cryptographic digital signatures) to represent the latest state of a blockchain.[4]

Blockchain innovators, seeking to leverage the potential for increased transparency, permanence, and efficiency of blockchain records envision, and in some cases, have developed, applications for payments, clearing and settlement, securities trading, supply chain management, identity management, notarial services, Internet of Things, land transfer and registration, health recordkeeping, voting, intellectual property management and more.

At the moment, blockchain recordkeeping is highly hyped.[5] This technology does have potential, but there are still significant questions surrounding its use for recordkeeping, such as how long-term authenticity and availability of blockchain records will be assured. This is a question that archival science, as the science underpinning recordkeeping, is particularly well-placed to assist in answering. Because most of the work on, and conversation regarding, blockchain applications has been within the community of blockchain innovators and enthusiasts, much of the conversation is focused on the possibilities of blockchain, with little awareness of the risks to the long-term availability of trustworthy digital records. Furthermore, some blockchain enthusiasts oppose a focus upon the risks due to fears of stifling innovation.

For Canadians to truly benefit from blockchain recordkeeping, those risks must be understood and, to the extent possible, mitigated. Some of the most significant risks of blockchain recordkeeping include:

- Consumers of blockchain recordkeeping solutions will not be able to see through the hype and will purchase solutions that disappoint or, worse, unintentionally or maliciously lead to negative consequences such as such as loss of competitive advantage, loss of a customer base, and loss of critical information, title to assets, or claims to certain rights.
- Blockchain innovators focused on using the technology to improve recordkeeping will wastefully "reinvent the wheel" (i.e., develop solutions for establishing authenticity of records already well-developed in archival science), or produce solutions that create, rather than solve, recordkeeping problems.
- Businesses and citizens will not be able to protect their legal rights or defend against legal claims due to unreliable and inaccessible records created on overhyped blockchain solutions.[6]
- Adopters of blockchain technology may introduce unintended sources of financial contagion via the micropayments that are made to secure transactions on the blockchain.

Given both the many possibilities and the potential risks of blockchain recordkeeping, a deeper understanding is necessary.

This knowledge synthesis represents a first step towards understanding blockchain recordkeeping beyond the hype. Because of the breadth of blockchain technology's potential applications, the current state of knowledge on a number of issues was examined, including: a) the design and operation of blockchain technology; b) current developments and applications of the technology in Canada and internationally to uncover the particularities of the Canadian "technoscape"; c) insights of archival science concerning trustworthy recordkeeping relevant to blockchain technology; d) the results of leading edge research on digital records, digital recordkeeping and preservation from research projects in which the principal investigator or her collaborators are involved and the application of these results to blockchain technology; e) the current state of

the law of evidence in Canada in relation to this technology; and f) standards concerning management, security, and preservation of records relevant to the security and preservation of blockchain records.

While blockchain recordkeeping is being developed and pursued globally, our focus on Canada revealed that the underlying conditions in Canada are particularly well-suited to leading blockchain research and implementation. Our investigation further revealed that Canada has a vibrant, highly active blockchain technoscape, with a diversity of start-ups and consultancies doing innovative work. Unfortunately, however, our research also indicates that Canada is not currently capitalizing on this potential; at time of writing, little programmatic research is being done in the area of blockchain recordkeeping, and academia-industry partnerships have not been developed. The state of knowledge with regard to blockchain technology for recordkeeping is largely undeveloped, with many important gaps that must be filled if Canadians are to see the benefits of blockchain technology for recordkeeping. There also appears to be little awareness in the blockchain community of archival science theory, principles and practice, or of recordkeeping requirements and standards derived from them. Blockchain technology is giving rise to new forms of records, such as smart contracts, that must be managed as evidence alongside other traditional records in order to meet business and societal purposes. Gaps in knowledge also exist around how blockchain records should be dealt with under Canada's law of evidence as well as how best to preserve their long-term authenticity and accessibility as evidence. Moreover, the implications for financial stability of 'financializing' (i.e., requiring tiny micro-payments for) our recordkeeping transactions have yet to be investigated.

There is growing support for the introduction of technical standards relating to blockchain technology as a spur to innovation. Standards focused on use of the blockchain for recordkeeping may help assure that blockchain technologies embed existing recordkeeping solutions and requirements in much the same way that earlier standards outlining functional requirements for electronic records management systems (ERMS) ensured that these systems supported effective recordkeeping. Yet, before effective standards can be developed in the area of blockchain recordkeeping, work must be done to close the knowledge gaps relating to, in particular, long-term authenticity and accessibility of blockchain records and recordkeeping systems.

The potential of blockchain technology is great. The blockchain community is developing seemingly endless creative business applications supported by recordkeeping functionality. As ideally imagined, blockchain recordkeeping could increase transparency, protect privacy, improve efficiency, and even help guard against obsolescence. However, there remains much to be learned and understood before such an ideal can be reached. Recordkeeping risks must be investigated and mitigated. The wisdom and knowledge of other disciplines, including archival science, should be brought to bear in the development of blockchain solutions reliant upon and/or supporting recordkeeping. And records professionals must work with the blockchain community to be prepared to adequately care for the new types of records that blockchain technology will bring within their purview and connect legacy systems to blockchain recordkeeping solutions. This report reveals that Canada is uniquely situated to benefit from and capitalize upon blockchain technology for recordkeeping, but only if we look beyond the hype, seize the opportunity and fill the knowledge gaps.

Context

The digital age has seen enormous change in how we create, communicate and keep recorded information. In the past twenty years, new information and communications technologies (ICTs), such as the Internet, have given us email, web content, social media, and the Cloud. The impact of these technologies, both positive and negative, has been far reaching, not least in how we understand what records are, and manage and preserve them in their new forms.[7]

Recently, another ICT innovation - blockchain technology – has dominated discussion of technological innovation. There is as yet no universally agreed definition of blockchain technology, but it is often described as a distributed ledger that maintains a continually growing list of publicly accessible records cryptographical secured from tampering and revision.[8] The blockchain's key technical features include:

- Tracking of transition from one state to another, e.g., the ownership status of digital currency.[9]

- A distributed operating model, comprised of computers, called "nodes", in the network that arrive at an agreement about the validity of transactions (i.e., a distributed "consensus mechanism").[10]
- Use of cryptographic hashes in the processing of transactions, which enables transparency without exposing content.
- Packaging of transactions into blocks (from which comes the name "blockchain") chained in chronological order and distributed across every full node.[11]
- More controversially, a cryptographic token like Bitcoin or Ether that represents actual value and is integral to incentivizing miners to participate in validating transactions and/or that is used to represent an asset.[12]

The blockchain is believed to create a persistent, immutable, and ever-growing, public ledger that can be updated (i.e., by appending information using cryptographic digital signatures) to represent the latest state of a blockchain.[13] Those who are new to the concept of the blockchain will find more information about how the blockchain operates in the "Additional Resources" section of this report.[1]

Although the above bullets comprise the key features of blockchain technology, there are non-trivial variations among blockchain platforms (e.g., Bitcoin, Ethereum, Ripple, Litecoin, Hyperledger and others). These include underlying code, use of tokens, consensus mechanisms, whether permissionless or permissioned[14], whether public or private, and application layers. This makes any generalizations about the technology a challenging proposition. This variety is to be expected of a technology that is still so new, however.

Since the launch of Bitcoin in 2009, which introduced the archetypal blockchain, innovation and investment in this technology has moved at a rapid pace.[15] According to the Tapscotts, "*In 2014 and 2015 alone, more than $1 billion of venture capital flooded into the emerging blockchain ecosystem, and the rate of investment is almost doubling annually*."[16]

Actual and proposed applications for blockchain technology are wide ranging, encompassing cryptocurrency, payment systems, clearing and settlement, securities trading, supply chain management, identity management, notarial services, the Internet of Things, land transfer and registration, health recordkeeping, voting, intellectual property management, and beyond. To illustrate, Volume 2, Appendix C provides examples of the wide range of companies working on or offering blockchain-based technologies and services. Some sources see no limit to the uses to which blockchain technology can be put to help solve societal and business problems. There are even predictions that the impact of this technology will be as far reaching as the Internet.[17]

While blockchain technology does seem poised to be transformative in many respects, much of the discussion about its application encountered at the start of this study (May 2016) was quite uncritical.[18] The relative absence of critical reflection, especially in regard to establishing long-term authenticity of digital records as evidence of transactions, may have been due to a focus on innovation, and a desire to avoid stifling a fledgling technology with enormous potential. Over the course of the study, however, more critical reflection on the potential of the blockchain has emerged. Some observers have asked what problem the blockchain will solve, and whether it is a solution in search of a problem.[19] Others have raised questions about governance of the blockchain, challenging the notion that it is truly decentralized and calling for recognition of blockchain developers/miners as fiduciaries.[20] And, following the DAO exploit on the Ethereum blockchain in June of 2016[21] and the Hong-Kong Bitfinex Bitcoin exchange security breach in August of 2016,[22] there has been greater critical reflection on blockchain security, information assurance, and risk management.[23] For example, the Ethereum hard fork has raised questions about whether blockchains are truly immutable and free from external interference, while the amalgamation of mining power in the Bitcoin network raises concerns about the potential for attacks and manipulation of the historical blockchain record. These critical reflections provide evidence of a maturing of the technology and its developers, as blockchain is put to the test. Nevertheless, critical commentators online have received strong negative feedback from a blockchain technology "fan base".[24]

With some uses of blockchain technology reaching higher levels of maturity and implementation, now is

[1] Volume 2, Appendix H.

the time for a thorough examination of the implications of this technology. Any new technology has the potential to be useful. Developing a critical understanding of the nature of its utility is key to successfully leveraging technological innovations like the blockchain for the benefit of all Canadians.

The goal of this study, therefore, was to survey existing knowledge about blockchain technology from as wide a range of sources as possible to ascertain the degree to which the technology can be helpful versus unhelpful; that is, evidence that proposed uses for blockchain are merely hype or can actually deliver on their stated functionality. In undertaking this study, we have examined our sources through the lens of our area of expertise, archival science, the science of recordkeeping. Other aspects of the technology and its application, such as its use as a basis for various cryptocurrencies, are outside the scope of this report. In spite of this limitation, because blockchain technology is a recordkeeping technology, as we argue in the following section, the scope of this report remains quite broad and has far-reaching implications.

Implications

Ensuring trustworthiness and long-term availability of records is a necessary requirement in a range of different contexts where systems of record provide critical underlying infrastructure. This is not only a problem for traditional archives, but also for many organizations that may never have thought of themselves as performing an archival function. This includes organizations responsible for civil registries of births, deaths and marriages, land registries, and repositories of financial transactions, to offer but a few examples. In each of these cases, if digital records are insecure or lack integrity, development or organizational objectives may be thwarted. For example, untrustworthy civil registration entries may mean that citizens are unable to prove their identities as a necessary precondition of accessing social protection benefits, or that opportunities for identity fraud emerge that undermine a country's immigration policies and national security. Insecure land registries may create opportunities for bad actors to acquire properties that they are not entitled to by fraudulently entering title transfers. Additionally, such records are often required for long periods of time that may extend well beyond the life span of a single database system or server. Loss or irretrievability of the records may prevent citizens from successfully making future claims to citizenship, land, social protection or other entitlements. In such cases, the inability to secure long-term trust in records can lead to a more generalized breakdown in trust in government, the financial sector and throughout society.

Blockchain technology is meant to prevent such bad outcomes. Characterized as an immutable distributed public ledger, blockchain is said to provide permanent, transparent and accurate records. However, at present, a number of blockchain innovators' claims relating to providing long-term availability of authentic records appear to be overhyped. For example, several companies claim that their solutions store records on the blockchain when, in reality, they only store the records' hash values.[25] Further, most innovators are unaware of existing theories, principles, practices and standards for recordkeeping that could inform development of new blockchain applications. Archival theories around long-term preservation of authentic digital records, such as those developed by the InterPARES over 30 years of research could assist blockchain solution developers in building robust blockchain recordkeeping solutions. Recordkeepers also lack understanding about new forms of blockchain records and the operation of blockchain-based recordkeeping systems, which prevents them from assisting blockchain innovators in designing good systems and from adapting this technology to solve their recordkeeping challenges. Unless steps are taken to close the knowledge gaps, there is a risk that:

- Consumers of blockchain recordkeeping solutions will not be able to see through the hype and will inadvertently purchase solutions that disappoint or, worse, unintentionally or maliciously create negative consequences such as loss of competitive advantage, loss of a customer base, and loss of critical information, title to assets, or claims to certain rights.
- Blockchain innovators focused on using the technology to improve recordkeeping will wastefully "reinvent the wheel" in a search for solutions to long-term authenticity of and access to records, and produce solutions that create, rather than solve, recordkeeping problems, such as how to generate

and preserve authentic records over the long-term, for which archival science solutions already exist. In addition, innovators usually focus on immediate business needs, whereas legal professionals, records managers and archivists tend to be more focused on longer-term consequences, legal requirements, preservation (including long-term) of authentic and usable evidence and information, and use of records in legal disputes, etc.

- Businesses and citizens will not be able to protect their legal rights or defend against legal claims due to unreliable and inaccessible blockchain records.
- Adopters of blockchain technology may introduce unintended sources of global financial contagion via the micropayments needed to complete transactions on many types of blockchains.

Approach

Preparation of this knowledge synthesis included looking into a) the design and operation of blockchain technology, b) current developments and applications of the technology in Canada and internationally to uncover the particularities of the Canadian "technoscape"; c) insights of archival science concerning trustworthy recordkeeping relevant to blockchain technology; d) the results of leading edge research on digital records, digital recordkeeping and preservation from research projects in which the principal investigator or her collaborators are involved and the application of these results to blockchain technology; e) the current state of the law of evidence in relation to this technology; f) and relevant standards concerning management, security and preservation of records that bear upon the security and preservation of blockchain records. The aim was to provide a general overview of blockchain technology and its current forms, a synthesis of the current state of knowledge, and a discussion of the economic, social, environmental, philosophical and legal implications of its development, adoption and use through an archival science lens. Here, it is important to underscore that archival science does not just concern preservation of historical documents, but is the science of the creation and preservation of records as trustworthy evidence. The study proceeded in three phases: Phase 1, a literature search and review; Phase 2, a thematic synthesis and Phase 3, final write-up and dissemination, which is ongoing as of October 2016.

During Phase1, the student members of the research team, according to their expertise and interests, conducted reviews of academic and other literature as well as other relevant sources, such as blogs and social media (e.g., Twitter, Reddit, Slack, etc). Their background research papers are provided for information as Volume 2, Appendix A of this report. In addition to gathering information from the sources used for the preparation of the background papers, during Phase 1, the principal investigator attended a W3C/Massachusetts Institute of Technology (MIT) Media Lab hosted workshop on blockchain technology and the Web.[26] Much useful information was gathered from reading the participants' papers and interacting with those in attendance. Following the literature search and review, the students then prepared a collective bibliography and background papers (see Volume 2, Appendix A) at the end of the first ten weeks of the project.

Phase 2 included conducting a thematic synthesis to identify the recurring themes or issues from the literature review, which generated an analytical understanding that extended beyond the conclusions of individual researchers or sources. The principal investigator and a doctoral student under her supervision performed the thematic synthesis using *NVIVO* qualitative data analysis software. The results of their individual coding were discussed and compared, and a final list of thematic codes was derived to guide drafting of the report. In addition to the thematic synthesis using *NVIVO*, Phase 2 also employed data science techniques, in particular, visual analytics, to explore samples of Twitter data. This technique was used due to the large scale of Twitter data to be analyzed, making use of big data analytical techniques much more effective for analysis of this source than analysis using *NVIVO*. Following analysis and synthesis of sources, the principal investigator, with the aid of a doctoral student and several Masters students, prepared the draft report, summarizing the findings. The draft report, together with the student papers, which had been prepared during Phase 1, was then circulated to collaborators for review and comment. A list of the collaborators consulted is included at Volume 2, Appendix E.

The final phase involved revising the study report according to the comments received from the collaborators, and disseminating the findings according to the Knowledge Mobilization plan, including at the SSHRC "Imagining Canada's Future" Fall Forum in Ottawa.

Results

Blockchain technology as a recordkeeping technology

Blockchain, which is actually an element in the bundle of technologies used in many so-called blockchain solutions, is often described as a value transfer technology, e.g., a technology used to transfer digital money from one person to another.[27] With its origins in cryptocurrency – i.e., a form of digital money – it may not be obvious that blockchain technology is fundamentally about recordkeeping as well. However, our synthesis of the literature confirmed our original supposition that it is, indeed a recordkeeping technology by nature.

What do we mean by recordkeeping technology? A *recordkeeping system* is "*a set of rules governing the storage, use, maintenance and disposition of records and/or information about records, and the tools and mechanisms used to implement these rules.*"[28] Records, as defined in the International Records Management Standard (ISO 15489-1:2016) are "*information created, received and maintained as evidence and as an asset by an organization or person, in pursuance of legal obligations or in the transaction of business*"[29] and as defined by InterPARES Trust, an international SSHRC-funded research consortium focused on the long-term preservation of authentic electronic records are, "*document[s] made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference*."[30] As the field of recordkeeping may be new to many readers of this report, a primer on recordkeeping terminology and concepts is included as Volume 2, Appendix G.

Ledger entries, which record financial transactions, are well-recognized types of accounting records; thus by extension, distributed ledgers, are a new form of ledger, and the transactions recorded on them qualify as new types of record.[31] Indeed, according to the Tapscotts, "This new digital ledger of economic transactions can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims . . . that can be expressed in code."[32] Indeed, many blockchain solution providers, organizations and governments have begun to or are planning to do just that.[33] It is notable that this list is comprised of different types of economically and socially significant records.

Though the claim in this report is that blockchain technology is a recordkeeping technology, in the sense of existing as, generating and, to some extent, storing new forms of records, the extent to which this new technology is capable of responding to recordkeeping requirements is open to question. As our investigations reveal, proponents of blockchain solutions make strong claims about the trustworthiness of information recorded in blockchains. However, from an archival science point of view, a *trusted recordkeeping system* comprises "*the whole of the rules that control the creation, maintenance use and disposition of the records of the creator and provide a circumstantial probability of the authenticity of the records, and the tools and mechanisms used to implement those rules.*"[34] As we discuss in the section on "Blockchain technology for recordkeeping: Help or Hype?", detailed examination reveals gaps between archival science and legal requirements needed to establish records as trustworthy, on the one hand, and how some blockchain solutions operate, on the other hand.

The Blockchain "technoscape"[35]

Blockchain-based applications have grown immensely since Bitcoin's arrival, and the "technoscape" is constantly expanding. In Volume 2, Appendix C, we provide a list of companies that we came across over the course of our research and the areas of development on which they are concentrating.

In terms of geographic spread, we observed that almost half of the work on development of blockchain-based technologies is being done in North America, with the rest spread out over Europe, Australia and other countries.

In Canada, the blockchain technoscape is vibrant and diverse. There are, for example, several blockchain initiatives and start-ups:

- Royal Bank of Canada, TD Bank, BMO Financial Group, and Scotiabank are part of a consortium of banks in a in collaboration with R3 to develop distributed ledger technologies for global financial markets.[36]
- Bluezelle, which is creating blockchain financial products centered on the foreign exchange market.[37]
- Rubix by Deloitte, which is producing blockchain enterprise solutions. Examples of what they are working on include: decentralized capital markets systems; peer-to-peer payments; and health data management. This team is also building an alternative asset management blockchain solution in collaboration with New York communications firm Estey-Hoover.[38]
- Blockstream, which creates sidechains that connect to other asset types and interoperates with bitcoin.[39]
- Cryptiv, which is pursuing blockchain for enterprise digital assets. [40]

Some Canadian organizations offer blockchain consultancy services. These include:

- decentral, that offers a wide variety of potential consulting services related to blockchain. Notably, its consultants include Anthony Di Iorio, a well known player in the Canadian blockchain scene and a one-time head of the Bitcoin Alliance of Canada.[41]
- Quadriga Fintech Solutions is opening the "Blockchain Innovation Lab" in Vancouver.[42] This is a partnership with Christine Duhaime, a Canadian lawyer and founder of the Digital Finance Institute, which aims to "address issues in respect of the nexus between financial innovation, digital finance policy and regulation, financial inclusion and women in financial technology."[43] Duhaime's firm, Duhaime Law, also offers information and presumably services related to the blockchain.[44]
- Ledger Labs is a Toronto-based blockchain consultancy that offers strategy, development, security, and training services.[45] Of note is Vitalik Buterin, the developer of the Ethereum blockchain, is a co-founder of this company.
- Velocity is a project that creates a distributed autonomous derivatives market place with Ethereum.[46]
- BitAccess has been commercializing blockchain technologies since 2013 by enabling Canadians to buy Bitcoins at 6,000 locations across Canada and developing next generation smart-contracts.[47]
- Privacy Shell, advised by Ethan Wilding, co-founder of Ledger Labs, focuses on building blockchain solutions for privacy, security and quality of data.[48]

Bitcoin, the original blockchain, and Ethereum are the preferred platforms for the development of blockchain applications, but a number of companies are also developing their own versions of the blockchain, including permissioned/private platforms (e.g., Ripple) for specific purposes, especially within the financial services industry. Over the course of this study, we observed a shift in focus from the notion of having one "canonical" blockchain to the idea of having many "fit for purpose" blockchains.

A key take away from our survey of blockchain innovation is that currently, in Canada and elsewhere, the focus of development is on business applications of the blockchain that rely upon some form of recordkeeping, rather than on its use in digital currencies. However, it is difficult to separate the two functions since recordkeeping on the blockchain often relies on using an underlying digital currency for purposes of validating transactions.[49]

Indeed, use of blockchain technology for the creation of trustworthy and transparent records is identified as a unique feature and selling point in many current and proposed applications of blockchain technology. The discussion below *uncritically* explores the possibilities to provide readers with an overview of some of the potential application areas. In addition, the list of start-ups and use cases discussed is not exhaustive and specific companies/organizations are mentioned only for illustrative purposes, not as representations of "best in class" nor endorsements of their solution(s).

Identity management

Identity records, like birth certificates, passports, drivers' licenses and marriage certificates, are among the most relied upon records the average Canadian will use throughout his or her lifetime. A number of blockchain start-ups have proposed solutions to put these records on the blockchain to ensure their integrity. With ShoCard, for example, a user's identity is encrypted, hashed and then the hash is written to the blockchain, where it can be called up when needed. Users can give banks or other organizations temporary access to the private side of this blockchain record in order to verify identity.[50] As another example, Bitnation is a governance 2.0 platform powered by blockchain technology which aims to foster a peer-to-peer voluntary governance system unconstrained by geo-politics. Bitnation has worked out an identification solution that includes a blockchain passport and a marriage certificate.[51]

Registration of title to assets

Registration of title to assets, particularly of land and intellectual property, has emerged as a major focal point for blockchain technology innovation. Bitcoin mining company BitFury is working with the Georgian government's National Agency of Public Registry (NAPR), an office of the Georgian Ministry of Justice, to develop a system for registering land titles using the blockchain.[52] Swedish blockchain company ChromaWay, consulting firm Kairos Future, and telecommunications service provider Telia have been exploring the use of blockchain technology for land registration in Sweden.[53] A new pilot project in West Africa, called Bitland is also using blockchain technology as a decentralized land registry.[54] And, Ubitquity, a US-based blockchain real estate market solution provider, recently recorded its first property ownership transfer on the Bitcoin blockchain.[55] A demonstration of how land registration using the blockchain might work is available at this link.

Individuals and organizations adopting the blockchain also hope to offer trustworthy registration and verification services for intellectual property. With registration of intellectual property on the blockchain, the technology is used in a manner that is analogous to copyright registration to provide documentary proof of creator and date of creation. Blockchain companies providing this service essentially offer users a certificate that acts as proof that the hash of their digital asset is embedded onto the blockchain. Companies *Proof of Existence* and *Blocksign* are only two examples among many that utilize this functionality of registration on the blockchain.[56] One of the most noteworthy examples of this use case is that of the British singer/songwriter Imogen Heap, who recently released a song from her new album via the blockchain, combining both registration and licencing fees payments processing.[57]

Notarization

The blockchain is also being used as a substitute for notarization services to verify the authenticity of documents. One such e-notary service that uses the blockchain is aptly-named *Virtual Notary* (VN). Offering services to "certify any factoid," VN checks the hash of your asset, creates a record of it which can be referred to later, and issues a cryptographically-signed certificate that attests to the factoid. You then have the option to record the certificate itself on the Bitcoin blockchain. In November, Bitcoin Magazine covered the plans of the Estonian government to partner with blockchain-based Governance 2.0 initiative Bitnation to offer a public notary and identity service to Estonian e-residents based on blockchain technology.[58]

Digital signature

Digital signatures facilitate the signing of documents, such as contracts, online. A digital signature is a mathematical calculation that validates and authenticates that a certain entity or person has "signed" the exact bitstream of a document; the data cannot be changed and still keep the validity of the added signature. It is designed to guard against the tampering and forging of an identity in digital communications.[59] It uses on asymmetric cryptography (key pairs) and, in most cases, relies on public-key infrastructure (PKI), which uses one private key and one public key in the key pair for binding the identity of persons with public keys. Digital signatures that use PKI also rely upon Certificate Authorities, as a "trusted third party" that vouchsafes the public key used in digital signatures.[60] Certificate Authorities can be compromised, however, and the certificates issued by them can expire, later raising questions about the authenticity of the signatures and the records to which they have been affixed. Using blockchain, it is possible to avoid these problems. Blockchain technology does not rely upon Certificate Authorities, instead using a decentralized consensus mechanism, such as the "proof of work" (PoW) method,[61] to validate a record. Expiring certificates are also not an issue, since blockchain technology operates to produce a time-ordered, validated distributed ledger that is said to provide ongoing proof of the authenticity of a record by virtue of its immutable placement in a validated chain of blocks. One major difference between the operation of PoW in the blockchain and traditional digital signatures (e.g., using PKI and CAs) is that blockchains operate pseudonymously, whereas digital signatures link the identity of a person or entity to the digital signature. Linking the identity to the signed record or, in the case of the blockchain, a hash of a record on chain is, in fact, of critical importance to ascertaining authenticity and one reason why blockchain-based approaches to authenticity could face legal challenges.

As an example of how the blockchain has been used as a form of digital signature, Bitcourt has worked with CESYT, an Argentinian college, to record proof of all their official career diplomas on Bitcoin's blockchain.[62] The University of Nicosia has also used blockchain technology to issue certificates to students completing its course on digital currency.[63] Blockchain-based careers platform APPII, which is undergirded by the Ethereum platform, has worked with the Open University in the UK to build out a platform that can register and verify student academic records.[64] Finally, MIT's Media Lab has also produced a prototype blockchain solution for certification of student records.[65] Some archival science researchers also see potential to use the blockchain to overcome the problem of obsolescent digital signatures in digital preservation.[66]

Privacy Protection

The era of big data has brought with it a growing public concern about user privacy. Organizations– both public and private-- now amass large quantities of sensitive personal information. Individuals have little or no control over the data that is stored about them and how it is used. In recent years, public media has repeatedly covered controversial incidents related to invasion of privacy and data breaches.[67] A number of start-ups propose to use blockchain technology to solve the privacy problem, particularly in the medical sector. Graham Rhodes, the developer of MedVault, has described his blockchain application as a means of " . . . *giving the patients control over their own medical records and the decision to make certain aspects public or private, while still being stored in a distributed global manner.*"[68]

Privacy-preserving blockchain solutions can work in different ways, but for the most part they take advantage of the fact that documents that are hashed and anchored on the blockchain are encrypted. If a user wants to grant someone else the right to view some specific records in decrypted form, but not all of them, she can create a different key for each document. Another approach is to use "secret sharing" (described in more detail here), which allows a user to encrypt a piece of data in such a way that a quorum of pre-designated users can cooperate to decrypt the data (e.g., 5 of 9 medical professionals in a hospital must decrypt a document).[69]

Provenance tracking

The tracing of provenance-- the origins of an asset-- is another interesting recordkeeping area where blockchain technology may be very helpful. Founder and CEO of Coin Sciences, Gideon Greenspan, argues that Provenance may be one of the most feasible promises of blockchain technology: "*Much has been said about the blockchain as an ownership layer. But what exactly does that mean? It means that blockchains represent ownership of an asset in terms of control over the data relating to that asset. In other words, only the current owner can authenticate a transaction that would cause that asset to be transferred to another owner. This is provenance expressed in protocol form.*"[70] Greenspan goes on to say that "*Provenance is one of the backbones of economies, whether it relates to artifacts or real estate. There has always been a need to authenticate that a party actually owns an asset prior to any business dealing involving that asset, to ensure that the asset is 'true' rather than stolen or faked.*"[71]

One UK company that has been in the news in this regard is Everledger, which is using blockchain technology to help the insurance industry solve diamond theft and fraud. Everledger uses Bitcoin blockchain as a platform for creating a permanent ledger for diamond certification and related transaction history, which helps insurance companies, law enforcement and other interested parties to verify ownership. A multi-layered digital fingerprint is created and imprinted on a given diamond and also recorded on the blockchain: *"[b]y using the immutable public blockchain for holding such data Everledger aims to provide transparency around all diamonds, [and] reveal their origin, trail of ownership, the processes they might have undergone."*[72] According to some, Everledger and similar provenance use cases offer a more robust and accessible solution than traditional paper certificates and receipts, which are more readily compromised.

The blockchain can also be used to "combine supply chain management with the Internet of Things to tag any asset, from food to a new piece of equipment, with a smart chip that communicates its provenance, ownership, warranties, or special information."[73] *Provenance.org* is a noteworthy platform using the blockchain to offer such services. By tracing the origins of products and providing reliable customer information for their manufacture, *Provenance* hopes to resolve product traceability issues by using distributed ledger technology to provide information that is traceable and verifiable. The company builds accountability for businesses, non-profits, and communities through the digitization of certifications and recording the verified information from awarding bodies on the blockchain.[74] "Increased information about the product's provenance" means that even tuna can be placed on the blockchain and its chain of custody traced from fisherman through the supply chain and on to the consumer.[75]

Smart contracts

Smart contracts are computer algorithms that embed the terms and conditions of a contract as source code that is compiled into bytecode and injected into a blockchain. Many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing or both, in theory making contractual processes more efficient, faster and less ambiguous. In the context of blockchain technology, smart contracts have become very popular because the code that makes up the smart contract can be entered as part of an entry to a blockchain ledger, meaning third parties unknown to each other can now enter into contractual relationships at a low cost due to the trust that is built into the blockchain as an authenticated data structure (a special type of database) that cannot be forged or tampered with.[76] Ethereum was the first blockchain platform to implement smart contracts, with Counterparty and Rootstock now also developing smart contracts for the Bitcoin ecosystem. Smart contracts are a core capability that is being used by a number of blockchain-based application developers as an underpinning of their solutions in use cases involving payments processing, clearing and settlements, digital signatures, privacy protection, and tracing provenance.

The above has been an uncritical survey of some of the business uses of blockchain reliant upon recordkeeping functionality. In the following section, we take a more critical look at some of the claims relating to blockchain recordkeeping.

Blockchain technology for recordkeeping: Help or Hype?

The blockchain is a powerful technology with the potential to help make improvements in many areas. Yet, there is also a good amount of hype in what blockchain solution developers claim about their applications. Below we discuss several areas that we believe bear further investigation.

Brian Deery, Chief Scientist at Factom has claimed that "*Blockchains are archival record keepers. Permanent and transparent, they are the perfect solution for an industry-wide problem of transmitting and archiving critical accurate records.*"[77] Looking closely at a number of blockchain solutions, including Factom's own solution, we see that they do not preserve, or archive, the records of the transactions at all. For example, Factom only anchors hashes of transactions on the blockchain.[78] Similarly, BlockTech has claimed that their blockchain-based distributed application, *Alexandria,*" *. . . preserves the integrity of the historical record. It taps into collective, on-the-ground reporting by scraping Twitter as events unfold and prevents after the fact censorship by archiving the information on a blockchain.*"[79] In spite of this claim, however, BlockTech's *Alexandria* application uses blockchain technology only to store and distribute magnet links; that is, links to content on the popular peer-to-peer file-sharing protocol BitTorrent, rather than storing any actual content.[80] This is not to suggest that records cannot be stored on the blockchain. From the outset of the Bitcoin blockchain, it has always been possible to store tiny bits of content in the space afforded for notes about a transaction, similar to the space provided for a brief message in a wire transfer.[81] And, with the advent of smart contracts we now see natively created blockchain records, which only exist on chain.

In the case of BlockTech and others who anchor only hashes on the blockchain, however, the purpose of what is actually stored on chain i.e., the hash, is not archiving but rather to establish that the original transaction record is authentic. In order to establish authenticity, however, the originally hashed records must be archived separately in a form that is unchanged and inviolate. This enables their rehashing for later comparison with the hash stored on the blockchain for purposes of confirming authenticity. If the original records are not preserved exactly as they were created, and hashed in exactly the same way, there is a risk that the hashes may not match and the authenticity mechanism may fail. Note that comparison of the hash of the original transaction records with the hash anchored on the blockchain is only the minimum requirement for establishing authenticity of the records; it would, in addition, be necessary to link the identity of the creator of the original record and the identity of the hash on the blockchain back to the same person or entity, and to trace the provenance of both the original record and the hash over time. Hashed content also cannot be reconstituted from its hash to enable it to serve as an archive. Hashing is a one-way function that cannot be reverse engineered.[82] Thus, claims that certain applications serve as permanent archives, as opposed to simply storing hashes of content, can be confusing to end users, who may think that they are purchasing an archiving solution rather than a solution to establish records' authenticity.[83]

As to claims about permanence, these are also open to question and unproven. Since the 18th century, permanent preservation of records has been the purview of centralized institutions, known as archives, which operate trusted repositories for preservation of material of long-term value, currently following such international standards as ISO 14721 - *Space Data and Information Transfer Systems—Open Archival Information System (OAIS) —Reference Model*.[84] Many of these archives are government archives, established by statute, "with reasonable expectations of continuing to be supported by the Parliament and citizenry to keep records and make them available as a feature of a democratic society."[85] In contrast, blockchain technology offers a new distributed model for preservation, premised on redundancy through decentralization of archival nodes. As one proponent argues, "*The 28gb list of current [Bitcoin] blocks is stored in enough places to be around forever. What is stored in the blockchain is stored amongst thousands of machines (and their backups) and won't disappear just because a different technology became more popular.*"[86] David S. Rosenthal, engineer and developer of the LOCKSS project (LOCKSS stands for "Lots of Copies Keeps Stuff Safe"), which is, itself, a peer-to-peer network that aims to preserve records through redundant storage, is skeptical about the potential for blockchain permanence. He has said, "*Clearly, a technology with this much volatility is a wonderful basis for gambling – shorting Bitcoin would have been a terrific investment over the past year had it been possible. But why would anyone think that it would make a suitable basis for any important social function, such as elections, or long-term information storage?*"[87] Skeptics, like Rosenthal, argue that if a blockchain community were to shut down, or if everyone moved on to a new fork or system, the specific records preserved on the obsolete fork or system would no longer be preserved and, moreover, there may be no backup archive proving the existence (or execution) of these records.[88] However, in the case of the DAO exploit the fork contains exact records of previous transactions. The difference in the DAO is that the attacker contract balance was moved; all other records remained the same.[89] The larger questions may be: which version is considered legitimate and authoritative and are there risks associated with shifting preservation from centralized institutional archives established by law to a market-driven, decentralized digital preservation model as introduced by the blockchain?[90]

One of the key features of blockchain technology that makes it so attractive is that, as Buterin observes, blockchain "*greatly increases reliability . . . and reduces the need for trust.*"[91] These claims also bear further scrutiny in our view. In archival science theory, trustworthiness encapsulates the concepts of accuracy, reliability and authenticity of a record. Based on what is known about these characteristics, an inference is made about how much to trust the record in question. From this standpoint, determining trust is a matter of making a reasoned risk assessment: if the risks to accuracy, reliability and authenticity are low enough, it is possible to trust the object or artifact concerned.[92] In other words, establishing trustworthiness goes beyond reliance upon a single technical system or cryptographic mechanism of asserting authenticity.

Accuracy points to the degree of precision and exactness of data in a record. With records stored off chain, even if hashed on chain, there can be no automatic guarantee of accuracy arising from anchoring such records on the blockchain, as this feature would be determined by factors outside of the blockchain platform. For on chain records, including, for example, smart contracts, accuracy would depend upon the operation of the software code; for example, whether the code accurately calculated payments, etc. This may very well depend upon the quality of the code, and whether it has been subject to effective quality controls. With the recent DAO exploit[93], there has been much discussion on this point.[94]

Authenticity refers to the quality of a record that it is what it purports to be in all respects (i.e., it is a transaction initiated with the will and authority of a particular person or agent for the purposes intended by that person or agent) and that it is free from tampering or corruption. Here again, the recent DAO exploit and Bitfinex hack raise questions because the will of the originators of the smart contracts and legitimate Bitfinex accounts was clearly thwarted.[95] Indeed, there are still a wide variety of security and operational risks associated with this technology.[96]

Reliability is the trustworthiness of a record as a statement of fact and exists when a record can stand for the fact that it is about, based on the competence of its author, the record's completeness, and the controls exercised on the process of its creation.[97] Here again, there can be no automatic guarantee of reliability for records created off chain, but hashed on chain, as factors affecting their reliability will be outside the purview of the blockchain system. For records created on chain, reliability will depend on controls over the process of creation -- including the quality of software code -- which to the best of our knowledge have yet to be instituted, codified or standardized in such a new technology. That generating or anchoring a record in the blockchain is insufficient to establish its reliability is recognized in the new Vermont blockchain legislation, which states that "a presumption of [the authenticity of a blockchain record] does not extend to the truthfulness, validity, or legal status of the contents of the fact or record."[98]

In addition to being trustworthy, records must also be available for the periods of time that their creators and society may need to refer to them. In the case of some records, such as identity documents or land titles, this can be a very long time. Open questions remain about how to ensure persistent availability over time of blockchain-based records.

In spite of a number of overhyped claims, we believe that blockchain technology can have a net positive effect if all claims are properly investigated, and any shortcomings and risks are acknowledged and mitigated.

Blockchain innovators' awareness of archival science

In spite of the potential utility of archival science theories, principles and practice, and various international standards related to trusted recordkeeping, to blockchain innovators, over the course of this study, we found very little evidence of awareness about these in the blockchain community. Indeed, we only found one recordkeeping blockchain solution developer, Enigio Time – a Swedish company – whose literature referenced archival standards.[99]

Nevertheless, there is anecdotal evidence – based on informal conversations over the course of this study--that developers whose solutions focus on recordkeeping see value in drawing upon archival theory, principles, practices and standards to solve open challenges. For example, at a W3C/MIT hosted workshop on "Blockchain and the Web," a presentation on archival theories, principles, and standards drew attention (see Volume 2, Appendix F, Figure 1). In particular, the concept of "archival bond" as a feature of provenance – relating to establishing linkages among records – was new to participants and seen as potentially useful in the linked open data/semantic web environment. Given the level of interest at the W3C/MIT workshop, we believe that more interaction between the archival and blockchain communities would be beneficial as a means of making blockchain developers aware of existing recordkeeping requirements and of helping archival scholars and practitioners better understand the capabilities of the technology for recordkeeping.

The Blockchain research landscape[100]

Blockchain technology is beginning to be recognized as a major research area worldwide, although Canada lags in dedicated programmatic blockchain research. Recognized technology hubs like the University of

Waterloo and the University of Toronto do not offer any clear information on programmatic blockchain research and do not appear to support any long term or organized research initiatives. Government agencies, however, are conducting research on blockchain technology in Canada. Notably the Bank of Canada is studying digital currencies and the implications these currencies could have for monetary policy and financial stability as well as the conceptual merits of issuing electronic money.[101] Carolyn Wilkins, Deputy Governor of the Bank of Canada, has reported that the Bank of Canada is partnering with Payments Canada, Canadian banks and R3—which leads a consortium of financial institutions developing a private blockchain ecosystem —to test drive distributed ledger with the aim of understanding "*the mechanics, limits and possibilities of this technology*."[102] The private sector fares better, and Canada is home to a small number of blockchain initiatives, start-ups, and consultancies, as previously mentioned, conducting their own research and development, though given that this research is privately-funded it is more difficult to determine its status.

A handful of individuals also are currently carrying on blockchain or Bitcoin related research in Canada outside of the umbrella of a wider project. Elizabeth Stobert, a former PhD student at Carleton University produced one paper on Bitcoin key management[103] before moving to ETH Zurich, which has a dedicated project on Security and Privacy of Bitcoin.[104] At the University of Toronto iSchool, PhD student Quinn DuPont is currently pursuing research on blockchains and distributed ledgers. This includes papers examining the relationship of blockchain and the law[105], and a paper examining bitcoin and cryptography.[106] Also at the University of Toronto, father and son team Donald and Alex Tapscott have produced one of the first widely distributed trade books on the subject entitled *Blockchain Revolution*. It does not appear that they undertake academic research on the blockchain within the university yet, however. At Concordia University, Jeremy Clark researches Bitcoin and the blockchain within the Institute for Information Systems Engineering. He spoke as an expert before the Canadian Senate committee that investigated digital currencies.[107] He has an extensive list of publications that are focused on security and cryptography, and has collaborated with many of the other researchers and institutions described in this paper. And, at École de technologie Supérieure, Françios Coallier has looked at blockchain standardization from a system engineering perspective.[108]

Our investigations did not uncover information about Industry-academia partnerships in Canada, aside from some sourcing of talent from the University of Waterloo, and the Bank of Canada research. Yet, there appears to be plenty of potential for such partnerships, whether they are via Canadian blockchain organizations, such as Blockchain Canada, the Toronto-based Blockchain Eduction Network[109] or with start-ups and individual blockchain innovators. We are in agreement with Carolyn Wilkins, Deputy Governor of the Bank of Canada, that blockchain research benefits from collaboration with FinTech entrepreneurs.[110]

Turning to look at other countries,[111] we found that the US currently possesses the largest and most detailed academic research projects regarding the blockchain. MIT, Cornell, Harvard, Princeton, Stanford, the University of Maryland, and the University of California (Irvine) all had ongoing programs of research or research projects, and there are many other individual researchers looking at specific aspects of the blockchain from their disciplinary perspective.

With respect to research on the use of blockchain technology for recordkeeping, aside from Quinn DuPont's research at the University of Toronto and research led by Hrvoje Stancic[112] at the University of Zagreb, this survey reveals a general absence of such research. Given what archival science has to offer to the development of blockchain technology, it is essential to fill this gap.

Archival science perspective needed

As blockchain technology is, at its core, a recordkeeping technology, albeit in a new decentralized form, it stands to reason that future development and implementation of this technology would benefit from the science underpinning recordkeeping, archival science. Archival science is a pure and applied discipline that involves the "scientific study of process-bound information, both as product and as agent of human thoughts, emotions, and activities, in its various *contexts*.[113] Among the aims of archival science are: capturing and fixing records at a point in time, giving them an identifier so that they can be retrieved in future, and preserving them in such a way that they remain inviolate over time. This is done to ensure that the records continue to provide trustworthy evidence of the facts recorded in them, whether that evidence is needed for legal reasons, historical research or some other purpose.

The International Research in Permanent Authentic Records in Electronic Systems (InterPARES) Projects are major international research initiatives that have investigated the necessary and sufficient components of a complete, reliable and authentic electronic record— essential for the maintenance and preservation of records— for the past twenty years. The InterPARES 2 Project (IP2) in particular looked at criteria for evaluating advanced technologies that were appropriate for the monitoring, maintenance and preservation of authentic records created in electronic environments. The projects investigated trusted record-making and record-keeping systems, maintaining that these encompass the whole of the rules that control the creation, maintenance and use of records, ultimately providing circumstantial probability of the accuracy, reliability, and authenticity of records within a system.[114] The analogous language and terminology employed by blockchain adopters to characterize the system as trustworthy and immutable warrants a consideration of the findings of IP2 as applied to blockchain technology as a recordkeeping system. As the findings of the InterPARES projects constitute general principles, being based on archival science theory, they are technology neutral.

In the digital environment, there are eight fundamental components of an electronic record: *medium*, the physical carrier of the content of the message; *physical form,* the formal attributes of the electronic record (such as script, language and special signs) without which the record is unintelligible to the user; *intellectual form*, the formal attributes that represent and communicate the action in which the record is involved and involves information configuration, content articulation, and annotations; *content*, the message itself the record is intended to convey; *action*, the act and intent that gives rise to the record; *persons*, the agents that participate in the creation of the record including the author, addressee, writer, creator, and originator (identities that are not always self-evident in electronic records); the *archival bond*, the complex of relationships between records relating to the same action which is expressed through physical location, classification codes, or registry numbers; and *context,* the framework of action in which the record participates (Duranti, 2002). It is important to note that with electronic records, the content, form and medium can exist separately.

Ensuring the ability to ascertain, check, and audit trustworthy records is essential in evaluating blockchain technology, especially since its potential is perceived as disrupting a range of industries including data and identity management, healthcare, insurance, and peer-to-peer economies. As already discussed, trustworthiness in archival theory encompasses the concepts of accuracy, reliability and authenticity of a record and is intertwined with the concept of provenance. Provenance in archival science has evolved from primarily being used in the context of arrangement of archival records to being one of the most important concepts in archival science. It still refers to the context of a record and is defined as the relationships between records and the organizations or individuals that created, accumulated and/or maintained and used them in the conduct of activity. The significance of provenance stems from its use an indicator of their trustworthiness of records.[115]

With the rise of blockchain technology for recordkeeping, there is a need to develop the criteria against which the trustworthiness of the blockchain can be evaluated as a technology for archival preservation. This is an opportunity, as many cultural heritage institutions, like Library and Archives Canada, are struggling to preserve and provide access to records in their care over periods of not just decades but hundreds or thousands of years. Blockchain technology could provide a basis for archiving of government records[116], but it seems unlikely that it will be successful in doing so without reference to archival science.

Blockchain records as legal evidence

Law exists largely to administer and mediate rights, providing citizens a trusted framework for asserting their rights vis à vis one another and resolving disputes when those rights come into conflict. The existence of a legal framework also serves to encourage trust between citizens. "By giving legal assurances of remedies for breaches of trust, the law makes parties more likely to be both trusting (thanks to the hedging effect of the legal remedy) and trustworthy (to avoid sanctions). The broad category of institutional-based trust "is dependent on legal or other actions to enforce trusting behaviour."[117]

With blockchain technology, some argue that we have moved beyond the need for legal assurances and remedies to an era of "trustless" contractual arrangements.[118] Blockchain, operating as a "trustless" system, brings records – including legal records – into a new paradigm, whereby rights are administered and mediated, not by a trusted institution or third party, but by the software code of the technology.[119] However, as the DAO exploit illustrates, software code is not infallible, and when operational errors occur, remedies must be sought in trusted third parties. In the case of the DAO exploit, those third parties were the seven developers responsible for the DAO and Ethereum code, and the remedy they eventually settled on was a hard fork[120] in the Ethereum blockchain,.[121] Their decision, ultimately sanctioned by a majority of the Ethereum community,[122] has raised questions about the immutability of blockchain technology, one of its chief attractions, and has been challenged by a group of hard fork dissenters who have continued to operate using "Ethereum classic."[123] It has also raised questions about the legal status of smart contracts, and legal liability for losses arising from the hard fork decision.[124] The DAO exploit points to the fact that at least some governance arrangements for blockchains likely will need to remain rooted in the traditions, institutions and rule of law, since there will inevitably be disputes that cannot be resolved by the usual blockchain consensus mechanisms, even if the majority of the time blockchains can run as ideally intended in a decentralized fashion and free of human intervention. As Quinn Dupont observes, contracts "*like promises . . . are made to be broken. That is to say, contracts only really get interesting in their initial formation and in their potential for breach.*"[125]

There is a need to understand how best to assess the trustworthiness of blockchain-based records and determine their status in relation to Canada's law of evidence; common law on the admissibility of evidence in criminal and civil courts; standards for electronic records as documentary evidence[126]; contract law; financial regulations, and other relevant sector-specific laws bearing upon recordkeeping.[127] In addition, when litigation is expected, it is necessary to conduct a search (called legal discovery) and implement legal holds in order to preserve any relevant evidence. Questions arise about how such holds can be implemented in a blockchain recordkeeping environment. Another question concerns how organizations, which typically dispose of records after a time to reduce the costs associated with storing records they no longer need, as well as to reduce their exposure to legal discovery and hold costs, will be able to implement records destruction on immutable blockchain infrastructure and, indeed, whether records destruction can take place at all without a major disruption to the immutability of a blockchain platform.[128] In some cases (e.g., criminal cases), evidence may be needed for a very long time.[129] The challenge has yet to be addressed of how to ensure that records are preserved in an authentic form to remain accessible over very long time frames.[130] Do such records always have to reside in the blockchain or should they be moved from the blockchain environment to a separate environment/repository? If they remain on the blockchain, will long-term preservation needs be affected by a limited supply of tokens?[131] These represent just a few of the issues requiring further investigation in relation to blockchain records as legal evidence. Without greater certainty about these issues, organizations may judge blockchain technology to be unhelpful or too risky, slowing its adoption.

Blockchain recordkeeping and financial stability

During this study, we examined literature from central banking authorities, macro-prudential supervisors and financial services self-regulating industry bodies that included discussion of the possible effects of blockchain technology on financial stability.

On the positive side, blockchain technology has the potential to reduce risk in the financial system in a number of ways. The technology could increase market transparency, an absence of which contributed to the 2007-2008 global financial crisis.[132] It could increase price-level predictability due to the deterministic rate at which new Bitcoins are created. [133] By eliminating the need for some transactions to flow through trusted third parties, blockchains could reduce concentrated risk exposures to those firms and payment infrastructures. In addition, by improving the speed and accuracy of settlement of trading, blockchain technology, combined with use of smart contracts, could reduce the counterparty and operational risks that arise when financial assets are exchanged, such as in the payment of bonds and insurance coupons, and free up collateral currently used for hedging to be used in more productive ways.[134]

Concerns about the possible effects of blockchain technology on financial stability included operational risks—such as, trade confirmation delay[135], collusion[136], cybersecurity breaches, poor code quality, and governance [137]—as well as currency competition, maturity transformation using a foreign currency, exchange rate fluctuation, upward pressure on interest rates,[138] and bank runs.[139] An aspect of blockchain technology that we did not see discussed was its use in recordkeeping.

There may appear to be no direct connection between the use of blockchain for recordkeeping and financial instability, aside from those issues already considered in the literature; however, use of the blockchain for recordkeeping bears consideration as a potential source of risk. In many current blockchain configurations, validation of transactions using blockchain technology relies upon payment of small amounts of digital currency to miners for each successfully validated transaction. Without such micro-payments, miners are not incentivized to work on the validation of transactions. To be clear, other forms of recordkeeping also requirement payment (e.g., cloud storage), but If blockchain technology is used as widely for recordkeeping as its proponents propose, those who wish to record transactions, such as land transfers or transfers of funds, will be obliged to pay a fee to incentivize miners – to use Bitcoin parlance - to mine. Via this mechanism, contagion could spread in a manner similar to other channels of contagion in the event of a shock to the financial system.[140] To illustrate, it is possible that if reliance on Bitcoin or other blockchain cryptocurrency were to become widespread, an "exogenous shock" that significantly devalues this currency could cause miners to drop out of validating and recording transactions because the income earned from mining would not cover their costs. Because the exact structure of the network may not be entirely transparent to end users, they may be unaware of the extent to which their recordkeeping, and the obligations and rights embedded in these records, is at risk in the event of such a scenario. In this case, we may see threats to the long-term availability of blockchain-based records. Miners may find ways to cover their costs and keep mining by raising their fees to "rebalance" their earnings; however, this may increase the costs of anchoring transactions on the blockchain to such an extent that originators, especially those whose currencies are weak relative to Bitcoin or other cryptocurrency, may have difficulty completing the anchoring of their transactions. This could lead to wide-spread failure of recordkeeping systems, such as we saw previously with the failure of Lehman Brothers in 2008, which lead to widespread confusion and lawsuits around payment obligations. We believe that this potential blockchain-related risk scenario merits exploration.

Blockchain Standards

In April 2016, Standards Australia proposed the introduction of international blockchain standards. In May 2016, national standards bodies, including the Canadian National Standards Board, sought comment from stakeholders on the proposal to create new ISO standards on blockchains. With support from several countries, this standardization initiative will move forward with a focus on defining the standard; creating the mechanisms to be a gateway to multiple blockchains; creating the governance framework; and having interoperability and compatibility with existing financial standards.[141] The work program envisions a suite of standards covering terminology; process and methods; trust and interoperability; privacy and security; and establishing authenticity.[142]

The European branch of the International Securities Association for Institutional Trade Communication (ISITC) has proposed 10 blockchain benchmarks to standardize blockchain tools currently available on the market. In putting forward the proposal, co-chair of the ISITC Blockchain DLT Working Group, Gary Wright has said, "*We won't be able to sell anything unless people understand what we're selling and what they want to buy. It's in our interest to standardize so people will invest.*"[143] The benchmarks include areas such as resilience, scalability, latency, data structure, auditability, governance, legal jurisdiction, regulation and software version control.[144] Also in financial services, four of the world's biggest banks, UBS, Deutsche Bank, Santander and BNY Mellon, and broker ICAP have joined forces develop a standard to clear and settle financial trades over blockchain. [145] W3C, the global internet standards body, has shown similar interest in blockchain standardization. In June, it co-hosted an event to explore the issue of blockchain and the Web, including discussion of the necessity of standards.[146] Participants at the workshop agreed that several areas of the blockchain were sufficiently mature as to warrant technical specifications, including Blockchain ID Authorization; Proof and Verification; IPLD and multi-formats; and LibP2P. Various working groups have been struck to begin looking in detail at each of these areas. Finally, the Linux Foundation's Hyperledger project, which has attracted over 80 business members since it launched in 2015, is aiming to build an open source distributed ledger architecture for applications, platforms, and protocols that enhance decentralized business transactions.[147] The Object Management Group's (OMG) Financial Domain Task Force has established a Distributed Ledger Working Group which has also begun to look at developing blockchain standards. The working group held its first meeting in March 2016. In subsequent meetings, the group determined its focus would be on standards for use with "smart contracts," which would ideally leverage existing OMB standards such as the Financial Industry Business Ontology (FIBO).[148]

Reaction to the idea of blockchain standards has not been universally positive. Writing for Bitcoin magazine, Brian Cohen has argued that Bitcoin was already a standard, so ISO standards were not needed. In Cohen's view "*The proposal is just one of many blockchain land grabs by legacy actors trying to stay relevant in a world of Bitcoin governance*."[149] A blockchain developer attending a Payments Innovation Alliance meeting thought standardization would come: "*It will happen the way we see it in most protocols, where it comes later, because there's a need,*" he said. "*Trying to do it in advance before there's a single production network in the world other than bitcoin—trying to create a standard before we do anything else—is a mistake*."[150]

Standardization in the area of blockchain recordkeeping is not envisioned as being part of any of the proposed standardization initiatives, though aspects of this topic may be covered in the aforementioned initiatives. We believe, however, that a separate technical standard focused on creation and long-term preservation of authentic blockchain records, drawing upon existing ISO archival standards as well as upon any new blockchain standards, would be highly beneficial as it would create greater certainty for consumers and help mitigate some of the risks to long-term preservation and accessibility of authentic records that we have discussed in previous sections of this report. In putting forth this argument, we take instruction from the history of the introduction of electronic records management systems in the 1990s, spurred by legal challenges to the admissibility of records. The first standard for these systems, US Department of Defense (DoD) 5015,[151] helped the records management software industry develop solutions to a clear set of specifications that they knew would be acceptable to US Federal Government agencies. It has also been used in the private sector to shortlist records management software for potential purchases, and as the starting point for such benchmarks as the United Kingdom's Public Record Office (PRO) standard and the European Union's Model Requirements (MoReq).[152] We note that, in the case of electronic records management standards, concerns about stifling innovation -- similar to those now being expressed within some parts of the blockchain community -- have not borne out over the past 20 years. Moreover, many ISO standards provide high-level principles and do not prescribe implementation details. Such standards are possible and might be very helpful.

State of Knowledge

Knowledge Strengths

Our study indicates that knowledge about the potential to apply blockchain technology is particularly strong within the blockchain community. There is no shortage of creative ideas involving the use of blockchain as a distributed public ledger to record and keep track of transactions. As already discussed, we encountered many examples of proposed or actual uses in identity management; registration of title to assets; notarization; digital signatures; privacy protection; and provenance tracking.

Knowledge Gaps

On the other hand, few recordkeeping professionals know much about blockchain technology and its potential application areas and use. Work needs to be done to bring these professionals up-to-speed on a technology that has the potential to fundamentally change the type of records they manage and preserve and the systems and processes they use to support their work.

Creative and innovative as the many proposed uses of blockchain for recordkeeping are, we also found a significant gap in knowledge within the blockchain community about archival theories, principles, practices and standards relating to the creation, management and preservation of authentic records. Since blockchain-based recordkeeping generates new kinds of records, and new challenges for the management of such records throughout their life cycle, a failure to address this knowledge gap could lead, at best, to a wasteful "reinvention of the wheel" and, at worst, to unintended consequences that create new risks.

Blockchain technology could lead to many changes in recordkeeping, including "financialization" of recordkeeping, referring to the requirement to pay blockchain miners to work on validating transactions; higher levels of decentralization in record creation and keeping than ever before, i.e., records and recordkeeping are distributed across many different systems and locations; distributed consensus mode of establishing trust, which differs from the traditional approach of relying on trusted third parties; and In some contexts, separation of the digital signature from originating records (and, in some cases, recordkeeping systems) for records stored off chain. There are, no doubt, other differences, but given the present state of our knowledge, we simply have not identified these as yet.

The implications of these differences also are not well understood and raise many new questions: Does financialization of recordkeeping increase the risk of financial instability? Does the editable blockchain actually undermine its fundamental idea of the blockchain? How would long-term digital preservation of trusted records work in a decentralized recordkeeping ecosystem like the blockchain? How can the different components of blockchain records be reassembled to provide long-term access? What are the implications of relying on smart contracts as documentary evidence in legal proceedings? How can legal requirements embedded in Canadian privacy laws for deletion of personal information be implemented when the information is stored on an immutable ledger? Further research is required to seek answers to questions about the implications of using blockchain technology for recordkeeping.

Additional resources

For Blockchain innovators and decision-makers

See the primer on records and recordkeeping in Volume 2, Appendix G.

For records professionals

See the primer on blockchain technology in Volume 2, Appendix H.

Knowledge Mobilization

To date, knowledge mobilization has targeted a number of discrete and overlapping audiences. The research was presented to the School of Library, Archival and Information Studies' doctoral students on October 5, 2016. In her capacity as Program Chair of the European Association for Banking and Financial History's (EABH) Summer School for Archivists, the principal investigator organized a panel discussion on the use of blockchain technology for recordkeeping. She has also disseminated the key findings of the report to the international records management community via the records management listserv, and these key findings were covered in two records management blog posts, one in the US and another in Russia. The principal investigator presented at the W3C's workshop at MIT in June 2016 and is connecting with this community via a body working on blockchain web standards. She has also disseminated the findings to the members of the Canadian mirror committee TC 307 relating to the establishment of international blockchain standards. The principal investigator has disseminated copies of the report to key contacts within the Canadian government and international agencies such as the World Bank. The principal investigator and two graduate research assistants also gave a presentation to the Vancouver-based decentral blockchain community in October 2016.

Appendix F illustrates some of the coverage given to the findings in the report to date. In an effort to promote collaborative academia-industry research and development, the principal investigator has also founded Blockchain@UBC. Blockchain@UBC will also be used as a platform to disseminate the results of this project.

As the third, and final, phase of this project, knowledge mobilization is still ongoing. Future activities will include a presentation in November 2016 at "Imagining Canada's Future" Fall Forum in Ottawa; dissemination through the InterPARES network of researchers via a blogpost; dissemination of the key messages using various social media channels (e.g., Twitter, LinkedIn, and YouTube); preparation of papers targeting peer-reviewed journals, such as *Archivaria*, the *Canadian Journal of Law and Technology*, the *Journal of Digital Forensics, Security and Law,* and the June 2017 Association of Canadian Archivists conference on "Archives Disrupted"; preparation of policy briefs and meetings with Canadian government officials to discuss the findings of the report; and additional presentations to blockchain and general business audiences.

Conclusion

Blockchain technology, with its extensive potential applications, could dramatically alter recordkeeping. Blockchain innovators envision the blockchain being entrusted with some of our most fundamental records, such as identity records, land and other property records, and voting systems; to entrust such records to the blockchain is to entrust our rights and social fabric to the blockchain. There are real arguments, of course, for such trust. Proponents of blockchain recordkeeping point to the decentralized, allegedly immutable nature of the blockchain, as well as the potential gains in transparency and efficiency when records are authenticated, not by slow, error-prone humans, but by code. However, there exists the possibility of significant risks to long-term authenticity of trustworthy digital records. There is a real need for both research and knowledge mobilization to enhance the relationship between the blockchain community – the innovators who will create the future of blockchain recordkeeping – and the archival science community – the records experts who will have to live in the blockchain future, and who have the hard-won knowledge and practice of recordkeeping from the past and present. Specifically, archival science has developed theory and methods for the assessment of the accuracy, reliability and authenticity of records, as well as principles, standards and techniques of ensuring long-term authenticity and availability of records that could assist blockchain solution developers to build these features into their systems. Archival concepts and techniques for representing and tracing provenance and the "archival bond" between distributed components of records can also be useful when applied to blockchain recordkeeping.

Blockchain technology could change our paradigm for trusting records; instead of turning to trusted third parties, such as government registries, for evidence, we could find ourselves turning to the blockchain. But it could also fragment components needed to establish authenticity (e.g., metadata and digital signatures) from records themselves, introduce financial instability through the financialization of recordkeeping, and undermine personal privacy as much as protecting it. There exists no unbreakable 100% fail safe technology. Ways to hack into blockchains or use them to swindle are already being searched for and found. That does not make the technology inherently "bad" or useless. The biggest danger actually comes not from the vulnerabilities, but from blind trust in the blockchain from blockchain developers, lawmakers, law enforcement and the general public in this technology. Thus far, however, there does seem to be a good amount of blind trust in this technology. The potential risks of adopting blockchain technology for recordkeeping have been little discussed and little researched, in part due to the fear of stifling innovation, and in part due to the lack of input from archival science researchers and other experts. By researching the risks, as well as the benefits, of blockchain technology, it will be possible to capitalize on the benefits while mitigating risks that come with this new recordkeeping technology. To succeed, it is also likely that blockchain innovations will have to integrate into the existing, or slightly modified, financial and legal systems. Archival science could be an enabler of this integration. The alternative scenario of redesigning these systems to accommodate the blockchain seems less likely to succeed.

In addition to enriching blockchain recordkeeping with the expertise and experience of archival science experts, greater exchange between the two communities will position archivists and other records professionals to capture, manage, and preserve blockchain records. Interdisciplinary research into blockchain, bringing legal, economics, archival, diplomatic, forensic, and computer and information academic researchers together with blockchain innovators, is a critical next step in blockchain recordkeeping. Canada is uniquely positioned to lead the way. With a vibrant blockchain community and a world-leading archival science research community, Canada has the capacity to lead a research effort that will allow our institutions, businesses, and people to benefit from the potential of blockchain recordkeeping.

References and Bibliography

[1] For a detailed discussion of the archival science definition of recordkeeping, see Volume 2, Appendix G.

[2] For a definition of the term "records", see the section in this report on "Blockchain technology as a recordkeeping technology" and Volume 2, Appendix G.

[3] See, for example, "The great chain of being sure about things," *The Economist,* http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[4] Ethereum Whitepaper. (n.d.). Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper (hereinafer referred to as Ethereum Whitepaper).

[5] Jamie Redman, 2016, September 1, "We've Hit Peak Blockchain Hype, Says New Report," https://news.bitcoin.com/blockchain-hype-peak-new-report/. The hype is, in part, driven by a highly-competitive startup culture that is exaggerating functionality/capability claims to attract early-stage investors and increase potential first-to-market share for specific blockchain-related services (parallels to the early dot com boom). This is one reason why we require neutral, academic analysis of the technology that is not tied to specific business interests.

[6] Unreliability or inaccessibility may arise from such things as security breaches or possible obsolescence of blockchains, as in the case of hard forks when the previous blockchain is no longer supported. It should be noted that similar risks arise with other technical systems; however, we know more about the risks of these systems and how to mitigate them than we do in the case of blockchain technology, which is still so new.

[7] A.F. Sheppard & L.D. Duranti, (2010), "The Canadian legal framework for evidence and the Digital Economy: a disjunction?" SSHRC Knowledge Synthesis Grants on the Digital Economy final report. https://interparestrust.org/assets/public/20101201_Canadian_Legal_Framework_for_Evidence.pdf.

[8] See, for example, The Economist article. Op. Cit., fn. 3.

[9] Ethereum whitepaper.

[10] S. Nakamoto (2008, October 31), "Bitcoin: A Peer-to-peer Electronic Cash Sytem," http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf

[11] Ethereum Whitepaper.

[12] Although most blockchains use tokens intrinsically, particularly for transaction validation and increasingly to represent a physical object, new initiatives for "tokenless" blockchains are emerging. However, even these tokenless blockchains usually still use tokens to represent physical objects even if tokens are not used for transaction validation. For more about the use of tokens on blockchains, see Anthony Lewis (2015), "A gentle introduction to digital tokens," https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/.

[13] Ethereum Whitepaper.

[14] A permissionless blockchain is one that anyone can use, whereas a permissioned blockchain is one that is only open for use by those with permission to use it i.e., it is private.

[15] D. Tapscott, Don & A. Tapscott (2016), B*lockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin (hereinafter referred to as Tapscotts, 2016). See also Chris Skinner, http://thefinanser.com/2016/08/applying-blockchain-clearing-settlement.html/ on investments in clearing and settlement within the financial services industry alone.

[16] Tapscotts, 2016, p. 9.

[17] W. Mougayar (2015, December 21), "Why the Blockchain Is the New Website." *Forbes*, http://www.forbes.com/sites/valleyvoices/2015/12/21/why-the-blockchain-is-the-new-website/#260618a6ac2e

[18] See, for example, Tapscotts, 2016, which reads as a catalogue of the amazing possibilities of blockchain technology.

[19] See, for example, Mougayar. Op Cit., fn. 17.

[20] A. Walch, A (2015), "The Bitcoin Blockchain As Financial Market Infrastructure: A Consideration of Operational Risk," *N.Y.U. Journal of Legislation & Public Policy*, *18*(4), 837–893; Angela Walch's blog in the American Banker (A. Walch, (2016, August 9),"Call Blockchain Developers What They Are: Fiduciaries," *American Banker*, http://www.americanbanker.com/bankthink/call-blockchain-developers-what-they-are-fiduciaries-1090632-1.html; and I. Kaminska (2016, August 25), "DLTs and the 'can't we all just get along?' barrier." *Financial Times*.

[21] D. Seigel, (2016, June 25). "Understanding the DAO Attack," *Coindesk*, http://www.coindesk.com/understanding-dao-hack-journalists/.
[22] Higgins, S. (2016, August 3), "The Bitfinex Bitcoin Hack: What We Know (And Don't Know)," *Coindesk*, http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/.
[23] Walch, 2016 and Kaminska, 2016 Op. Cit., fn. 20.
[24] As an example, see the comment posted in response to Angela Walch's blog in the *American Banker* [A. Walch, 2016, Op. Cit., fn. 20.]
[25] That records are actually stored on the blockchain is a common misunderstanding for those just introduced to the technology. In the vast majority of cases, records are not stored on a blockchain. Rather it is the hashes of records stored elsewhere. Increasingly it is actually hashes of Merkle trees consisting of hashes of records. This technical complexity has led to emergence of third-party services (e.g. Tierion) to handle the blockchain registration and verification which means that these are could become centralized points for exploitation and negate the 'trustless' network argument [See, https://twitter.com/pjvangarderen/status/732983136594710528]. This is an area most ripe for further research and archival-science backed standards that come from a not-for-profit party that does not have commercial interests.
For a more detailed discussion on this point, see the section on "Blockchain technology for recordkeeping: Help or Hype?" in this report.
[26] W3C Blockchains and the Web Workshop, 29–30 June 2016, in Cambridge, Massachusetts. Information about this workshop is available at https://www.w3.org/2016/04/blockchain-workshop/
[27] Statements about blockchain technology as a value exchange technology are ubiquitous, but see, for example, Evry Labs (n.d.), "Blockchain: Powering the Internet of Value, https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf.
[28] InterPARES 2 (n.d.) Terminology Database, https://interparestrust.org/assets/public/20101201_Canadian_Legal_Framework_for_Evidence.pdf
[29] ISO/IEC 2016. ISO 15489-1:2016 – Information and Documentation – Records Management – Part I: General Information and Documentation – Records Management – Part I: General. ISO, http://www.iso.org/iso/catalogue_detail?csnumber=31908 (hereinafter ISO 15489).
[30] InterPARES 2, Terminology Database, Op. Cit. fn. 28.
[31]Quinn Dupont and Bill Maurer (2014), "Ledgers and the Law in Blockchain," *The King's* Review., http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain/#top). This paper traces the blockchain's roots back to earlier forms of accounting ledgers to discuss some of the ways in which they are similar and also differ; however, their paper is written from the perspective of the philosophy of information rather than archival science, and therefore, is less technically detailed than needed for archival purposes. It also only covers certain types of blockchain applications. Much more extensive archival research would be necessary to understand blockchain ledgers as records in a wide variety of configurations, and to assess the implications of their characteristics for the production and preservation of trustworthy evidence.
[32] Tapscotts, 2016, p. 7.
[33] Recent examples include the Government of Estonia, which is working with Bitnation to provide notarization and identity services to e-residents on the blockchain [See, Bitnation.co, n.d.,"GOVERNANCE 2.0 BORDERLESS | DECENTRALIZED | VOLUNTARY," https://bitnation.co/join-the-team/] and the government of Dubai, which recently announced that it wants all government records on the blockchain by 2020 [See, Michael del Castillo (2016, October 5), "Dubai Wants All Government Documents on Blockchain By 2020," http://www.coindesk.com/dubai-government-documents-blockchain-strategy-2020/. The UK Government has also written a major report calling for exploration of the application of blockchain technology in a wide variety of areas [See UK Government Chief Scientific Advisor (2016), "Distributed Ledger Technology: beyond the block chain," Government Office for Science, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf]. For a good general overview of government activity in the blockchain space, see William Mougayar, (2016, August 22), "The Blockchain is Perfect for Government Services, but Where is Canada?," *The Huffington Post*, http://www.huffingtonpost.com/william-mougayar/the-blockchain-is-perfect_b_11657794.html.
[34] InterPARES 2 Terminology Database, Op. Cit, fn. 28.
[35] We admit to several limitations of our survey of the technoscape: Teams of innovators are often international in nature, so the place of registration of the company does not always tell the full story. Also, government and financial industry projects are not well-advertised in general. Finally, non-English-speaking projects often do not translate their news into English, so we likely missed many European projects outside the UK, as well as from other non-English-speaking jurisdictions.
[36] See the R3 website, https://r3cev.com/about/.
[37] "Blockchain and Ripple Solutions | Bluzelle - We build solutions over Blockchain and Ripple," n.d. http://bluzelle.com.

[38] Hanumanth K. Jayakumar | LinkedIn. n.d., https://www.linkedin.com/in/hanumanthk.
[39] Blockstream, n.d., https://www.blockstream.com/.
[40] “Cryptiv,” n.d., https://cryptiv.com/.
[41] Bitcoin Alliance of Canada | Promoting Bitcoin in Canada, n.d., http://bitcoinalliance.ca/.
[42] Business Wire (2015, November 13), “Quadriga to Launch First Canadian Blockchain R&D Lab,” http://www.businesswire.com/news/home/20151112006775/en/Quadriga-Launch-Canadian-Blockchain-Lab.
[43] What we do – Digital Finance Institute, n.d., http://www.digitalfinanceinstitute.org/?page_id=892.
[44] Ibid.
[45] “What we do – Digital Finance Institute,” n.d., Op Cit.
[46] See, http://velocity.technology/#about-velocity-team.
[47] See, https://www.bitaccess.co.
[48] See, https://privacyshell.com/about-us/.
[49] For example, Deputy Governor of the Bank of Canada, Carolyn Wilkins has noted that “the potential for DLT is actually stronger for applications outside of digital currencies. We have seen test cases related to payments and post-trade processes, including the clearing and settlement of financial instruments such as repos, bonds, derivatives and equities.”, [C. Wilkins, (2016, June 17), “Fintech and the Financial Ecosystem: Evolution or Revolution? Bank of Canada,” http://www.bankofcanada.ca/2016/06/fintech-financial-ecosystem-evolution-revolution/]. Also, Digital Asset Holdings is one company that has projects under way to explore the use of distributed ledgers with the Australian Securities Exchange (ASX) for the Australian equity market and with Depository Trust & Clearing Corporation for the clearing of repo transactions in the United States.
[50] Amit (2016, March 28), “12 Companies Leveraging Blockchain for Identification and Authentication,” https://letstalkpayments.com/12-companies-leveraging-blockchain-for-identification-and-authentication/.
[51] See, Bitnation.co, (n.d.), Op. Cit., fn. 33.
[52] S. Higgins, (2016, April 22), “Republic of Georgia to Develop Blockchain Land Registry,” *Coindesk*, http://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry/.
[53] G. Chavez-Dreyfus, (2016, June 16), Sweden tests blockchain technology for land registry,” http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV.
[54] J. Redman, (2016, May 26), “Bitland: Blockchain Land Registry Against ‘Corrupt Government’,” https://news.bitcoin.com/bitland-blockchain-land-registry/
[55] I. Allison (2016, July 11). “Blockchain-powered real estate platform Ubitquity records first property ownership transfer on the Bitcoin public ledger,” http://www.ibtimes.co.uk/blockchain-powered-real-estate-platform-ubitquity-does-first-property-ownership-transfer-bitcoin-1569980.
[56] See, for example, The LTB Network, YouTube, https://www.youtube.com/user/LetsTalkBitcoinChan.
[57] See L. Kuo, (2016, February 19), “Imogen Heap wants to use blockchain technology to revolutionize the music industry,” http://qz.com/620454/imogen-heap-wants-to-use-blockchain-technology-to-revolutionize-the-music-industry/
[58] G. Prisco, (2016, April 27), “BitFury Announces Blockchain Land Titling Project with the Republic of Georgia and Economist Hernando De Soto,” https://bitcoinmagazine.com/articles/bitfury-announces-blockchain-land-titling-project-with-the-republic-of-georgia-and-economist-hernando-de-soto-1461769012
[59] M. Rouse, M, (2014), “Digital signature,” SearchSecurity.TechTarget, http://searchsecurity.techtarget.com/definition/digital-signature.
[60] For more information about how Certificate Authorities fit into the public key infrastructure (PKI) typically used in digital signatures, see the background paper by Stephen Thompson, Volume 2, Appendix A of this report.
[61] Proof of Work (PoW) refers to the computational problem-solving process that the Bitcoin and other blockchain miners carry out while verifying a transaction, a block or document transfer. It works on the same principle as a CAPTCHA where the prospective user has to pass a test in order to access a service [F. Pedro, (2015), “Understanding Bitcoin: Cryptography, engineering and economics,” (Chichester: John Wiley & Sons Ltd), p. 102). Proof-of-work utilizes the blockchain’s computational power against attempts to tamper with the blocks (p. 95). Proof-of-work relates to the main principle of hashing: the hashing is a proof-of-work that the document has been authenticated.
[62] F. Amati, (2016). “Using the blockchain as a digital signature scheme,” *Medium.com*, Consentio blog, https://medium.com/consentio-blog/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826#.rklubpmd0.
[63] (n.d.), “Academic Certificates on the Blockchain,” MSc in Digital Currency, University of Nicosia, http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/.
[64] I. Allison (2016, June 29), “Ethereum-based APPII works with Open University to verify academic records on blockchains,” *International Business Times,* http://www.ibtimes.co.uk/ethereum-based-appii-working-open-university-verify-qualifications-blockchains-1568092.

[65] See, MIT Media Lab (2016, June 2), "What we learned from designing an academic certificates system on the blockchain," https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196#.2dwu2ka94.

[66] H. Stancic (2016, September 18), "Blockchain-based records management," European Association for Banking and Financial History (EABH) Summer School for Archivists on "Transparency and information management in financial institutions," Banco de España, Madrid.

[67] G. Zyskind, O. Nathan & A. Pentland (2015, May), "Decentralizing privacy: Using blockchain to protect personal data.," in *IEEE Security and Privacy Workshops (SPW),* pp. 180-184, http://web.media.mit.edu/~guyzys/data/ZNP15.pdf.

[68] Y.B. Perez (2015), "Medical Records Project Wins Top Prize at Blockchain Hackathon," *Coindesk,* http://www.coindesk.com/medvault-wins-e5000-at-deloitte-sponsored-blockchain-hackathon/.

[69] V. Buterin (2016, January 15), "Privacy on the Blockchain," *Ethereum Blog*, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

[70] G. Greenspan & M. Zehavi (2016, January 17), "Will Provenance Be the Blockchain's Break Out Use Case in 2016?," *CoinDesk*, http://www.coindesk.com/provenance-blockchain-tech-app/.

[71] Ibid.

[72] K. Patel (2015, September 15), "Everledger: putting bling on the blockchain," FusionWire, http://www.fusionwire.net/innovators/everledger-putting-bling-on-the-blockchain/.

[73] Tapscotts, 2016, p. 205.

[74] (n.d.), "Provenance | For Non-Profits, https://www.provenance.org/how_it_works/non_profits.

[75] Y.B. Perez (2015, December 17), "How Provenance is Channeling the Blockchain for Social Good," http://www.coindesk.com/provenance-channeling-blockchain-social-good/.

[76] M. von Haller Gronbaek (2016, June 16) "Blockchain 2.0, smart contracts and challenges," *Bird & Bird,* http://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges.

[77] B. Deery (2016, May 7), "The Blockchain & Future of Business Records - Brian Deery, Chief Scientist of Factom, Inc," *Blockchain News*, http://www.the-blockchain.com/2016/05/07/blockchain-future-business-records-brian-deery-chief-scientist-factom-inc/

[78] See a detailed analysis of the Factom solution by this author: V.L. Lemieux (2016), "Trusting Records: Is Blockchain Technology the Answer?" *Records Management Journal*, 26(2): 110 – 139.

[79] Cited in C. Finlay(2015), "Decentralised and inviolate: the blockchain and its uses for digital archives," https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.

[80] A. van Wirdum, Aaron (2015), "Blocktech Introduces Uncensorable Peer-to-Peer Media 'Library' Alexandria," The Cointelegraph, https://cointelegraph.com/news/blocktech-introduces-uncensorable-peer-to-peer-media-library-alexandria

[81] K. Shirriff (2014), "Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software," *Ken Shirriff's blog,* http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html

[82] To say that hashes cannot be reversed engineered does not imply that they cannot be broken. With the improvement of IT, older functions are breakable. As an example, the Estonian digital signature first developed in late 1990's is relatively weak; thus, the reason for replacing it two years ago for a newer format and more secure hash algorithms [feedback on this report from Kuldar Aas Deputy Digital Archivist, National Archives of Estonia].

[83] Cassie Findlay, (2015), Op. Cit., fn. 66, states that that blockchain " . . . could offer an uncontested space from which records could be accessed. Documents and other sets of data can be validated by the blockchain – even if an application you used to get it there is not working. It is decentralized proof which can't be erased or modified by anyone; competitors, third parties, governments. This is what distinguishes using the blockchain from other forms of data timestamping and authentication."

[84] ISO/IEC, 2012. ISO 14721: 2012 – Space data and information transfer systems – Open archival information system (OAIS) – Reference model, http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284

[85] Finlay, 2015, op. cit., fn. 79.

[86] rblockologist cited in Finlay, 2015, op. cit., fn. 79.

[87] Ibid. Rosenthal is referring specifically to the Bitcoin blockchain, but his criticisms may be extended to other blockchains as well.

[88] DuPont and Maurer, 2014, op. cit., fn. 31.

[89] Feedback to the principal investigator on the September 30 draft of this report from Ethan Wilding.

[90] For more on the shift in preservation model see Peter van Garderen, (2016, April 11), "Decentralized Autonomous Collections," https://medium.com/on-archivy/decentralized-autonomous-collections-ff256267cbd6#.pb3suwrj5. We already see these risks potentially materializing in the form of transactions that do not complete, i.e., do not become anchored on

the Bitcoin blockchain, because end users have not bid high enough for recordation to incentivize miners to validate the transactions. On this point, see Nicola Minichiello, "The Bitcoin Fee Event Cometh," https://www.factom.com/the-bitcoin-fee-event-cometh/. On the other hand, if all the world's libraries and archives came together to operate as one blockchain network, it may be possible to realize a purpose-built distributed archival preservation model.

[91] Buterin, 2016, Op. Cit., fn 69.

[92] See, Lemieux, 2016, Op. Cit., fn. 78; G. Yeo (2013), "Trust and context in cyberspace," *Archives and Records 34*(2): 380; L. Duranti & C. Rogers (2012), "Trust in digital records: An increasingly cloudy legal area," *Computer Law & Security Report*, *28*(5): 522.

[93] See fn. 122.

[94] See, for example, P. Vessenes, 2016. "Ethereum Contracts are Going to be Candy for Hackers," Peter Vessenes blog, http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/;
"Ethereum Contracts Are Going To Be Candy For Hackers," 2016, c. June 8, *EthTrader Reddit* site, and "Ethereum contracts are going to be candy for hackers," 2016, c. June 8., Hacker news, https://news.ycombinator.com/item?id=11725624

[95] "The tampering aspect, with the DAO, is a transfer of balance to a different contract; all fully auditable. Here too there is a record of the changes to the data structure. The concern is that the community voted (with mining power) to move funds from one account to another, and thereby violate in a small measure the idea of complete immutability. Nevertheless, the changes have been recorded and are public record." [Feedback to principal investigator on the September 30 draft of this report from Ethan Wilding].

[96] See, for example, Lemieux, 2016, Op. Cit. fn. 65, and Walch, 2016, Op. Cit., fn. 20.

[97] InterPARES 2 Terminology Database, Op. Cit, fn. 33.

[98] Vermont Legislature (2016, May 6), 12 V.S.A. § 1913 Sec. I.1, "Blockchain Technology," http://legislature.vermont.gov/assets/Documents/2016/Docs/JOURNAL/hj160506

[99] The company states that its solution Alfa E-archive assurer is based on the OAIS (ISO 14721) principles and supports metadata schema according to Metadata Encoding and Transmission Standards (METS) using Dublin Core, Metadata Object Description Schema (MODS), and Preservation Metadata Maintenance Activity (PREMIS) metadata schemas. In their system, records are stored in their own system and all added records, metadata or changes are timestamped with Enigio's time:beat technology. Then, the hashes and digital fingerprints of the records and metadata are anchored in Enigio's blockchain aggregation. [See, https://enigio.com/e-archive].

[100] This section is based upon the paper by Mark Penney in this report [see Volume 2, Appendix A]. Penney's paper contains much more detail about the global blockchain research landscape, and readers are encouraged to review it for more information. In addition, Penney has prepared a compendium of blockchain research (see Appendix D).

[101] Wilkins, 2016, Op. Cit., fn. 49.

[102] Ibid.

[103] S. Eskandari, D. Barrera, E. Stobert, & J. Clark (n.d.). "A First Look at the Usability of Bitcoin Key Management," USEC 2015 Workshop, San Diego, CA: Internet Society, http://www.internetsociety.org/sites/default/files/05_3_3.pdf

[104] (n.d.), "Security and Privacy of Bitcoin," http://www.syssec.ethz.ch/research/Bitcoin.html

[105] DuPont and Maurer, 2014, Op. Cit., fn. 31.

[106] Q. DuPont (2014), "The Politics of Cryptography: Bitcoin and The Ordering Machines » The Journal of Peer Production," Journal of Peer Production, (4), http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/.

[107] Proceedings of the Standing Senate Committee on Banking, Trade and Commerce (n.d.), http://www.parl.gc.ca/content/sen/committee/412/BANC/07EV-51307-E.HTM

[108] François Coallier, (2016), "A Systems Engineering Perspective to Blockchain Standardization," https://docs.google.com/presentation/d/11WwKRK8RrGokPvrm3APshHY_DlyYOKz_ipc8K2wXVmA/pub?start=false&loop=false&delayms=3000&slide=id.p4.

[109] See http://blockchaincanada.org and https://blockchainedu.org/.

[110] Ibid.

[111] For a more detailed discussion of our findings on research initiatives outside of Canada, refer to Penney's background paper (This report, Volume 2, Appendix A).

[112] Stancic is also a member of InterPARES Trust, a SSHRC-funded international research consortium focused on the long-term preservation of authentic electronic records, which is based at the University of British Columbia and led by Professor Luciana Duranti. See, https://interparestrust.org.

[113] T. Thomassen (2015), "Archival science," in L. Duranti & P. Franks, *Encyclopedia of Archival science* (Rowman & Littlefield),

[114] L. Duranti, & R. Preston (2008), *International research on permanent authentic records in electronic systems (InterPARES) 2: Experiential, interactive and dynamic records*, (CLEUP), pp. 34-35.
[115] See also V. Lemieux, 2016. "Provenance: Past, Present and Future in Interdisciplinary and Multidisciplinary Perspective," in *Building Trust in Information* (Springer International Publishing), pp. 3-45.
[116] For more on the potential of blockchain in this regard, see Jason R. Baron (2016), "A Blockchain Future?: The need to ensure our digital heritage remains trustworthy, increases with time," *Legal Tech News* (March/April), http://www.legaltechnews.com/id=1202753737799/Blockchains-The-Future-of-Recordkeeping?slreturn=20160329105023 and van Garderen, Op. Cit., fn. 90.
[117] F. B. Cross, F. B. (2004), "Law and Trust." *Geo. Law Journal* 93: 1484.
[118] E. D. Baker (2015), "Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange." *Southwestern Law Review* 45: 341–433.
[119] See, for example, the classic paper on this theme by Nick Szabo (1997-1999), The God Protocol, http://szabo.best.vwh.net/msc.html.
[120] A hard fork involves splitting a blockchain so that future transactions are recorded on a new chain stemming from the original chain.
[121] V. Buterin (2016, July 26), "Onward from the Hard Fork," *Ethereum Blog*.https://blog.ethereum.org/2016/07/26/onward_from_the_hard_fork/. See also, ____ (2016, July 18), "Everthing you need to know about the Ethereum 'hard fork,'" *Quartz*, http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/. According to Ethan Wilding of Ledger Labs, the hard fork involved moving all funds from contracts with the code hash 7278d050619a624f84f51987149ddb439cdaadfba5966f7cfaea7ad44340a4ba to a new contract "RefundDAO" and replacing the contract at the main DAO with a simple refund contract with only one function. This function takes one parameter (address of childDAO), to determine a combined balance of mainDAO and childDAO and then paid back Ether accordingly (in order to also pay back DAO token holders who did already split)"[Feedback to principal investigator on September 30 draft of this report].
[122] Ethereum blockchain is proposing to use a different consensus mechanism. Rather than using Satoshi Nakamoto's "proof of work" (PoW) consensus algorithm, Ethereum proposed to use a "proof of stake" (PoS) approach, wherein those who hold Ether, Ethereum's base cryptocurrency, "vote" on accepting transactions according to their share of Ether. On the rationale for the PoS, see V. Buterin (2016, July 27), "On Inflation, Transactions fees and Cryptocurrency Monetary Policy," *Ethereum Blog*, https://blog.ethereum.org/2016/07/27/inflation-transaction-fees-cryptocurrency-monetary-policy/
[123] Op Cit, and Buterin (2016, July 26), Op. Cit., fn. 121. Read in particular the comments on the blog post. It should be noted that the hard fork strategy is not unique to Ethereum. Bitcoin miners have performed at least one rollback, in 2010, to fix a technical glitch, and in March 2013 there was also a fork [See, Vitalik Buterin (2013, March 13), "Bitcoin Network Shaken by Blockchain Fork," https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448.
[124] See, for example, I. Allison, (2016, June 19). "Legal experts examine the DAO attack and Ethereum fork," *International Business Times*, http://www.ibtimes.co.uk/legal-experts-examine-dao-attack-ethereum-fork-1566318;
M. Levine (2016, June 17), "Blockchain Company's Smart Contracts were Dumb," *BoombergView*, https://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb.
[125] Dupont and Maurer, 2014, fn. 31.
[126] Canadian General Standards Board. (2005). National standard of Canada ; CAN/CGSB-72.34-2005: Electronic records as documentary evidence. Gatineau, Quebec: National Standards of Canada.
[127] For a fuller discussion of these laws and associated legal issues, see the background paper in this report (Volume, 2 Appendix A) by Darra Hofman.
[128] Accenture recently announced an "editable" blockchain, but since immutability is one of the key features establishing the "trustless" nature of the blockchain, this innovation raises questions about how the solution differs from standard database technology [See, Martin Arnold (2016,September 19), "Accenture to unveil blockchain editing technique," *Financial Times*, https://www.ft.com/content/f5cd6754-7e83-11e6-8e50-8ec15fb462f4].
[129] Long retention periods will also apply in cases where records are needed to prove ownership of land, proof of identity (e.g., for citizenship purposes), or historical research purposes. The same issues of long-term preservation, authenticity and accessibility apply in these cases.
[130] Lemieux, 2016, Op. Cit., fn. 115.
[131] For more on the issues associated with relying on blockchain technology for preservation of digital heritage, see Baron Op. Cit., fn. 116.
[132] V. Lemieux, ed. (201*Financial Analysis and Risk Management: Data Governance, Analytics and Life Cycle Management*. (Springer Science & Business Media).

[133] J. Barrdear & M. Kumhof (2016, July). "The macroeconomics of central bank issued digital currencies," Bank of England Staff Working Paper No. 605, http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf
[134] US Treasury, Financial Stability Oversight Council (2016), Annual Report, https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf and W.E. Weber, 2016. "A Bitcoin Standard: Lessons fromthe Gold Standard," Bank of Canada Staff Working Paper 2016-14.
[135] Ibid.
[136] Op. cit., fn. 105.
[137] See, for example, Walch, 2015 and 2016. Several in the industry say that there does not seem to be consensus on how to properly compensate the relatively resource-intense (in terms of computing power) blockchain. This itself could be an avenue for a significant amount of fraud, not necessarily within the system (e.g. malicious actors) but motivating the theft of computing resources. Specifically, anecdotal evidence has indicated that many people have already been victims of identity theft with the explicit goal of overtaking cloud-computing virtual machines and using them as part of Bitcoin-farms, incurring potentially millions in costs [Feedback on a draft this report from Nicholas Connizzo, September 2016].
[138] D. Andolfatto (2016, May 1), "Monetary Policy Implications of Blockchain Technology." MacroMania Andolfatto Blogspot, http://andolfatto.blogspot.ca/2016/05/monetary-policy-implications-of.html.
[139] Barrdear and Kumhof, 2016.
[140] For a survey of theories on financial contagion see, for example, P. Glasserman & H.P Young (2015, October 20), "Contagion in Financial Networks," OFR Working Paper, https://financialresearch.gov/working-papers/files/OFRwp-2015-21_Contagion-in-Financial-Networks.pdf.
[141] Op Cit.
[142] Op Ct, fn. 84.
[143] M. del Castillo, Michael (2016, July 18,) "ISITC Europe Proposes 10 Blockchain Standards Benchmarks," CoinDesk, http://www.coindesk.com/isitc-blockchain-standards-benchmarks/.
[144] ISITC Europe (n.d.) "ISITC Blockchain Working Group: A Framework for DLT Standards," http://www.isitc-europe.com/files/documents/160705-ISITC-Website-Standards.pdf.
[145] M. Arnold (2016, 23 August), "Big banks plan to coin new digital currency," *Financial Times*,
[146] This event was attended by the principle investigator. More information is available here: https://www.w3.org/2016/04/blockchain-workshop/report.html.
[147] J. Redman (2016, September 9), "Wanda Group Joins Hyperledger to Create New Blockchain Standards," https://news.bitcoin.com/cinema-wanda-group-hyperledger-project/.
[148] See, http://www.omgwiki.org/OMG-FDTF/doku.php?id=blockchain-wg-page
[149] B. Cohen (2016, May 25), "ISO May Propose Certified Standards for Blockchains and Distributed Ledgers," *Bitcoin Magazine,* https://bitcoinmagazine.com/articles/iso-may-propose-certified-standards-for-blockchains-and-distributed-ledgers-1464189647.
[150] A. Deichler (2016, February 2), "Blockchain Talk: Technology First, Standards Second," *AFP,* http://www.afponline.org/trends-topics/topics/articles/Details/blockchain-talk-technology-first-standards-second.
[151] See, US National Archives and Records Administration (n.d), "Department of Defense (DoD) Standard 5015.2," http://www.archives.gov/records-mgmt/initiatives/dod-standard-5015-2.html.
[152] J. Gable (2002), "Everything You Wanted to Know about DoD5015.2," *Information Management* 36, 6, https://www.questia.com/magazine/1P3-270189821/everything-you-wanted-to-know-about-dod5015-2