Blockchain Technology for Recordkeeping

Help or Hype?

A Background Paper "Blockchain Technology for Recordkeeping – Help or Hype?" a SSHRC Knowledge Synthesis Grant Study on "How can emerging technologies be leveraged to benefit Canadians?"

Investigator Dr. Victoria L. Lemieux
vlemieux@mail.ubc.ca

Volume 2: Appendices

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

Table of Contents

Report……Volume 1

Appendix A – Background Paper……34
Appendix B - Terminology Report ……103
Appendix C – Blockchain Companies ……142
Appendix D – Blockchain Research Initiatives ……155
Appendix E – Consultation Collaborators……160
Appendix F – Dissemination Coverage ……161
Appendix G - A Primer on Records and Recordkeeping……162
Appendix H - A Primer on the Blockchain and how it operates……165

Appendix A – Background Papers

The papers in this appendix should be viewed as works in progress and not as polished reports representing the final views of the project team.

Blockchain Technology for Recordkeeping

The Law Beyond Trust: Legal Implications of Blockchain Technology for Records Management

A Background Paper "Blockchain Technology for Recordkeeping – Help or Hype?" a SSHRC Knowledge Synthesis Grant Study on "How can emerging technologies be leveraged to benefit Canadians?"

Prepared by: Dara Hofman, Doctoral Student, Archival science for Principal Investigator Dr. Victoria L. Lemieux

The University of British Columbia, Vancouver, BC, V6T 1Z1
Phone: 604 822 2404
E-Mail: vlemieux@mail.ubc.ca

Table of Contents

INTRODUCTION **36**
FINANCIAL REGULATION **37**
PROPERTY RIGHTS **38**
REAL PROPERTY **39**
PERSONAL PROPERTY **40**
INTELLECTUAL PROPERTY **41**
"SMART CONTRACTS" AND CONTRACT LAW **41**
DRAFTING, SPECIFIC PERFORMANCE AND EQUITABLE PRINCIPLES **42**
"SMART PROBATE": TRUSTS AND ESTATES **42**
EVIDENCE **43**
CONCLUSION **44**
REFERENCES **44**

Introduction

The relationship between law and archival science is an ancient one, based upon society's need for trust. 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 behavior'."[1] The law, in turn, must have trustworthy records in order to provide remedies that provide a sense of justice; without a trustworthy copy of a contract, for example, a court cannot say if a breach has occurred, and if it has, which parties are owed what remedy. Archival science has developed to meet the need for trustworthy records. However, advancing information and communication technologies (ICTs) have required us to continually update our paradigm for assessing the trustworthiness of records, especially as records are increasingly born-digital. Now, some scholars assert that, thanks to blockchain technology, we're moving beyond trust, to an era of "trustless transfer" leading to an extralegal system of rights management (Baker, 2015).

Blockchain technology, also known as distributed ledger technology (DLT), is not yet a concept with an agreed upon definition. For the purposes of this paper, we will define blockchain as a technology that records transactions in a distributed ledger, using cryptographic hashes to record and verify each transaction (Lemieux, 2015). The most famous blockchain, the Bitcoin blockchain, uses as anonymized public ledger, which authenticates blocks using "proof of work," where users "earn" the ability to verify blocks on the chain by using their computer processing power to solve equations. However, the Bitcoin blockchain is not the only possible configuration. Private blockchains – such as the one being experimented with by the consortium R3CEV, which includes a number of major banks – are also possible. Authentication by "proof of stake," in which users buy their right to authenticate blocks by spending resources is also a possibility. Each of these configurations has different operational risks, discussed more fully in Walch, 2016, that in turn, alter the liabilities and legal risks that attach to the blockchain as recordkeeping system.

[1] Cross, 2003, p.1484).

Because blockchain is a "trustless" system, it 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 technology. However, this "trustless" system does not actually move us beyond the need for trusted third parties, nor does it remove the enormity of the law in preserving rights and ensuring public trust. As Victoria Lemieux explains, at least with regards to systems where the records themselves are created and maintained outside of the blockchain: "Does using the Bitcoin Blockchain ensure the trustworthiness of the records? No. Trustworthiness is only guaranteed if the records are both reliable and authentic.2 Blockchain solutions do not address the reliability of records, and there are many features of the Bitcoin Blockchain that may negatively affect the authenticity of information as well." (2016). The issue or reliability is different with regards to cases such as smart contracts or smart probate, where the record itself is hashed to the blockchain. In such a case, reliability is inherently bound up in the blockchain.[3]

Blockchain technology has largely been associated with cryptocurrencies heretofore, and much of the legislation and regulation that directly addresses blockchain thus far comes from financial and securities law. However, blockchain technology has potential recordkeeping uses far beyond cryptocurrency, and those uses have significant and wide-ranging legal ramifications. Financial uses being explored include payment systems, corporate share issuance, and same day Treasury and security settlement. Potential uses outside of finance include smart contracts and wills, blockchain protection of personally identifiable information in data lakes, and automating back office procedures. Because of the breadth of potential uses for blockchain technology, a substantial number of legal issues are raised by its implementation, including financial regulation, property rights, contract drafting and enforcement, trusts and estates, information security and privacy law, and the law of evidence and rules of civil and criminal procedure. Each of these areas encompasses an extremely large body of law; to address each area and its interrelationship with the blockchain in depth could generate papers, if not books. This paper explores the broad, common legal issues raised by the use blockchain for recordkeeping. Furthermore, while these issues are common to jurisdictions where the blockchain is being used, their regulation and ultimate resolution will depend on the legal landscape in that jurisdiction.

Financial Regulation

Unsurprisingly, given blockchain's close association with Bitcoin and other cryptocurrencies, most of the existing regulation that directly addresses blockchain comes from the various financial regulatory bodies. In some ways, the financial regulations and guidances that have arisen in regards to blockchain technology, and specifically cryptocurrency, are a grab bag: regulations pursued retroactively as issues have arisen, rather than proactively as part of a broader blockchain strategy. Ultimately, it remains an area of law in deep fluxand taxation." However, several themes emerge that are relevant to understanding the role of blockchain recordkeeping from a legal perspective. Much of the tension with regards to permissionless, public blockchain technology, like Bitcoin, for financial purposes arises from its decentralized nature (Walch, 2015, p. 869). While this decentralization is seen "by the Bitcoin Foundation as '[a] key characteristic of Bitcoin and a source of its strength," (Walch, 2015, p. 869), it none the less poses significant operational risks should such blockchain technology be used as the backbone of financial transactions and recordkeeping beyond the cryptocurrency;

[2] "Reliability" and "authenticity" are both terms of art within archival science. Richard Pearce-Moses, in the Society of American Archivists' Glossary of Records and Archival Terminology, defines reliability as "n. (reliable, adj.) ~ 1. The quality of being dependable and worthy of trust. - 2. The quality of being consistent and undeviating. - 3. Diplomatics · Created by a competent authority, according to established processes, and being complete in all formal elements." Authenticity, on the other hand, is "The quality of being genuine, not a counterfeit, and free from tampering, and is typically inferred from internal and external evidence, including its physical characteristics, structure, content, and context." In other words, reliability must be present at the creation of a document, while authenticity must be continuously preserved.

[3] Although, as discussed *infra*, issues such as fraud can still lead to the creation of records that, while trustworthy, are nonetheless legally unenforceable.

those operational risks raise the spectre of significant, far-reaching liability. However, private blockchains, particularly if they rely on permissions or proof-of-stake, as opposed to proof-of-work, invoke the same concerns about the trusted custodian as more traditional means of recordkeeping. Furthermore, utilizing the blockchain, even outside of cryptocurrency, could theoretically bring users under the purview of extensive financial regulations.

In Canada, for example, a report issued by the Standing Senate Committee on Banking, Trade and Finance noted the many types of regulatory authority that could be brought to bear on digital currency, noting specifically that "the Department of Finance noted that the federal government has broad oversight responsibilities" with regards to payment systems (2016, p. 56). Even though the report comes down favorably regarding digital currency, the committee notes a number of potential challenges, including "potential criminality, losses, taxation issues, and access to information and protection for users, […] the Bitcoin verification process; seignorage revenue for the Bank of Canada and the federal government; and the ability of businesses to access letters of credit for digital currencies" (2016, p. 56). Many of these issues are likely to the point of near certainty to require legislation and regulation to resolve.

In the U.S., FinCEN has held that issuing proof of ownership on the blockchain brings one under FinCEN's authority under the Bank Secrecy Act, because those digital titles can then be transferred, making them analogous to a bearer bond, and the issuer regulable as a money transmitter (FIN-2013-G001; I.R.S. Notice 2014-21,2014-16 I.R.B. 938; FIN-2015-R001). In Canada, FINTRAC similarly holds that "any person who is in the business of effecting a transfer of currency through the medium of a bitcoin transfer is a "money services business" who must comply with FINTRAC reporting regulations. A person operating such a "money services business" (MSB) must register with FINTRAC and file appropriate reports of all currency transactions" (Johnson, 2016). The IRS classifies digital currency, including blockchain-based cryptocurrency, as personal property, subject to taxation (I.R.S. Notice 2014-21, 2014-16 I.R.B. 938). The FTC and SEC are both actively figuring out the contours of regulation, deciding, respectively, whether cryptocurrency is a commodity or a security, and how to address it under their respective regulatory schemes. In short, cryptocurrency – and blockchain more broadly – are not a libertarian alternative to the current legal system, but are yet another technology that the legal system will have to grapple with using extant tools and policies.

Property Rights

"Property" is a very broad concept in the law, encompassing "the right to possess, use, and enjoy a determinate thing […]; the right of ownership […and] [a]ny external thing over which the rights of possession, use, and enjoyment are exercised" (Garner, 2001, p. 987). The breadth of rights and obligations encompassed within property law means that the records related thereto are of critical importance. Bell and Parchomovsky, calling for renewed study of registries, explain the ongoing importance of property records and registries:

> The property-information interface is perhaps the most crucial and under-theorized dimension of property law. Information about property can make or break property rights. Information about assets and property rights can dramatically enhance the value of ownership. Conversely, dearth of information can significantly reduce the benefit associated with ownership. It is surprising, therefore, that contemporary property theorists do not engage in sustained analysis of the property-information interface and in particular of registries — the repositories of information about property (2016, p. 237).

As Lemieux discusses, using blockchain for registry purposes offers potential benefits, including a theoretically impossible to alter audit trail (2015). However, it is not without costs and risks. In particular, most of the costs of setting up a Trusted Digital Repository are still at hand with a blockchain registry, and the data storage required to maintain an immutable blockchain of any size is considerable. Furthermore, a property blockchain registry raises specific challenges and opportunities within different categories of property. Discussed *infra* are the three

broad categories of "property" most often discussed in the law: real property, personal property, and intellectual property.

Real Property

Real property is "land and anything growing on, attached to, or erected on it, excluding anything that may be severed without injury to the land" (Garner, 2001, p. 988). Of all the types of property, real property is perhaps the least obvious for the application of blockchain. However, some of the oldest, most well-developed legal forms and recordkeeping system revolve around real property rights – deeds, land registries, mortgages, surveys, encumbrances, and easements must all be created and maintained in as reliable, authentic, and accurate a form as possible to preserve rights and resolve disputes. One possible application of the blockchain is in creating and preserving digital real property records, either in conjunction with or in place of traditional real property records systems. For example, both Honduras and the Republic of Georgia have announced their intentions to pursue blockchain land registries (Rizzo, 2015; Higgins, 2016), although the Honduran project has since stalled (Rizzo, 2015).

The vision of blockchain based land recording is ambitious and highly optimistic. The chairman of Georgia's National Agency of Public Registry stated:

> By building a Blockchain-based property registry and taking full advantage of the security provided by the Blockchain technology, the Republic of Georgia can show the world that we are a modern, transparent and corruption-free country that can lead the world in changing the way land titling is done and pave the way to additional prosperity for all (Higgins, 2016).

With either a nascent or reborn legislative framework to support such a system, it's possible that a blockchain land record system could indeed have good results. However, in a complex, mature set of systems such as those in the U.S. and Canada, implementing a blockchain land registry would require significant political buy-in (and would only apply to a particular state, province, or territory). Furthermore, a "corruption-free" system still requires reliable, corruption-free underlying documentation; as discussed below, even such a "trustless" system ultimately depends upon trustworthy third parties, not just trustworthy algorithms.

It's difficult to discuss land recording in the U.S. or Canada in too much detail within the scope of this paper, because each state, province, and territory has its own laws controlling land conveyance, recording, and remedies. However, general principles can be discerned which show the complexity of applying blockchain to such mature land recording regimes. For example, the fallout from the subprime mortgage crisis in the United States revealed massive flaws in the way records related to mortgages are preserved and controlled, particularly in cases where the debt was either sold to or serviced by a party other than the original lender and with mortgages entered in the Mortgage Electronic Registration System (MERS); the records problem found its worst incarnation in the "robo-signing" scandal wherein servers presented the courts with thousands of falsified affidavits to support foreclosure actions wherein the original documents could not be produced (Mosson, 2012). Blockchain enterpreneurs, such as Factom CEO Peter Kirby, see blockchain as the solution:

> The mortgage process is just a record keeping problem. What happened when? And did the sequence match the compliance rules? If we can timestamp the compliance events and make the records immutable, then we have a powerful way to prove that the loan was correctly made. We can also use the same system to track payment records and court proceedings." (Mizrahi, 2016).

Even Kirby, however, acknowledges the challenges of ensuring that the original mortgages verified by the

blockchain are reliable, or, as he puts it, "the 'garbage in, equals garbage out' problem" (Mizrahi, 2016). While Kirby discusses the power of an "immutable audit trail" (Mizrahi, 2016) to keep parties honest, the question of reliable mortgages at the outset still requires, not technological solutions, but trusted parties.
Furthermore, while a blockchain mortgage system can track court proceedings, the courts themselves are not bound to recognize the blockchain system. Disputes regarding real property rights are still, ultimately, the province of the court to resolve, and parties can seek to admit evidence in addition to that found on the blockchain (for example, evidence of material fraud or equitable concerns). Discretion ultimately remains with the court – not the blockchain – to determine the facts of the case and to resolve any disputes. Even a self-executing blockchain contract – including a real property contract – is not beyond the bounds of a court to void or modify, if legal and factual justification exists. Thus, without significant legislative change, blockchain mortgages, while theoretically more trustworthy than their paper or non-blockchain digital counterparts, would provide just another form of evidence, and not a definitive answer, when real property rights are in dispute.

Looking specifically to Ontario, one finds an example of an existing system that could presumably solve the reliability problem with regards to land records, at least in a majority of cases. Under the *Land Registration Reform Act*, only "lawyers entitled to practice law and who have obtained the required Real Estate Practice Coverage Option (REPCO) from Lawyers Professional Indemenity Company are able to approve electronic documents containing compliance with law statements" (The Law Society of Upper Canada, 2015). A compliance with law statement is a legally binding assurance on the part of the lawyer registering documents with the electronic land registry that legally sufficient evidence exists to register that particular electronic document. In other words, a trusted party (a lawyer) must certify the reliability of the record in order to enter it into the system. Once such a record is entered, the law presumes that other parties may rely upon it as being both reliable and authentic. Such a system could theoretically employ blockchain technology to improve its authenticity, but the value of the records as a trustworthy memory of land rights needs both the trust of a reliable record and the trustless preservation of the blockchain.

Personal Property

Personal property is "any moveable or intangible thing that is subject to ownership and not classified as real property" (Garner, 2001, p. 988). Similarly to real property, the breadth of laws and regulations concerning personal property is such as prohibit a deep dive into any one aspect within the scope of this paper; personal property entails planes, trains, automobiles…almost everything including the kitchen sink. This breadth, however, makes personal property the ideal property type for blockchain experimentation.

In the realm of personal property, one sees the best illustration of Bell and Parchomovsky's primary contention regarding property title: "the value of title to property rights vitally depends on the degree to which it is known by people in the world, including the property owner" (2016, p. 241). In a sense, this is a very old proposition; it is not by accident that the blockchain is regularly compared to traditional public registries. As discussed *supra,* much of the strength of the blockchain is the extreme difficulty in changing it because of its distributed nature (and, in the case of Bitcoin, its public nature). However, blockchain registries are perhaps more appealing for personal property than for real property. Lemieux presents a valuable "Heuristic for Thinking about the Suitability of Blockchain Solutions for Recordkeeping":

> [This] heuristic [is useful] for thinking about where different Blockchain technology use cases may fall along two important dimensions: record retention requirements and evidential requirements (for which the bar is higher when the loss may be borne by the public as well as by a single individual). Use cases wherein the retention requirements are short and the evidential requirements are low may be most suited to use of Blockchain-based solutions, while those with longer retention requirements and higher

evidential requirements may be least well-suited. This does not take into consideration that new designs may mitigate some of the risks identified, making even use cases that now appear less well-suited more viable in future.

Retention Requirements **H**

Evidential Requirements **L**

Securities trades between private parties	Least suitable: Land transfers between private parties
Most suitable: Low value money transfers between private parties	High value money transfers between private parties

In the case of personal property, especially lower value personal property (such as bicycles on a university campus), both the retention and evidentiary requirements are lower than those for land records. While the need is perhaps not as urgent for personal property registries as for land registries in developing nations, they represent a more fertile ground for experimentation, one which is more closely aligned with what blockchain is best suited to do.

Intellectual Property

Finally, intellectual property, the least material of the broad categories of property, is "a category of intangible rights protecting commercially valuable products of the human intellect. The category comprises primarily trademark, copyright, and patent rights, but also includes trade-secret rights, publicity rights, moral rights, and rights against unfair competition" (Garner, 2001, p. 649).
Nick Vogel argues that "copyrights will have less legal effect in the realm of a decentralized Internet" (2015, p. 137), a realm that the blockchain helps make more likely. This is because it will be impossible to identify (and therefore to sue) the infringing party on the blockchain. However, the blockchain offers the opposite opportunity as well: for rights management to be on the blockchain, making it impossible to override on a whim. Indeed, one could imagine the blockchain being used with the Internet of Things to enforce and protect various rights, such as only letting a rightful owner use an item.

"Smart Contracts" and Contract Law

Contract law is an incredibly rich area of law, with immense amounts of history, statutory law, and common law at play within it. Even the word "contract" conceives of a number of different, yet related things:

> 1. An agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law <a binding contract>. 2. The writing that sets forth such an agreement […]. 3. Loosely, an unenforceable agreement between two or more parties to do or not do a thing or set of things; a compact […]. 4. A promise or set of promises by a party to a transaction, enforceable or otherwise recognizable at law; the writing expressing that promise or set of promises […]. 5. Broadly, any legal duty or set of duties not imposed by the law of tort; esp., a duty created by a decree or declaration of a court […]. 6. The body of law dealing with agreements and exchange <the general theory of contract>. 7. The terms of an agreement, or any particular term (Garner, 2001, p. 259).

It's important to understand how extensive the scope of "contract" and "contract law" is, because it provides context for evaluating the potential risks and benefits of blockchain-based "smart contracts." Smart contracts are "automated programs that transfer digital assets within the block-chain upon certain triggering conditions" (Fairfield, 2014, p. 38).
An excellent example of the idealized idea of "smart contracts" comes from EtherScripter, an Ethereum-based smart contract-generation platform: "Agreements are ambiguous. And enforcement is hard. Ethereum solves both these problems. It does this with the marriage of two special ingredients: a digital currency and a

complete programming language." Although this author finds it a step too far to assert that the problems are "solved," blockchain-based smart contracts do have the potential to streamline both drafting and enforcement of contracts. However, smart contracts are not a panacea; many of the current problems with contracts – ambiguous terms, unforeseen circumstances, material fraud, unconscionable clauses – will continue to exist in a smart contract world.

Drafting, Specific Performance and Equitable Principles

Smart contracts pose two major changes to the drafting of contracts. The first, and less revolutionary, will likely be the need to incorporate coding into drafting, creating standardized code for common terms and training lawyers to utilize the new tools of the trade. More significant is the potential impact upon the balance of power between online merchants and consumers. As Fairfield argues, the necessity of intermediaries to facilitate online transactions has left consumers with only two options vis a vis online offerings: accept or decline. (2014, p. 37). If, as Fairfield argues, blockchain based smart contracts truly permit disintermediated transactions, "then they can begin to make disintermediated contractual arrangements" (2014, p. 41). Fairfield envisions blockchain permitting a system of online contracting wherein "consumers can express their preferences to automated agents (often termed "bots" or "robots," despite the agents' lack of physicality), and then expect their preferences to be enforced" (Fairfield, 2014, p. 44). In many ways, smart contracts offer the possibility of negotiated terms – as opposed to boilerplate – becoming the standard again.

Where this author departs from Fairfield is his assertion that, "if consumers can hold money without banks, they can enforce contracts without courts" (Fairfield, 2014, p. 41). Similarly, Hinkes envisions "a world where specific performance of contracts is no longer a cause of action because the contracts themselves automatically execute the agreement of the parties" (2014). At a simple, transactional level, this is correct: a smart contract can execute independently, automatically moving digital assets from one party to another upon the occurrence of a trigger condition. This, however, does not translate to the end of the courts' role in contract enforcement. For example, if two parties contract to exchange a piece of art for a certain amount of ether, but the wrong artwork is due to error at the warehouse, there is still a cause for specific performance. Similarly, equitable principles cannot be eliminated from contract law simply by using smart contracts; it is as possible for one party to negotiate in bad faith on the block chain as by mail or telephone, and such a case will still require remedy. Adrian Myers perhaps put it best: "We can write bad code just like we can write bad contracts and, when that happens, we need those fusty old courts to save us" (2016).

"Smart Probate": Trusts and Estates

"Smart wills" or "smart probate" would operate, technically, in much the same way as a smart contract. Once a pre-establish variable occurred (typically, the testator(s) death(s), although for a smart trust, conditions such as a beneficiary coming of age could be imagined), the will would then execute, transferring the testator(s)'s estate according to the terms contained therein. Theoretically, this could streamline the probate process significantly, reducing the work upon (or even eliminating the need for) an executor, and reducing will contests by making the testator(s)'s intentions unambigious and verifiable (there could be no backdating of a codicil on the blockchain, for example). However, these outcomes are far from guaranteed.

Gary Howard, elaborating on a quote from Eric Dixon, legal counsel to Blockchain Technology Corp., states the value and challenge of blockchain for probate well:

> The blockchain cannot eliminate [...legal challenges to a will] or the factual basis for them," says Dixon. That is important because a common attack on the smart contract concept is premised on the fear that technology (through the blockchain) would remove a person's 'due process right' to have his or her day in court. "What the blockchain can do," continued Dixon, "is make it much easier for a genuine will

> to be upheld, for a bogus challenge to be dismissed, and for courts to come to factual findings much more quickly" (Howard, 2015).

The legal challenges that cannot be eliminated include challenges to the capacity of the testator, claims that the testator was under duress, and even ambiguous terms. Particularly as smart wills and trusts are being created, standardized forms and code will have to be developed through literal trial and error. Much as with smart contracts, the benefits of blockchain wills are less likely to be wholly revolutionary, and more likely to consist of improvements in efficiency and execution within the extent system.

Evidence

"Evidence" is the heart of the relationship between law and archival science; the principals of archival science have largely evolved to preserve the evidentiary character of records. Evidence is also a particularly large area of law; this is natural, given that the evidence admitted determines the "facts" upon which a case is determined. The rules of evidence also vary, not just from jurisdiction to jurisdiction, but from tribunal to tribunal; in Canada and the U.S., local, provincial, and federal rules of evidence determine the admissibility of a particular piece of evidence. Given the complexity and breadth of this legal area, it is only within the scope of this paper to discuss the potential impacts of blockchain at the most general of levels.

Blockchain records would fall within the broader category of "electronic evidence." "Electronic evidence" is a contentious category; even its definition remains open to debate and discussion. In attempting to come up with a sufficiently broad definition to include future, as yet uncreated forms of electronic evidence (such as "wet computing" or even the blockchain), Schafer and Mason, key in on three primary elements:

> Electronic evidence [is] data (comprising the output of analogue devices or data in digital format) that is manipulated, stored, or communicated by any man-made device, computer, or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be with the evidence (2012, p. 27).

Blockchain records, then, are clearly within the boundaries of "electronic evidence," and could well be admissible as such, subject, of course, to the law and requirements of the particular tribunal. Indeed, depending on how broadly "financial institution" is interpreted, it's possible that blockchain records could be not just automatically admissible, but even *prima facie* proof of the matters contained therein under the Canada Evidence Act[4]:

> Subject to this section, a copy of any entry in any book or record kept in any financial institution shall in all legal proceedings be admitted in evidence as proof, in the absence of evidence to the contrary, of the entry and of the matters, transactions and accounts therein recorded (Canada Evidence Act, R.S.C., 195, c. C-5, §29(1)).

Admissibility of blockchain records will largely depend upon the approach of courts and legislatures, however, this author would argue that blockchain records – particularly records such as smart contracts where the record itself is hashed to the blockchain – are more comparable to traditional paper records than to electronic records. One of the major challenges regarding electronic records as evidence is that "[i[t is a fact established by research and experience that we cannot preserve electronic records, but only our capacity to reproduce them time after time."[5] (The blockchain, however, offers the possibility of inviolable – as opposed to merely

[4] It should be noted that such records must have been kept in the ordinary and usual course of business.

[5] Sheppard, Duranti, & Rogers, 2010, p. 98).

reproducible – electronic records; blockchain records could, theoretically, move the evidentiary ball into a space wherein electronic records can be governed with a degree of ease under the existing evidentiary regime. However, little research has been generated on this subject; the evidentiary character and admissibility of blockchain records will have to be examined in greater depth by evidence specialists.

Conclusion

Ultimately, blockchain technology offers a new, innovative way to assure the ongoing authenticity and accuracy of digital records with a plethora of legal meanings and uses. However, it is not a panacea that will move us into a world beyond trust. Public, permissionless blockchain registries could well function like the public registries in Continental Europe – by providing a publicly visible, immutable record of the records, the blockchain could allow greater certainty regarding legal rights and quicker resolution of disputes. However, a registry is only as good as its underlying records. The presence of a clerk or even an archivist cannot guarantee that forgeries or other unreliable records have not been placed in the register; the blockchain, in and of itself, cannot ensure that smart contracts, probate, mortgages and other records are reliable.

Ultimately, blockchain records, like all records, are only as trustworthy as their creator. Thus, the idea of a "trustless" system is misleading when it comes to blockchain applications beyond cryptocurrency. While blockchain technology could be used to ensure the authenticity and even execution of a diversity of legal documents, those documents – and their parties – remain accountable to the legal system. Contracts that have executed can nonetheless be voided, and parties made whole. Furthermore, there is no one monolithic "legal system," and therefore no one regulatory approach to blockchain. Different jurisdictions approach property, contracts, and evidence differently, and there is no reason that would not be true of jurisdictions' approach to the blockchain. Ultimately, even if blockchain serves to disrupt how legal acts are performed, they will still be performed in trust that legal systems – and not just the blockchain – will protect peoples' rights and mediate disputes. This trust is the foundational element that lets us experiment with trustless disruption.

References

Allison, I. (2016, April 18). Barclays' Smart Contract Templates stars in first ever public demo of R3's Corda platform. *International Business Times*.

Allison, I. (2016, July 11). Blockchain-powered real estate platform Ubitquity records first property ownership transfer on the Bitcoin public ledger. *International Business Times.* Retrieved on October 8, 2016 from http://www.ibtimes.co.uk/blockchain-powered-real-estate-platform-ubitquity-does-first-property-ownership-transfer-bitcoin-1569980

Baker, Edward D. (2015). "Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange." *Southwestern Law Review* 45: 341–433.

Bell, Abraham, and Gideon Parchomovsky. (2016). "OF PROPERTY AND INFORMATION." *Columbia Law Review* 116, no. 1: 237-286.

Canada, Government of. Standing Senate Committee on Banking, Trade and Finance. (2015). "Digital Currency: You Can't Flip This Coin!" Retrieved from http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf

Canada Evidence Act. (R.S.C., 195, c. C-5)

Chang, Joyce L.T. (2014). "The Dark Cloud of Convenience: How the New HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Information." *Loyola of Los Angeles Entertainment Law Review* 34: 119. doi:10.1525/sp.2007.54.1.23.

Cross, Frank B. (2004). "Law and Trust." *Geo. Law Journal* 93: 1458–1545. doi:10.1525/sp.2007.54.1.23.
Dewey, Joe, and Shawn Amuial. (25 June 2015). "Blockchain Technology Will Transform the Practice of Law." *Bloomberg Law*. Retrieved from https://bol.bna.com/blockchain-technology-will-transform-the-practice-of-law/
Erlandson, McKillop Bradford. (2014). "Revisiting Progressive Federalism: Voice, Exit, and Endless Money." *U. Miami L. Rev* 68: 853. doi:10.1525/sp.2007.54.1.23.
Fairfield, Joshua. (2014). "Smart contracts, Bitcoin bots, and consumer protection." *Wash. & Lee L. Rev. Online* 71 35-299.
Higgins, Stan. (22 April 2016). "Republic of Georgia to Develop Blockchain Land Registry." *CoinDesk*. Retrieved from http://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry/
Hinkes, Andrew. (29 July 2014). "Blockchain, smart contracts, and the death of specific performance." *InsideCounsel Magazine*. Retrieved from http://www.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci?slreturn=1464801770
Garner, B. A. (2001). *A dictionary of modern legal usage*. Oxford University Press, USA.
Gottehrer, Gail. (2015). "'Connected' Discovery: What the Ubiuity of Digital Evidence Means for Lawyers and Litigation." *Rich. J.L. & Tech.* 22 (3). doi:10.1525/sp.2007.54.1.23.
Gruber, Sarah. (2014). "Trust, Identity, and Disclosure:" *Quinnipiac Law Review* 32 (1): 135–208. doi:10.1525/sp.2007.54.1.23.
Johnson, Don. (25 April 2016). "More on the Law of the Blockchain." *The Spotlight: Media, Sports, and Communication Law Blog*. Retrieved from http://thespotlight.ca/index.php/more-on-the-law-of-the-blockchain/
Karch, Gregory M. (2014). "Bitcoin, The Law and Emerging Public Policy: Towards a 21st Century Regulatory Scheme." *Fla. A&M U.L. Rev.* 10: 1–52. doi:10.1525/sp.2007.54.1.23.
Law Society of Upper Canada, The. (2015). *Practice Guidelines for Electronic Registration of Title Documents*. Retrieved from https://www.lsuc.on.ca/with.aspx?id=2147501945#PRACTICE_GUIDELINE_6
Lemieux, Victoria Louise. (2016). "Trusting Records: Is Blockchain Technology the Answer?." *Records Management Journal* 26, no. 2.
Mandjee, Tara. (2014). "Bitcoin, Its Legal Classification and Its Regulatory Framework." *Journal of Business & Securities Law* 15: 1. doi:10.1525/sp.2007.54.1.23.
Marshall, Russ. (2015). "Bitcoin : Where Two Worlds Collide." *Bond L. Rev.* 27: 89–112.
Mizrahi, Avi. (3 March 2016). "Factom CEO: Blockchain-based Transparent Mortgages Can Restore Trust in Markets." *Finance Magnates*. Retrieved from http://www.financemagnates.com/cryptocurrency/interview-2/factom-ceo-blockchain-based-transparent-mortgages-can-restore-trust-in-markets/
Mosson, G. H. (2012). Robosigning Foreclosures: How It Violates Law, Must Be Stopped, and Why Mortgage Law Reform Is Needed to Ensure the Certainty and Values of Real Property. *W. St UL Rev.*, *40*, 31.
Myers, Adrian. (1 July 2016). "When smart contracts are not so smart." *The Globe and Mail*.
Noonan, Aubrey K. (2014). "Bitcoin or Bust: Can One Really Trust One's Digital Assets." *Est. Plan. & Cmty. Prop. LJ* 7: 583.
Ponsford, Matthew. (2015). "A Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States." *Hong Kong Journal of Legal Studies* 9: 29. doi:10.1525/sp.2007.54.1.23.
Raskin, Max I. (2015). "Realm of the Coin: Bitcoin and Civil Procedure." *Fordham Journal of Corporate & Financial Law* 20 (4): 969–1011. Retrieved from http://0-search.proquest.com.innopac.up.ac.za/abicomplete/docview/1698197371/D473299919644AE6PQ/2?accountid=14717.
Rizzo, Pete. (26 December 2015). "Blockchain Land Title Project Stalls in Honduras." *CoinDesk*. Retrieved from http://www.coindesk.com/debate-factom-land-title-honduras/
Shcherbak, Sergii. (2014) "How Should Bitcoin Be Regulated?" *Eur. J. Legal Stud.* 7: 41. doi:10.1525/sp.2007.54.1.23.
Sorrell, William H., Attorney General, and Vermont Office of Attorney General. (2016) *Blockchain Technology:*

Opportunities and Risks.
Stancic, H. (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.
Vigna, Paul. (1 May 2016). "Delaware Considers Using Blockchain Technology." *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/delaware-considers-using-blockchain-technology-1462145802
Vogel, Nick. (2015). "Great Decentralization: How Web 3.0 Will Weaken Copyrights, The." *John Marshall Review of Intellectual Property Law* 15(1): 136-149.
Walch, Angela. (2015). "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk." *New York University Journal of Legislation & Public Policy* 18: 837–94.
Zyskind, Guy, and Alex Sandy Pentland. (2015). "Decentralizing Privacy : Using Blockchain to Protect Personal Data." doi:10.1109/SPW.2015.27.

Blockchain Technology for Recordkeeping

Blockchain for Recordkeeping: An Overview of Use Cases

A Background Paper "Blockchain Technology for Recordkeeping – Help or Hype?" a SSHRC Knowledge Synthesis Grant Study on "How can emerging technologies be leveraged to benefit Canadians?"

Prepared by: Victor Liang, Masters of Archival science and Library Information Studies Student for Principal Investigator Dr. Victoria L. Lemieux

The University of British Columbia, Vancouver, BC, V6T 1Z1
Phone: 604 822 2404
E-Mail: vlemieux@mail.ubc.ca

Table of Contents

INTRODUCTION **47**
GENERAL OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND RECORDKEEPING IMPLICATIONS **48**
RECORDKEEPING USE CASES **48**
A. ALTERNATIVES TO THE BITCOIN BLOCKCHAIN **49**
B. SMART CONTRACT USE CASES **50**
C. TIMESTAMPING USE CASES **51**
D. PROVENANCE USE CASES **52**
BENEFITS **53**
CHALLENGES **53**
REFERENCES **56**

Introduction

Blockchain technology was born out of the Bitcoin movement and has grown to become a platform with "the potential for unleashing countless new applications and as yet unrealized capabilities [—of which bitcoin currency is only the first—] that have the potential to transform everything" (Tapscott & Tapscott, 2016, p. 6). By surveying the techno landscape this paper explores some of these capabilities in terms of recordkeeping related use cases of blockchain technology. Business and financial experts Don and Alex Tapscott state that

blockchain technology has "spread like wildfire to businesses, governments, privacy advocates, social development activists, media theorists, and journalists, to name a few, everywhere"(p. 5). The impact on record keeping, according to the Tapscotts, is widespread: "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, votes, provenance of food, and anything else that can be expressed in code" (p. 7).

General Overview of Blockchain Technology and Recordkeeping Implications

Since blockchain's early days, when it started off as the structural foundation for the cryptocurrency Bitcoin, blockchain applications have grown immensely in a short time, and have expanded into different sectors and industries. Most of us are familiar with Bitcoin, the cryptocurrency created by (the pseudonymous) Satoshi Nakamoto in 2009, and that operates through a decentralized peer-to-peer network that is powered by its users without a central authority ("What is Bitcoin?" n.d.). Because of the lack of a central authority to monitor, protect and verify transactions, Bitcoin operates on a network sharing a public ledger called the blockchain, containing every Bitcoin transaction ever processed, allowing a user's computer to verify the validity of each transaction, which is how the whole system, generally speaking, maintains trust amongst users ("What is Bitcoin?" n.d.). Verification of new transactions to the blockchain is achieved through a Proof-of-Work system ("POW"), involving mining computers who compete to solve a complex set of algorithms, and upon completion broadcast their results to the rest of the miners who will then confirm that the result is correct. When a majority has been reached, the confirmed block of information is cryptographically sealed and added to the blockchain. The incentive for the miners come in the form bitcoins that are awarded to "winning" miners (*"Israel: A Hotspot,"* 2016, p. 7).

Ensuring the trustworthiness of records becomes even more important and complicated as records are increasingly being created, transferred, and stored digitally. According to Sheppard and Duranti (2010), digital records "are different from traditional analogue records in many ways . . . [they] can be more volatile and transitory, and easier to alter or replicate, but more difficult to obliterate" (p. 9). They also add that "[d]igital technology is subject to a rapidly increasing rate of obsolescence and this has implications for the long-term retention, preservation and accessibility of digital material" (p. 9). Because of these issues with digital records, long-term preservation of authentic digital records needs to address technical dangers, including "rapid changes to software, hardware, network links to related information, and failure to capture or loss of semantic information. That said, the problem of long-term preservation is not just a technical issue. There are also organizational, legal, industrial, scientific and cultural issues to be considered in protecting records over the long-term" (Lemieux, 2016, p. 4).

In this regard, many industry experts argue that the structure of blockchain technology and the way it works makes it an attractive technology for managing and storing digital records, and solving recordkeeping problems. The next section will examine some of the blockchain use cases and work being done around recordkeeping.

Recordkeeping Use Cases

Cryptocurrency and the process for making payments with it can be thought of as just the first application built on a blockchain system, with new protocols being built on top of the foundational technology that could lead to easy-to-use consumer products and services. The companies and use cases described below show that the type of products and services would be anything that would benefit from having information stored in a

decentralized, unchangeable database that is accessible from anywhere at any time (Orcutt, 2015). It is these features that have made blockchain technology attractive for recordkeeping solutions. This sentiment is echoed by those in the recordkeeping industry, such as digital archivist and recordkeeping professional Cassie Findlay (2015), who states that "Bitcoin is just one application utilising the infrastructure of the blockchain. In recent times developers have started to use blockchain in new ways that sound very familiar to those of us working in recordkeeping - building applications for keeping trusted records in a neutral, decentralised environment" (para. 12). Findlay goes on to describe the blockchain in the context of recordkeeping:

> A decentralised archive utilising the blockchain as a storage mechanism 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. (para. 13)

Ever since Bitcoin came onto the scene, the expansion of the Bitcoin blockchain and blockchain applications have grown immensely and is constantly shifting. Keeping this in mind, it is difficult to capture all of the companies doing work in this area. Hence, the list of companies and use cases in the Appendix is a non-exhaustive one, but should provide an idea of the general technoscape. As the list shows, almost half of the work is being done in North America, with the rest spread out over Europe and Australia. Bitcoin and Ethereum are the preferred blockchain platforms, with companies looking to create applications that can function across different platforms, but a lot of companies are also developing their own permissioned/private platforms for their own specific purposes, especially those working in the financial services industry. The following companies and use cases described below are a few of the more notable ones doing work in this regard, and that exemplify crucial recordkeeping mechanisms services on blockchains. The descriptions are broad and largely based on claims by the companies - with a discussion of the strengths and weaknesses in the following section. They have been grouped into categories where blockchain technology could potentially have the greatest effect on recordkeeping, beginning with a discussion of . Please see the Appendix to this paper for a list of other companies leveraging blockchain technology for recordkeeping solutions.

A. Alternatives to the Bitcoin Blockchain

The Bitcoin blockchain is not the only blockchain network available; as the technology has grown in popularity, so have alternatives to the Bitcoin blockchain with the possibilities of creating and running more accessible, wider-reaching, and industry-specific applications than are possible on the Bitcoin blockchain. While there are many, I will describe two of the bigger platforms, *Ripple* and *Ethereum*.

Ripple is a popular US fintech blockchain platform that was founded in 2012 and focuses on providing permissioned/private network solutions to financial institutions, who may not find the transparency and public nature of the Bitcoin blockchain attractive or suitable for its business model, especially where privacy is crucial to business operations (Rizzo, 2016). Case in point, Ripple is currently working with numerous leading global banks, including RBC, CIBC, Santander, UniCredit, and UBS. Ripple uses the distributed ledger technology of blockchain to enable simpler and faster cross-border payments between financial institutions. Unlike a public blockchain, the Ripple ledger contains the current state of the network as opposed to a chain of historical events with the nodes in Ripple jointly constructing an update to the ledger as their consensus mechanism (Bains, 2015).

Of note here is that "Blockchains created by banks, even a consortium of banks, are likely to fall under regulations similar to the ones that already apply to the traditional financial system. The existence of these

regulations have implications for these blockchains as completely immutable ledgers" (Torpey, 2016, n.p.). On the other hand, consensus is determined by a set of chosen validators, unlike the open consensus in POW, hence, there are often few nodes with high trust levels making for much faster transaction speeds than in a public blockchain (Parker, 2016).

Ethereum is arguably the biggest name and most used after Bitcoin as far as public blockchain platforms. Ethereum had its beginnings in the mind of Russian-Canadian cryptocurrency researcher and programmer Vitalik Buterin, who before the age of 20, had already begun work on what is now Ethereum. Development of Ethereum began in 2013 and went live in 2015, with funding initially coming from crowdsourcing (Caffyn, 2015). Ethereum is now run by the Ethereum Foundation, a Swiss nonprofit, which is made up of an advisory board and special advisors, including Buterin ("About the Ethereum Foundation," n.d.).

Essentially, Ethereum is a public blockchain that allows developers to easily deploy decentralized applications. What is notable about the Ethereum blockchain is that it offers more flexibility than the Bitcoin blockchain in terms of the applications that can run on it. This is because the Ethereum blockchain's programming language is Turing complete, meaning it is a system "in which a program can be written to find an answer - or to execute a smart contract that can buy something, sell something, or do something," while the Bitcoin blockchain scripting language is more restrictive, limited, and less user-friendly (Pangburn, 2015, para. 5). Ethereum is currently transitioning Proof-of-Stake system ("POS") to verify blocks and reach consensus. In brief, POS is an alternative to POW, that also attempts to provide consensus and prevention of doublespending, but focuses on the stake one has in validating transactions; in other words, this method of validation requires holders of Ether, the cryptocurrency used by Ethereum, to prove how much they hold and that determines how much they can "mine". For example, a person owning 5% of Ether can mine 5% of the blocks (Graydon, 2014). Because of the immense real-world computational energy required by POW, there's an incentive to centralize hashing power, which defeats the purpose of decentralized network; while POS does not require this level of energy output, instead, using coins as collateral to validate blocks.

According to its website, Ethereum is a "decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference" ("Ethereum Project," n.d., n.p.). What is important here is that smart contracts supported by a Turing complete platform can lead to decentralized autonomous organizations, which are entire companies run without human managerial interactivity (Buterin, 2014). Smart contracts is the category that will be discussed next.

B. Smart Contract Use Cases

Smart contracts are computer protocols that embed the terms and conditions of a contract as source code that are compiled into executable computer code that can run on a network, thus, many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing or both, making contractual processes more efficient and faster. 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 a database that cannot be forged or tampered with (von Haller Gronbaek, 2016). With blockchain-based smart contracts there is no longer a need for a third party for recordkeeping or enforcement, and should, technically, eliminate ambiguity.

One of the biggest companies in the field of smart contracts is the DAO, an open-source investor-directed venture capital fund application running on top of the Ethereum blockchain that was developed by German programmer, Christoph Jentzsch, and was launched in 2016. Many industry experts and observers, as well as

the mainstream media, have had difficulty to fully describe what it is that the DAO does or offers, although, it has generated a lot of excitement and has managed to raise over $150 million from investors through crowdfunding, making it the most successful crowdfunded venture ever - this popularity also speaks to the attractiveness of POS because users actually have a stake in the system (Popper, 2015). One way of describing the DAO and what it does is that it is a collection of Ethereum-based smart contracts that, when taken collectively, amount to a series of by-laws and other founding documents that determine how its constituency - anyone who has bought DAO tokens with ethers - votes on decisions, allocates resources, and, thereby, creates a return on investment from the projects the DAO helps fund (del Castillo). Unlike a traditional company that has a designated managerial structure, the DAO is run and owned by everyone who has purchased a DAO token, although, on top of this structure exists a group of Curators who are there to provide a failsafe mechanism and security from attacks and fraud. The Curators do not add centralization to the DAO, as they are nominated by investors and can be fired at any time, for any reason ("The DAO - Curator," n.d.).

One of the challenges facing the DAO, and any stateless decentralized autonomous organization for that matter, is the question of its legal and regulatory status. In his white paper on the DAO, Jentzsch, who worked previously as the lead tester at Ethereum, addresses this concern and warns that anyone using the DAO code does so at their own risk: "the legal status of DAOs remains the subject of active and vigorous debate and discussion. Not everyone shares the same definition. Some have said that they are autonomous code and can operate independently of legal systems; others have said that they must be owned or operated by humans or human created entities. There will be many uses cases, and the DAO code will develop over time. Ultimately, how a DAO functions and its legal status will depend on many factors, including how DAO code is used, where it is used, and who uses it" (Jentzsch, 2016, p. 1). The latter speaks to another major issue with smart contracts, and contracts in general, that being the human factor in creating and using the code, which is something that will be explored further when discussing the 2016 hack of the DAO in the section looking at challenges with these use cases.

C. Timestamping Use Cases

Timestamping is the process of securely keeping track of the creation and modification time of a document, allowing vested parties to know with certainty that a document existed at a particular date and time. Timestamping is a business tool seemingly well-suited for blockchain technology because by design a blockchain transaction includes date and time that is secured by the blockchain through a hash that can later certify the existence of data (Parker, "Timestamping" 2015, n.p.). This recordkeeping functionality has a wide range of uses - especially, in cases where trust between parties may be an issue including establishing copyright and registering land - which is enhanced by the decentralized and tamper-proof solution of blockchain technology. There are numerous blockchain companies doing work in this area of which I will discuss two companies that utilize hashes secured in the blockchain for timestamping but with slightly different approaches: *Factom* and *Enigio Time*.

Factom was developed in 2014 by the Texas Bitcoin Conference founder Paul Snow, investment and tech specialists Peter Kirby and David Johnston, all of whom still run Factom. Factom is an open-source distributed, decentralized protocol running on top of the Bitcoin blockchain that collects, packages, and secures data into the Bitcoin blockchain through hashes and a network of Federated servers, whom delegate responsibility in the system, Notably, no "single server is ever in control of the whole system, and no server is permanently in control of any part of the system; the responsibility for each part of the system cycles among the servers each minute" (Bitcoinist.net, 2015, n.p.).

Factom is about proof of publication, proof of process, and proof of audit ("Factom - FAQs," n.d.). Factom publishes a hash of a document, or a digital fingerprint of a document, which lets you validate and verify a document without revealing any private information. This hash is then secured into the Bitcoin Blockchain

where it remains immutable. To reiterate an earlier point, obviously, these hashes are not the actual records themselves, and the hashes are only used to authenticate the original records, but only if those originals have been exactly preserved so as to produce the same hashes as on the blockchain, since a blockchain hash cannot be reverse engineered (Lemieux, 2016, p. 15). As stated in their white paper, Factom does not validate entries, meaning, and this is an important point to be made with regards to timestamping in the blockchain context, their platform is essentially a database that merely streamlines the auditing process.

Enigio was developed in Sweden in 2012 by Göran Almgren, Mats Stengård and Hans Almgren, who also form the Enigio management team. Enigio delivers solutions for qualified electronic time stamping, traceability and E-archives, functioning as a "modern digital notary service, a seal for documents of the twenty-first century" and supporting records management standards RFC 3161 and ISO/IEC 18014 ("About Enigio Time," n.d., n.p.). Enigio has created their own blockchain, which functions as, they describe, as a Blockchain Aggregator, and that references the Bitcoin blockchain, other blockchains, and published data. The specific advantages to this include easy and low cost access to the advantages of the Bitcoin blockchain; several channels and references; more precise proof; easier to verify proof; and continuously validating the chain of proof and alert if integrity is compromised ("Blockchain Technology," 2016).

Enigio's Integrated time:stamp application works by creating a unique digital fingerprint for a document as a proof of existence. The digital fingerprint is then sent to Enigio's servers where a secure time stamp is created. Of significance, and in contrast to the Factom protocol, this proof is generated by equations that bind the document's timestamp with a number of public reliable sources - Twitter, Youtube, popular blog platforms, news sites and newspapers - and published codes which essentially make it impossible to manipulate, and that can be accessed on the Enigio website at any time for verification purposes (Almgren, 2016). These processes guarantee that records have not been manipulated, thus, helping to ensure trustworthiness.

D. Provenance Use Cases

Provenance is another interesting recordkeeping category where blockchain technology may be highly suitable. When one considers the touted characteristics of blockchain technology, this will quickly become apparent. Founder and CEO of Coin Sciences, Gideon Greenspan (2016), 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" (Greenspan, 2016, n.p.). 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" and blockchains, by their nature, can serve as the infrastructure for registering and authenticating asset ownership between untrusting parties with common interests.

One UK company that has been in the news a lot in this regard is Everledger, who is using blockchain technology to help the insurance industry solve diamond theft and fraud. Founded in 2015 by Leanne Kemp, Everledger uses the Bitcoin blockchain as a platform for creating a permanent ledger registry for diamond certification and related transaction history, which helps insurance companies, law enforcement and other interested parties to verify ownership. In conjunction with certified diamond laboratories 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, reveal their origin, trail of ownership, the processes they might have undergone" (Patel, 2015, n.p.). Everledger and similar provenance use cases offers a more robust and accessible solution than traditional paper certificates and receipts, which are more readily compromised.

Benefits

Bitcoin introduced trust through computation of mathematical algorithms that everyone can have access to, creating a context where you trust no one and have open dealing to address this lack of trust - in contrast to traditional trust systems, such as a bank and wherever a centralized intermediary is present to manage and oversee transactions, thereby creating a context where access is restricted and limited and trust is given only to those who have access. In a Deloitte report on blockchain technology, various benefits were identified including the following with potential consequences for recordkeeping: users are in control of all of their information and transactions; blockchain data is complete, consistent, timely, accurate, and widely available; due to the decentralized networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks; users can trust that transactions will be executed exactly as the protocol commands removing the need for a trusted third party; changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are immutable; blockchains use a single public ledger, thus reducing clutter and complications of multiple ledgers (Boersma, n.d.).

According to Findlay (2015), blockchain technology "potentially offers a means for society - or at least groups within society - to keep their own records with some assurance about inviolobility and longevity that was not possible before. This has huge ramifications in terms of the ability to guard against censorship of information that is damaging to the powerful" (para. 14). As well, blockchain can also be an authenticating mechanism through "trust by computation": instead of using a central authority, the proof of a document's veracity can be asserted via distributed cryptographic confirmation (para. 16).

These benefits of blockchain technology are exemplified in the use cases described above. In the case of the DAO and their use of smart contracts: blockchain technology gives relationships and obligations operating under smart contracts the security provided by blockchain technology and also the increase in verifiability and certainty that comes with distributed technology (Eris Explainer, "What are Smart Contracts?" n.d.). As mentioned, smart contracts are essentially software scripts like any other software script but because of its connection to the blockchain it has certainty, or, in other words, smart contracts on the blockchain are "applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third party interference" (Thompson, 2016, n.p.) Although, as will be discussed below, the benefits of blockchain-based smart contracts can also create issues, in particular, if the code is written in such a way that a smart contract can be exploited or attacked as in the case of the DAO hack.

Factom's blockchain anchoring approach to recordkeeping utilizes the benefits of blockchain ledger technology by recording hashes of data in the Bitcoin blockchain that are permanent and timestamped, thus cryptographically proving data came in at a certain time. Once secured in the blockchain, these records are now subject to the Bitcoin blockchain's immutability stemming from its Proof-of-Work and distributed consensus mechanisms. Furthermore, if the Factom protocol were to disappear, its data can be validated as long the user has a copy of their data, and has access to the Bitcoin blockchain (Factom FAQs). Enigio Time's timestamping service also uses blockchain technology in the same manner to provide immutable digital proof that data existed at a particular time, but take it a step further by utilizing other reference sources outside of the blockchain for publishing timestamped hashes, such as Twitter, Youtube, popular blogs, and other public feeds (Almgren, 2016). Everledger's use of the public Bitcoin blockchain allows it to openly track certified diamonds, recorded on the blockchain, as they change hands, helping to reduce insurance fraud and increase the value of diamonds, in this sense, the blockchain functions as an uncontested space from which the authenticity and history of the diamonds can be openly accessed at any time.

Challenges

Despite all of the noted benefits and overall euphoria around blockchain technology and its promises, one has to keep in mind that it is still a nascent technology, and with that comes numerous challenges and issues. As

much as the benefits of blockchain technology have been documented and touted, there are substantial drawbacks to blockchain technology that need to be addressed before blockchain technology can be fully trusted and employed en masse.

For recordkeeping purposes, it is important to understand what the Bitcoin blockchain and other similar blockchains do not do. Information Management Specialist Vicki Lemieux describes three key points here: first, original records are not stored on the blockchain, only hashes of original records (this is important when considering applications like Factom and Enigio Time, which operate in this manner); second, it is not possible to reproduce an original record from a hash stored on a blockchain; and third, and most significantly, blockchains do not ensure the trustworthiness of records, as blockchain solutions do not address the reliability of records (Lemieux, 2016, p. 10). These three points are important to keep in mind when considering the challenges and drawbacks to the use cases, claims made by the companies, and the hype around blockchain technology.

Furthermore, there are other concerns that may make blockchain technology not feasible for recordkeeping, such as it being a nascent technology with technical limitations (transaction speed, verification process, and data limits) that limits its wide applicability; uncertain regulatory and legal status; POW's large energy consumption; control, security, and privacy; integration with existing systems; and a cultural shift to a decentralized network (Boersma, n.d.).

Looking at Factom and the DAO as examples, we can see the manifestation of many of the above challenges. The solution offered by Factom, and of any current Blockchain-based solution, as described in this report do not address the issue of records reliability, and because Factom is an open and public system, erroneous and unauthorized entries may be entered upstream, and because Factom does not validate data in any meaningful way beyond timestamping collected data, it is possible that bad records are hashed and secured in the blockchain as if they were honest (Lemieux, 2016, p. 16). While it has been noted that maintaining record integrity is one of the main strengths of blockchain technology, such as Factom's timestamping and Everledger's provenance application, the technology's ability to maintain records' authenticity is still dependant on the susceptibility of the system to faults and security breaches (p. 16). For timestamping, a significant security breach would be related to timing errors and attacks; nodes keeping track of the network time need to be working properly in order to get the correct time, and attackers have the ability to manipulate a node's network time counter by connecting as multiple peer nodes and reporting inaccurate timestamps (p. 17). Another concern that applies to companies like Factom and Everledger and blockchain technology in general are the questions of who controls the blockchain and how long will it survive? To which there are currently no clear answers (p. 17).

The DAO hack that has been alluded to earlier in this paper put a significant damper on the excitement around Ethereum, The DAO, smart contracts, and blockchain technology. As mentioned, smart contracts can, in theory, be fully automated and self-enforcing, and nothing outside of its code can change its transactional rules. Of course, this code is written by humans, and "drafting a contract that takes into account all possible contingencies and states all their responses is not possible" or, at least, extremely difficult (von Haller Gronbaek, 2016, para. 19). By exposing a legal loophole in the contract code, The DAO hacker managed to exploit the contract unilaterally, allowing the hacker to reportedly drain more than 3.6 million ether into a "child DAO" resembling the structure of The DAO (Siegel, 2016). Without going into further details of the hack, what this situation shows is that regardless of the immutability of the blockchain technology supporting smart contracts, they are still not immune from human error that can expose the code to exploitation; the inflexibility of smart contracts can make it very difficult to deal with changing circumstances; the lack of a third party to swiftly and readily intervene; and the existence of smart contracts outside of state regulations and laws, which would have provided some redress in this case for all of the victims. Speaking to the hack, Matt Levine (2016) of Bloomberg View offers a harsh but sobering critique of smart contracts that addresses the tension between blockchain enthusiasts and detractors:

> The most fascinating thing about the DAO hack may be the way it exposes these tensions. To true

believers in smart contracts, there is no problem here. The system is fine; the failures -- writing bad code and not anticipating this attack -- were trivial, mere human error. Next time, write better smart contracts and you'll be fine. To those true believers, changing the code after the fact -- even to conform it to almost-everyone's reasonable expectations about how the DAO would work -- would be a betrayal of the smart-contract ideal. On the other hand, to the humans who read the English descriptions of the DAO and invested their money based on their reasonable expectations, their losses probably *do* seem like a problem. You can't *really* base the financial system of the future on computers rather than humans, on trusting to immutable code no matter what happens. Financial systems are supposed to work for humans. If the code rips off the humans, something has gone wrong. (para. 14)

Conclusion

My high-level overview of the above use cases gives a glimpse into how blockchain technology can be used for recordkeeping. The major interconnection between the companies behind all of these use cases is a philosophical leaning toward decentralization and greater transparency, as evidenced by the popularity of public blockchains over private ones, although, private blockchains are increasingly gaining traction in the financial services industry, as well as the increased usage of hybrid blockchains. Alternative blockchain platforms like Ripple and Ethereum have carved out a niche market, the use cases also show that much of the work being done with blockchain still leverages the Bitcoin protocol, as this remains the most tested and trusted protocol. Despite all of the criticism of the Bitcoin protocol - more restrictive and limited, high energy consumption, slow transaction speed, bloating - a lot of those on the development side seem to share the sentiment that it is still the most reliable and secure permissionless blockchain, at least in terms of the qualities that have made blockchain technology such a popular tool, that being computational security, transparency, and immutability. POW may be inefficient but this is because it uses a lot of resources to reach consensus, making its history highly trustworthy and effectively immutable, giving users more confidence in the data it records (Lopp, 2016). Quite tellingly, we have yet to see an attack the scale of the hack that affected The DAO and Ethereum on the Bitcoin side.

Despite the excitement around Blockchain technology, we need to be cautious about how we use it for recordkeeping. Although companies like Ethereum have developed blockchains expressly for "use as information storage and processing as opposed to ledger blockchains centred around cryptocurrencies, their blockchains are orders of magnitude smaller than bitcoin's. There are strong indications that this is the direction where innovation in blockchains is heading, yet caution and patience are advised until they have proven their reliability and security" (Niccolai, 2015, p. 9). Indeed, as industries are warming to the idea of blockchains, a lot of the alternative blockchains and applications are starting to look like they have a lot less to do with virtual currencies and more about digital record keeping (Thomas, 2016). Still, these issues speak, perhaps, more to the infancy of the technology as opposed to its viability and potential. Going forward, for the purposes of recordkeeping, it is important that records managers and other recordkeeping professionals collaborate with blockchain developers to ensure that the technology is both technologically and legally sound to ensure the security and trustworthiness of records. In this regard, blockchain technology for mainstream adoption is not at the stage yet where we can confidently eliminate centralized human intervention, at least not without further research and extensive real-world testing; as Ivan Niccolai (2015) argues: "The blockchain offers a trustless, distributed approach but is also carries its own set of new risks and cautions. Despite the hype, no cryptographic algorithm can replace sound governance as the trust dilemma, like user identification, has never been a technology problem. Use cases like smart contracts and escrow services must be seen for their value in automation, not as a substitute for legal and commercial due diligence in contract management" (p. 15).

References

"About Enigio Time." (n.d.). Retrieved from https://enigio.com/about-us.

"About the Ethereum Foundation." (n.d.). Retrieved from https://www.ethereum.org/foundation.

Allison, Ian. (February 4, 2016). "Factom Signs Smart City Deal to Roll out Blockchain Verification across China." Retrieved from https://uk.news.yahoo.com/factom-signs-smart-city-deal-212854516.html.

Allison, Ian. (March 3, 2016)."Guardtime Secures over a Million Estonian Healthcare Records on the Blockchain." *Business Times UK*. Retrieved from http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367.

Allison, Ian. (March 10, 2016). "Ubitquity Using Bitcoin Blockchain to Secure Real Estate Titles." Retrieved from

https://uk.news.yahoo.com/ubitquity-using-bitcoin-blockchain-secure-085620221.html.
Almgren, Hans. (n.d.). "Method for creating signals for time-stamping of documents and method for time-stamping of documents." *Google Patents*. Retrieved from https://patents.google.com/patent/WO2015020599A1/en?assignee=Enigio.
Bains, Pavel. (September 16, 2015)."Ripple Versus The Blockchain." *bluzelle*. Retrieved from http://bluzelle.com/ripple-versus-the-blockchain/.
Bitcoinist.net. (June 1, 2015). "The Factom Protocol - A Technical Overview." *Inside Bitcoins*. Retrieved from http://insidebitcoins.com/news/the-factom-protocol-a-technical-overview/32872.
"Blockchain Technology." (n.d). Retrieved from https://enigio.com/blockchainTech
Boersma, Jacob & Bulters, Jeroen. (n.d.). "Blockchain technology: 9 benefits & 7 challenges." *Deloitte*. Retrieved from http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html.
Burke, Scott. (May 2, 2016). "Ending Homeless Hunger with the Blockchain." *BlockCrushr*. Retrieved from https://www.blockcrushr.com/ending-homeless-hunger-with-the-blockchain.
Buterin, Vitalik. (January 24, 2014). "Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform." *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211.
Caffyn, Grace. (July 30, 2015). "Ethereum Launches Long-Awaited Decentralized App Network." *CoinDesk*. Retrieved from http://www.coindesk.com/ethereum-decentralized-app-network-launch/.
Deery, Brian. (May 7, 2016). "The Blockchain & Future of Business Records – Brian Deery, Chief Scientist of Factom, Inc." *Blockchain News*. Retrieved from http://www.the-blockchain.com/2016/05/07/blockchain-future-business-records-brian-deery-chief-scientist-factom-inc/.
del Castillo, Michael. (May 12, 2016). "The DAO: Or How A Leaderless Ethereum Project Raised $50 Million." *CoinDesk*. Retrieved from http://www.coindesk.com/the-dao-just-raised-50-million-but-what-is-it/.
Deloitte. (February 2016.). *Israel: A Hotspot for Blockchain Innovation*. *Deloitte*. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovatie-blockchain-israel-a-hotspot-for-blockchain-innovation.pdf
Eris Explainer. (n.d.). "What are Smart Contracts?" Retrieved from https://docs.erisindustries.com/explainers/smart_contracts/
"Ethereum Project." (n.d.). Retrieved from https://www.ethereum.org/.
"FAQs." (n.d.). Retrieved from https://www.factom.com/faqs/.
Findlay, Cassie. (January 23, 2015). "Decentralised and inviolate: the blockchain and its uses for digital archives." *Recordkeeping Roundtable*. Retrieved from https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.
Finley, Klint. (June 18, 2016). "A $50 Million Hack Just Showed That the DAO Was All Too Human." *WIRED*. Retrieved from http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/.
Finley, Klint. (January 27, 2014)."Out in the Open: Teenage Hacker Transforms Web into One Giant Bitcoin Network." *WIRED*. Retrieved from http://www.wired.com/2014/01/ethereum/.
Gottfried, Gideon. (August 5, 2015). "How 'the Blockchain' Could Actually Change the Music Industry." *Billboard*. Retrieved from http://www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry.
Graydon, Carter. (August 30, 2014). "Bitcoin's Future: Proof-of-stake vs Proof-of-work." *CryptoCoinsNews*. Retrieved from https://www.cryptocoinsnews.com/bitcoins-future-proof-of-stake-vs-proof-of-work/.
Greenspan, Gideon & Zehavi, Maya. (January 7, 2016). "Will Provenance Be the Blockchain's Break Out Use Case in 2016?" *CoinDesk*. Retrieved from http://www.coindesk.com/provenance-blockchain-tech-app/.
Jentzsch, Christoph. (n.d.). "Decentralized Autonomous Organization to Automate Governance." White Paper.

Retrieved from https://download.slock.it/public/DAO/WhitePaper.pdf.
Kahn, Jeremy. (April 25, 2016). "U.S. Wants Its Own Secure and Self-Destructing Messaging App." *Bloomberg.com*. Retrieved from http://www.bloomberg.com/news/articles/2016-04-25/u-s-wants-its-own-secure-and-self-destructing-messaging-app.
Lemieux, Victoria L. (2016). "Trusting Records: Is Blockchain Technology the Answer?" Records Management Journal 26:2. Retrieved from http://www.emeraldinsight.com/doi/pdfplus/10.1108/RMJ-12-2015-0042.
Levine, Matt. (June 17, 2016). "Blockchain Company's Smart Contracts Were Dumb." *BloombergView*. Retrieved from https://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb
Lopp, Jameson. (July 23, 2016). "Bitcoin: The Trust Anchor in a Sea of Blockchains." *CoinDesk*. Retrieved from http://www.coindesk.com/bitcoin-the-trust-anchor-in-a-sea-of-blockchains/.
Molle, Gregoire. (July 4, 2016). "How Blockchain Helps Brooklyn Dwellers Use Neighbors' Solar Energy." *NPR.org*. Retrieved from http://www.npr.org/sections/alltechconsidered/2016/07/04/482958497/how-blockchain-helps-brooklyn-dwellers-use-neighbors-solar-energy.
Niccolai, Ivan. (December 2015). "Demystifying the Blockchain." KuppingerCole. Retrieved from https://www.kuppingercole.com/access/adnote_blockchain71555261115.
Orcutt, Mike. (May 8, 2015). "Why Bitcoin Could Be Much More Than a Currency." *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/537246/why-bitcoin-could-be-much-more-than-a-currency/.
Pangburn, DJ. (June 19, 2015). "The Humans Who Dream of Companies That Won't Need Us." *Fast Company*, Retrieved from http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them.
Parker, Luke. (April 21, 2016). "Private versus Public Blockchains: Is there room for both to prevail?" *Magnr*. Retrieved from https://magnr.com/blog/technology/private-vs-public-blockchains-bitcoin/.
Patel, Kam. (September 15, 2015). "Everledger: putting bling on the blockchain." *FusionWire*. Retrieved from http://www.fusionwire.net/innovators/everledger-putting-bling-on-the-blockchain/.
Popper, Nathaniel. (May 21, 2016). "A Venture Fund with Plenty of Virtual Capital, but No Capitalist." *The New York Times*. Retrieved from http://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html.
Popper, Nathaniel. (August 28, 2015)."Bitcoin Technology Piques Interest on Wall St." *The New York Times*. Retrieved from http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html.
Quentson, Andrew. (July 4, 2016). "Ethereum's Blockchain to Secure Sneakers in Honor of Kanye West." *Coinjournal*. Retrieved from http://coinjournal.net/ethereums-blockchain-secure-sneakers-honor-kanye-west/.
Rizzo, Pete. (March 2, 2016). "The Case for Ripple in the Age of Big Bank Blockchains." *CoinDesk*. Retrieved from http://www.coindesk.com/ripple-big-bank-blockchains/.
Schout, Sergio. (May 18, 2015). "Exclusive Interview With Factom CEO Peter Kirby." *Bitcoinist.net*. Retrieved from http://bitcoinist.net/exclusive-interview-factom-ceo-peter-kirby/.
Scott, Allen. (June 1, 2016). "Here's Why Your House Is 'Much More Valuable' on the Blockchain." *Bitcoin News*, Retrieved from https://news.bitcoin.com/house-property-value-blockchain/.
Sheppard, Anthony F., & Duranti, Luciana. (December 1, 2010). "The Canadian legal framework for evidence and the Digital Economy: a disjunction?" SSHRC Knowledge Synthesis Grants on the Digital Economy.
Siegel, David. (2016). "Understanding The DAO Attack." *CoinDesk*. Retrieved from http://www.coindesk.com/understanding-dao-hack-journalists/.
Snow, Paul, Brian Deery, David Johnston, Peter Kirby, and Jack Lu. (November 2014). "Factom: Business Processes Secured by Immutable Audit Trails on the Blockchain." White Paper. Retrieved from http://factom.org/.
Standing Senate Committee on Banking, Trade and Commerce. (2015). *Digital Currency: You Can't Flip This*

Coin! Canada: Parliament of Canada. Retrieved from http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf.

"State of the Dapps." (n.d.). Retrieved from http://dapps.ethercasts.com/.

Tapscott, Don & Tapscott, Alex. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.

"The DAO - Curator." (n.d.). Retrieved from https://daohub.org/curator.html.

"The Great Chain of Being Sure about Things." (October 31, 2015). *The Economist.* Retrieved from http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable/.

"This is how Enigio Integrated time:shot works." (n.d.). Retrieved from https://enigio.com/learnmore-timeshot.

"This is how Enigio Integrated time:stamp works." (n.d.). Retrieved from https://enigio.com/integrated.

Thomas, Zoe. (May 6, 2016). "Does Bitcoin still matter?" *BBC*. Retrieved from http://www.bbc.com/news/technology-36197703.

Thompson, Collin. (June 21, 2016). "The DAO of Ethereum." *Linkedin*. Retrieved from https://www.linkedin.com/pulse/dao-ethereum-analysing-hack-blockchain-smart-law-collin-thompson.

Torpey, Kyle. (March 2, 2016). "Vitalik Buterin on Misconceptions in the Private vs Public Blockchain Debate." *Coinjournal*. Retrieved from http://coinjournal.net/vitalik-buterin-on-misconceptions-in-the-private-vs-public-blockchain-debate/.

"UBITQUITY - The Blockchain-Secured Platform for Real Estate Transactions (About)." (n.d.). Retrieved from https://www.ubitquity.io/home/about.html.

"UBITQUITY - The Blockchain-Secured Platform for Real Estate Transactions. (Use Cases)." (n.d.). Retrieved from https://www.ubitquity.io/home/usecases.html.

UK Government Chief Scientific Adviser. (n.d.). "Distributed Ledger Technology: Beyond Block Chain." United Kingdom: Government Office for Science. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Vigna, Paul & Casey, Michael J. (2015). *The Age of Cryptocurrency: How bitcoin and digital money are challenging the global economic order*. St. Martin's Press.

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

"What is Bitcoin?" (n.d.). Retrieved from https://bitcoin.org/en/faq#what-is-bitcoin.

"What is Factom?" (n.d.). Retrieved from https://www.weusecoins.com/what-is-factom/.

Blockchain Technology for Recordkeeping

Overview of Research Initiatives Relating to Blockchain Technology in Canada and Internationally

A Background Paper "Blockchain Technology for Recordkeeping – Help or Hype?" a SSHRC Knowledge Synthesis Grant Study on "How can emerging technologies be leveraged to benefit Canadians?"

Prepared by: Mark Penney, Masters of Archival science and Library Information Studies Student for Principal Investigator Dr. Victoria L. Lemieux

The University of British Columbia, Vancouver, BC, V6T 1Z1
Phone: 604 822 2404
E-Mail: vlemieux@mail.ubc.ca

Table of Contents

INTRODUCTION **61**
SPECIAL CONSIDERATIONS **61**
Distinguishing Research from Hype *61*
Opacity of Private Research *62*
CANADA AND THE BLOCKCHAIN **62**
Research Projects *62*
Individual Researchers *62*
CANADIAN BLOCKCHAIN CONSULTANCIES AND START UPS **63**
POTENTIAL INDUSTRY-ACADEMIA PARTNERSHIPS **63**
SUMMARY **64**
OTHER REGIONS **65**
UNITED STATES OF AMERICA 65
Research Projects *65*
Individual Researchers *67*
Conclusions *68*
UNITED KINGDOM 68
Research Projects *68*

Individual Researchers *69*
Conclusions *70*
AUSTRALIA 70
Research Projects *70*
Conclusions *70*
OTHER COUNTRIES 70
Research Projects *70*
Individual Researchers *71*
PRIVATE SECTOR RESEARCH 71
FINANCIAL INSTITUTIONS AND BANKS 71
GOVERNMENTS 72
RELEVANT CONFERENCES 72
CONCLUSION 73
REFERENCES 74

Introduction

Over the last several years, interest in the blockchain has been growing among computer engineers, business people, financial specialists, and now academics. Blockchain is a computer-based system that forms a key part of the architecture of the Bitcoin cryptocurrency. It announces, publishes, and/or records transactions between anonymous parties across a decentralized network of participating computers. Each transaction generates a cryptographic hash that is linked to a previous transaction's hash, making it extremely difficult to perform certain kinds of fraud. Most importantly, it does these things without the need for a trusted third party (which in the case of financial transactions is usually a bank or other financial services provider). The blockchain is of great interest to financial service providers and many have moved quickly to investigate its potential applications.

Academia has been slower in turning its attentions towards the blockchain. Aside from a few large, technology-forward institutions, blockchain is still primarily the preserve of business. This paper intends to survey the academic world, mostly in the anglosphere, in an attempt to provide a picture of academic blockchain research as it stands in 2016. Specific attention will be paid to blockchain innovation and research in Canada, with a focus on research that is relevant to archives and records management professionals.

Special Considerations

Distinguishing Research from Hype

A great deal of the material available about Blockchain, both online and off, is journalism and publicity material for new businesses. As the prime drivers of blockchain innovation are the tech companies building new blockchain-based services, it should be kept in mind that the materials they produce are not the result of academic or peer reviewed research. Furthermore, collaborations between some of these companies and universities make this space a complicated one. One example of note is the dominance of the Massachusetts Institute of Technology (MIT) in blockchain research and its relationship to Bitcoin's developers. Three of Bitcoin's dedicated developers, Gavin Andresen, Waldimir van der Laan, and Corey Fields are members of MIT's Digital

Currency Initiative ("Welcome to the Media Lab," n.d.). Although Andresen states that MIT does not direct Bitcoin development, it is worth noting this close contact (Andresen, n.d.). MIT, because of its association with Bitcoin, is likely to be the major centre of academic production on the blockchain.

Opacity of Private Research

A great deal of blockchain research is currently happening at banks and other financial institutions. These private institutions are known to jealously guard their secrets. Although some of this research may yet see the light of day, it is more difficult to determine the state and nature of this material than research projects being conducted at universities.

Canada and the Blockchain

The following describes the state of academic research on the blockchain in Canada. It goes on to propose collaborations between academia and the private sector and to discuss Canada's place in future blockchain endeavours.

Research Projects

The academic research landscape for the blockchain in Canada is not well developed. Recognized tech hubs like the University of Waterloo and the University of Toronto do not offer any clear information on blockchain research and do not appear to support any long term or organized research initiatives.
The University of Waterloo currently lists a Cryptography, Security, and Privacy project with a sub-project on cryptocurrencies headed by professor Sergey Gorbunov. It does not appear to be producing any substantial research about the blockchain specifically, although considering its subject focus it is possible it may be an area of study in the future ("Cryptography, Security, and Privacy," n.d.). There is also some research occurring or that has occurred at the Universite de Montreal ("Technologies de confiance," n.d.).

Individual Researchers

A small handful of individuals 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 (Eskandari, Barrera, Stobert & Clark, n.d.) before moving to ETH Zurich, which has a dedicated project on Security and Privacy of Bitcoin ("Security and Privacy of Bitcoin," n.d.). More information on ETH Zurich is available below.
At the University of Toronto iSchool, PhD student Quinn DuPont is currently pursuing research on blockchains and distributed ledgers (Quinn Dupont | Faculty of Information," n.d.). This includes papers examining the relationship of blockchain and the law ("Ledgers and Law in the Blockchain," n.d.), and a paper examining bitcoin and cryptography, where he argues that cryptography can be viewed as a "notational system" (Dupont, 2014, para. 5).
Also at the University of Toronto, father and son team Donald and Alex Tapscott (2016) 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 subject within the university, however the book is an important resource for projected blockchain use cases and a trove of start-ups and consultancies.
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 ("Proceedings of the Standing Senate Committee," n.d.). 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. Finally, Clark was formerly a PhD student at University of Waterloo in the Cryptography, Security, and Privacy project ("Jeremy Clark," n.d.).

Canadian Blockchain Consultancies and Start ups

Some Canadian Bitcoin businesses and organizations offer blockchain consultancy services. These include:

- decentral, that offers a wide variety of potential consulting services related to Blockchain. Of note here is that its consultants includes Anthony Di Iorio and Vitalik Buterin, who are constant players in the Canadian Bitcoin scene. Di Iorio is the one time head of the Bitcoin Alliance of Canada ("Bitcoin Alliance of Canada | Promoting Bitcoin in Canada," n.d.), while Buterin is the founder of Ethereum, the premiere blockchain start up("Decentral Consulting - Blockchain Consulting Services," n.d.).

- Quadriga Fintech Solutions, who are opening the "Blockchain Innovation Lab," in Vancouver. It claims to be Canada's first blockchain research and development lab ("Quadriga to Launch First Canadian Blockchain R&D Lab," 2015). 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"("What we do – Digital Finance Institute," n.d.)· Duhaime's firm, Duhaime Law, also offers information and presumably services related to blockchains ("Blockchain Duhaime Law," n.d.).

- Ledger Labs is a Toronto-based blockchain consultancy that offers strategy, development, security, and training services ("Services - Ledger Labs," n.d.).

There are also a handful of Canada-based blockchain start-ups. These include:

- Bluezelle, which is creating blockchain financial products centered on the foreign exchange market ([1] "Blockchain and Ripple Solutions," n.d.).

- Rubix by Deloitte, which is producing blockchain enterprise solutions. Some examples provided include: decentralized capital markets systems; peer-to-peer payments; and health data management. There is also a note regarding an alternative asset management blockchain solution that this team is building in collaboration with New York communications firm Estey-Hoover ("RUBIX - Build Great Decentralized Applications," n.d.). This initiative deliberately uses the term records management. Deloitte appears to be recruiting from the university of Waterloo, as at least two current employees (Hanumanth Kumar Jayakumar and Hengyi (Tony) Liu) are currently or were recently students there ("Hanumanth K. Jayakumar | LinkedIn," n.d.).

- Blockstream, which creates sidechains that connect to other asset types and interoperates with bitcoin ("Blockstream," n.d.).

- Cryptiv, which is pursuing blockchain for enterprise digital assets ("Cryptiv," n.d.).

Potential Industry-Academia Partnerships

At the time of writing no industry-academia partnerships appear to exist in Canada. Aside from Deloitte's Rubix project and its sourcing of talent from the University of Waterloo, there are no large scale co-operations. Interested academics looking to explore potential partnerships could start with their local Bitcoin meet up (these meet ups are common in many large cities). A further approach is to contact the "Bitcoin Embassy" in Montreal ("Bitcoin Embassy - World's first Blockchain hub," n.d.) or the Bitcoin Alliance of Canada as likely places to make the connections necessary to understanding this rapidly changing space. The Bitcoin Alliance was involved in championing Bitcoin and related technologies before the senate ("BAC to Appear Before Senate Banking, Trade and Commerce Committee," n.d.). Additionally, an event called the Blockchain World Expo will be taking place on Sept. 19-21, 2016 in Toronto, ON ("Fintech and Blockchain World Expo," n.d.). This event is sponsored by Ethereum, perhaps the premiere organization in the blockchain space worldwide, and decentral, which is one of Canada's largest blockchain start-ups.

On a more technical level, computer science programs across Canada would do well to seek out initiatives like Rubix, Ethereum, and others in an attempt to partner. From a pure research perspective, UBC iSchool's nascent blockchain research group (of which this paper forms a part) and researchers like Quinn DuPont at the University of Toronto iSchool may wish to seek partnerships with organizations like Quadriga Fintech Solution's Blockchain Innovation Lab. This space seems to offer the possibility to gain from the technical expertise often lacking in the archives and records management profession, and also the potential of addressing pressing legal questions of concern to archives and records management. Potential collaborations with Deloitte, Ethereum, and other universities pursuing projects relevant to archives and records management issues (such as MIT's MedRec and Media Lab Digital Certificates; Cornell's Theoretical Foundations for Secure Decentralized Systems, Hawk, Town Crier, Virtual Notary; and Princeton/Blockstack Labs) may also be worth pursuing.

Summary

Although Canada currently lacks robust academic research into blockchains, it is poised to be a potential leader in the Bitcoin, and by extension potentially blockchain, space. In an article describing the Canadian senate hearings on Bitcoin, Bitcoin Magazine noted that:

> There was a strong argument made by witnesses that Canada is well placed with tech expertise, cheaper energy rates and a knowledge infrastructure to be the No. 1 Bitcoin country in the world (Willms, 2015, para. 29).

In keeping with this belief, the 2015 Senate report entitled "Digital Currency: You Can't Flip This Coin!" calls for: The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies (Standing Senate Committee on Banking, Trade and Finance, 2015, p. 9).

Whether this regulatory light touch will ultimately be realized is another question. Also open to question is whether Bitcoin innovators will materialize in Canada. At the moment (and aside from decentral and handful of others noted above) the majority of Bitcoin/blockchain innovation appears to be taking place in the United States. One piece of evidence supporting Bitcoin Magazine's conclusions is that Deloitte has headquartered its Rubix blockchain application team in Toronto.

Other Regions

United States of America

Research Projects

The United States of America currently possesses the largest and most detailed academic research projects regarding the Blockchain.

Massachusetts Institute of Technology (MIT)

Besides being the current home of some of the core Bitcoin developers, MIT is the American leader in the blockchain research space. MIT blockchain research is performed at the MIT Media Lab's Digital Currency Initiative, headed by Brian Forde. It has an active collaboration with the Harvard Berkman Centre for Internet and Society (to be discussed further). There are currently several projects stemming from this initiative of interest to archives and records management professionals. These are:

MedRec

An Ethereum-based blockchain electronic medical records (EMRs) solution. It describes itself as a "decentralized records management system for EMRs that uses blockchain technology to manage authentication, confidentiality, accountability, and data sharing." One interesting aspect of MedRec is that it allows medical researchers to use anonymous patient data for research purposes by placing them in the role of miners in the analogous Bitcoin system ("MedRec," 2016, n.p.).

Enigma

Enigma is "A peer-to-peer network, enabling different parties to jointly store and run computations on data while keeping the data completely private" ("Enigma," n.d., n.p.). A blockchain acts as the network's "controller.' Enigma promises "autonomous control of personal data" with no need for a trusted third party (n.p.).

Media Lab Digital Certificates

This project uses a blockchain to "store and manage digital credentials" ("Media Lab Projects," 2016, p. 64). In the brief description provided for this project, it is described thusly: "certificates are registered on the blockchain, cryptographically signed, and tamper-proof" (p.64). On the projects devoted page, it is further described as being education focused ("Digital Certificates Project," n.d.).

Altogether, MIT is the premier location for blockchain research in the United States.

Cornell

Cornell University is another institution with major blockchain research underway. Blockchain research at Cornell falls under the umbrella of the IC3, or Initiative for Cryptocurrencies & Contracts, headed by Ari Juells. It is a collaboration between Cornell University, Cornell Tech, UC Berkeley, University of Illinois Urbana-Champaign, and the Technion (part of the Israel Institute of Technology) ("IC3 About," n.d.). It currently has twelve blockchain related research projects.

Solidus

Solidus is a centralized cryptocurrency for use by "trustworthy entities" – noted as banks, governments, or auditors ("IC3 Projects," n.d., para. 1). Its official description notes that "while it retains some of the benefits of decentralization, Solidus offers higher performance and tighter governance and control than existing cryptocurrencies such as Bitcoin" (para. 1). The name appears to be a deliberate reference to the solidus (a type of gold coin) of the roman emperor Diocletian, who introduced it in order to fight currency debasement.

Bitcoin-NG

Bitcoin-NG is a protocol that aims to address transaction speed problems in blockchain-based systems. It is

described thus:
It addresses the scalability bottleneck of Bitcoin by enabling the Bitcoin network to achieve the highest throughput allowed by the network conditions. Paradoxically, not only does it improve transaction throughput, it also reduces transaction latencies -- it is possible to get an initial transaction confirmation in seconds rather than in minutes. And it does so without changing Bitcoin's open architecture and trust model ("IC3 Projects," n.d., para. 2).

Miniature World

Miniature World is a blockchain emulation test-bed of 1000 nodes for research purposes ("IC3 Projects," n.d., para. 3).

Fruitchain

Fruitchain appears to be a blockchain security tool. It is described as a "methodology that discourages dishonest gaming," or attacks against Bitcoin systems. Interestingly, the description claims that IC3 researchers have proven that Bitcoin systems are susceptible to attacks below the commonly understood 50% mining hash power threshold, and that Fruitchain is a response to this ("IC3 Projects," n.d., para. 4).

Falcon Network

Falcon Network is similar to Bitcoin-NG, in that it addresses transaction speeds. Its official website states that it is a: "fast relay network for disseminating Bitcoin blocks. It connects miners and full nodes and ferries blocks using a novel technique to reduce orphans, which in turn helps miners get the most for their effort, and helps the network efficiently convert the spent energy into security" ("IC3 Projects," n.d., para. 5).

FLAC

Flow-Limited Authorization Calculus (FLAC) is a security tool. It is "both a simple, expressive model for reasoning about dynamic authorization and also a language for securely implementing various authorization mechanisms" ("IC3 Projects," n.d., para. 6)

Theoretical Foundations for Secure Decentralized Systems

As opposed to the other IC3 projects that are usually organized around a tool or system, this initiative is a pure research project that "explores the theoretical basis for the security and stability of open decentralized systems" ("IC3 Projects," n.d., para. 7)

Hawk

Hawk is described as a "privacy-preserving blockchain & smart contracts." It would appear that Hawk does away with the ability of all users to see the details of financial transactions on a Bitcoin/blockchain system and makes these details private ("IC3 Projects," n.d., para. 8).

Town Crier

Town Crier examines the integration of authenticated data feeds into smart contracts. Authenticated data feeds provide "live" data for smart contracts that can influence the functions of the contract ("IC3 Projects," n.d., para. 9).

Virtual Notary

Virtual notary is just that, and states that it "issues both freestanding certificates as well as immutable records on the Bitcoin blockchain" ("IC3 Projects," n.d., para. 10).

Etherscrape

Etherscrape is an Ethereum/smart contract tool that reveals a great deal of information that is obscured between the source code of a smart contract and its "bytecode" in application ("IC3 Projects," n.d., para. 11).

Gyges

Gyges is a research project examining the intersection of smart contracts and crime ("IC3 Projects," n.d., para. 12).

Harvard University

Current research on the blockchain at Harvard is being performed through its Berkman Center for Internet and Society's Digital Finance Initiative ("Digital Finance Initiative | Berkman Klein Center," n.d.). This initiative is

occurring in partnership with MIT. Primavera De Fillipi, a Harvard-associated scholar, has published extensively on legal ramifications of Bitcoin and the blockchain ("Primavera De Filippi | Berkman Klein Center," n.d.).

Princeton University

Princeton has an association with an organization called Blockstack labs. Blockstack appears to be the new name of an organization of formerly known as Onename. The Onename website currently states that a user can "Register an Identity" and that it is a "global database for people, companies, websites and more." Blockstack itself is a service for buildings apps that run on the decentralized blockchain system instead of via a server ("Blockstack," n.d.). The authors of the initiating paper on Blockstack, Muneeb Ali, Jude Nelson, and Michael J. Freedman, are all associated with Princeton. Furthermore, professor Arvind Narayanan and several other contributors have produced a major volume on Bitcoin and blockchain, and continue to perform research on the subject (Narayanan, Bonneau, Felten, Miller, & Goldfeder, n.d.). Incidentally, this book is available for free online. Arvind Narayanan advises a number of students who are also producing research on Bitcoin, including Harry Kalodner, who is interested in public adoption of Bitcoin and blockchain systems (Kalodner, n.d.).

Stanford University

The home of bitcoin and blockchain related research at Stanford is in its Applied Cryptography research group ("Applied Cryptography Group | Stanford University," n.d.). Notable scholars there include Joseph Bonneau, who was a co-author on "Bitcoin and Cryptocurrency Technologies" ("Joseph Bonneau — index," n.d.), and Dan Boneh ("Dan Boneh," n.d.).

University of Maryland

The University of Maryland possesses a Cybersecurity Center with a heavy interest in cryptography ("Maryland Cybersecurity Center," n.d.). Although it does not appear to currently be producing any Bitcoin or blockchain specific research, it is a space to monitor. Previous student Andrew Miller was a co-author on *Bitcoin and Cryptocurrency Technologies (*Narayanan, Bonneau, Felten, Miller, & Goldfeder, n.d.), and he continues his research at the University of Illinois at Urbanan-Champaign ("Andrew Miller," n.d.). He has also collaborated on the Cornell Hawk project and is the Assistant Director of Cornell's IC3.

Individual Researchers

A large number of American academics are currently pursuing blockchain research outside of a dedicated research program or unit.

- David Yermack of NYU is currently examining the financial applications of blockchain ("NYU Stern - David Yermack," n.d.).
- Angela Walch of St. Mary's University School of Law examines blockchain and the law ("Angela Walch," n.d.).
- Aaron Wright at Cardozo School of Law (Yeshiva University) works on legal aspects of blockchain; he has a book forthcoming with Primavera De Fillippi on the subject of the blockchain ("Aaron-Wright | Cardozo Law," n.d.).
- Elizabeth Stark at Yale Law School is producing legal scholarship on the blockchain (Tapscott & Tapscott, 2016, p. 288).
- Dawn Song, a professor of computer science at UC Berkeley is pursuing blockchain research from a security and cryptography perspective (Tapscott & Tapscott, 2016, p. 288).
- Tariq B. Ahmad at The University of Massachusetts, Amherst, who is interested in "open source blockchain analytics on blockchain and other data sources using Big Data tools in a browser

environment" and researches on security and parallel computing (Ahmad, n.d.).
- Joshua J. Doguet, a former student of Louisiana State University, published an article on legal and regulatory issues for Bitcoin (Doguet, 2013).
- Bill Maurer of UC Irvine, a cultural anthropologist, pursues anthropological/legal research on blockchain ("Research | Bill Maurer," n.d.).
- Gaby Dagher of Boise State University is pursuing computer science research regarding Bitcoin and cryptography, privacy, and cybersecurity ("Dr. Gaby Dagher," n.d.).
- Ethan Heilman, Foteini Baldimsti, and Sharon Goldberg at Boston University have published a paper about smart contracts (Heilman, Baldimtsi, & Goldberg, n.d.).
- Sarah Jane Hughes at Indiana University Bloomington's Maurer School of Law has performed some research on virtual currencies ("Sarah Jane Hughes: Faculty and Staff of Indiana University Maurer School of Law," n.d.).

Conclusions

Most research projects in the USA on the blockchain are associated with the production of a program, application, or tool. Compared to other nations, the USA easily leads in the blockchain research space.

United Kingdom

Research Projects

The United Kingdom follows the United States in its concentration of blockchain research. The research produced at UK institutions tends to be much more theoretical.

University College London

University College London has two on-going initiatives with a significant blockchain component. The first is the Centre for Law, Economics and Society (CLES) that has a Digital Currencies, Digital Finance, and Constitution of a New Financial Order research project. Unlike many American projects, this one is not associated with an application or tool, and is indeed a research project solely focused on financial, or economic perspectives. The College's second initiative is the UCL Centre for Blockchain Technologies, which aims to produce blockchain research in the three key areas of science and technology, economics and finance, and regulation and law ("ABOUT US | UCL Blockchain," n.d.). Finally, it is also worth noting that UCL scholars M. Angela Sasse, George Danezis, and Sara Meiklejohn contributed to the UK Government Office for Science's Distributed Ledger Technology report, specifically the fourth chapter on Security and Privacy ("Distributed ledger technology," n.d.).

Imperial College London

Imperial College London also has two initiatives. One is the Centre for Cryptocurrency Research and Engineering, which aims to (I) research, design, and improve blockchain technology, (II) understand "dynamic operations of blockchains and associated markets," and (III) to explore "novel blockchain-based applications across multiple domains" ("About us | Imperial College London," n.d., n.p.). The second initiative is called Cryptocurrency Effects in Digital Transformations, which is part of the Imperial College London Business School. It examines digital currencies and distributed ledger systems, and aims to create a Bitcoin/blockchain methodology and to run pilot studies to understand impacts ("Cryptocurrency Effects in Digital Transformations | Imperial College Business School," n.d.). It is run in conjunction with the University of Surrey, whose blockchain researching academics appear to solely consist of Philip Godsif ("Philip Godsiff - University of Surrey - Guildford," n.d.). One of the principals in each project is Catherine Mulligan, who contributed to the UK Government

Office for Science's Distributed Ledger Technology report, specifically chapter six, "Applications in Government" ("Distributed ledger technology," n.d.).

Cambridge University

Cambridge University runs a Center for Alternative Finance that uses a picture of a Bitcoin prominently on its main page. However, it does not appear that any dedicated research on Bitcoin, the blockchain, cryptocurrencies or distributed ledgers is currently being performed there ("Cambridge Centre for Alternative Finance," n.d.).

Coventry University

Coventry University's Centre for Business in Society possesses a program called Bitcoin and Beyond: Block Chain, Digital Currencies and the Construction of Alternative Economies. It aims to examine the potential links between Bitcoin, blockchain, and social innovations. Unfortunately it appears to have ended ("Bitcoin and beyond," n.d.).

University of Cumbria

The University of Cumbria's Institute for Leadership and Sustainability has performed "Research on alternative currencies and exchange systems," specifically on Bitcoin ("Research into Currencies | University of Cumbria," n.d.).

University of Edinburgh

The University of Edinburgh has a Design in Action research project that is part of the College of Art. This project explores artistic applications of the blockchain. The project has produced three articles "Story blocks: Reimaging narrative through the blockchain," "Effing the ineffable: Opening up understandings of the blockchain," and "Blockchain City" ("ECA, University of Edinburgh," n.d.).

Middlesex University London

Similar to the University of Edinburgh, Middlesex University London's Schools of Media & Performing Arts and Science & Technology have collaborated on a research group called Blockchain for Creative Industries. It has produced one article about the potential effect of blockchain on recorded music, as well as a conference presentation ("Blockchain for Creative Industries | Middlesex University London," n.d.).

Oxford University

Oxford University currently has a dedicated research project on the subject of blockchain for undergraduates and masters students known as "Bitcoin and block chain for physical computing." It's goals are to: "[implement] a sensor that makes physical measurements in return for Bitcoin payments, and/or [implement] smart Bitcoin cash, which unlike a Bitcoin wallet, doesn't hold your Bitcoin, but is the Bitcoin (i.e. it has its own Bitcoin address and private key)" ("Student project: Bitcoin and block chain for physical computing," n.d.).

Open University

The Open University has a significant blockchain project known as Open Blockchain. This project investigates the applications of blockchain to higher education and eportfolios/feedback/accreditation. Additionally, they have been conducting experiments using Ethereum smart contracts ("Open BlockChain," n.d.).

Individual Researchers

There are a small number of individual UK blockchain researchers with noteworthy work:

- Steve Huckle at the University of Sussex, looking at blockchain from an Informatics background ("Research: Steve Huckle: University of Sussex," n.d.).
- Tatianna Cutts at the University of Birmingham, who gave a presentation entitled "Tracing Bitcoins." She is a professor of law who studies property ("Blockchain and financial markets technology," n.d.).
- Debbie Maxwell at the University of York is researching social aspects of blockchain via design modelling ("Dr. Debbie Maxwell - Publications - Research Database, The University of York," n.d.).
- Philip Godsif at the University of Surrey's Business department has at least one publication on blockchains ("Philip Godsiff - University of Surrey - Guildford," n.d.). He also contributed to the fourth and fifth chapter of the UK's Distributed Ledger report ("Distributed ledger technology," n.d.).

Conclusions

Blockchain research in the UK is focused more on theoretical points than on practical applications as in the United States. Nevertheless, the large amount of ongoing blockchain research means that the UK is a space to watch in blockchain innovation.

Australia

Research Projects

There are several active blockchain research projects in Australia.

University of Melbourne

The University of Melbourne's Melbourne Networked Society Institute (MNSI) currently lists Blockchain as a 2016 research Focus Area under the "Financial" category ("Seed Funding 2016," n.d.).

University of Western Australia

An undergraduate student project at the University of Western Australia created a blockchain based voting system, which won a $5000 prize at a Young Entrepreneurship Bootcamp ("UniHallers Win $5000 Grant | UniHall - UWA," n.d.).

University of Technology, Sydney

The Finance Discipline Group contributed to the Australian Senate's report on Bitcoin (Parliament of Australia, n.d.). Additionally, the school also has an Innovation & Creative Intelligence Unit that is running a series of workshops exploring the blockchain, from July to October 2016 ("UTS: ICI Creative Clusters - Blockchain | University of Technology Sydney," n.d.).

Conclusions

Australia is not currently producing much in the way of blockchain research, however the University of Melbourne's stated research interest holds out the promise of useful material to come.

Other Countries

Research Projects

National Institute of Informatics, Japan

Three researchers at the National Institute of Informatics in Japan have produced a paper entitled "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin." The authors are Bela Gipp, Norman Meuschke, and André Gernandt, The abstract offers: "a web-based service that uses the decentralized Bitcoin block chain to store anonymous, tamper-proof timestamps for digital content. The service allows users to hash files, such as text, photos or videos, and store the created hashes in the Bitcoin block chain" (Gipp, Meuschke, & Gernandt, 2015).

ETH Zurich

ETH Zurich's Institute of Information Security has a System Security Group with a Security and Privacy of Bitcoin project. It is further divided into the following research themes:

- Tampering with the Delivery of Blocks and Transactions in Bitcoin
- Quantifying Location Privacy Leakage from Transaction Prices
- Misbehavior in Bitcoin: A Study of Double-Spending and Accountability
- On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients
- Is Bitcoin a Decentralized Currency?
- Double-spending Attacks on Fast Payments in Bitcoin; Evaluating User Privacy in Bitcoin

This project is also notable because it has the participation of Elizabeth Stobert, formerly of Carleton University in Ottawa ("Security and Privacy of Bitcoin," n.d.).

National University of Singapore

Researchers at the National University of Singapore are currently conducting research on smart contracts(Luu, Chu, Olickel, Saxena, & Hobor, n.d.). The Security Research Cluster, and particularly students working with Prateek Saxena, are producing this research ("Prateek Saxena's Home Page," n.d.).

Individual Researchers

There are a large number of international scholars producing blockchain research outside of a wider project.

- Aggelos Kiayas at the University of Athens / University of Connecticut has focused on the applicability of blockchain to voting systems ("Home of Aggelos Kiayias," n.d.).
- Donncha Kavanagh at University College Dublin has some interest in blockchain but has not produced any published research ("UCD Home: The UCD Centre for Innovation, Technology & Organisation," n.d.).
- Kaitai Liang at Aalto University (Finland) has also identified blockchain as a research interest, but has not produced any published material ("Kaitai Liang," n.d.).
- Kenji Saito at Keio University has produced research on Bitcoin and the blockchain from a computer science perspective (Saito, n.d.).
- Matteo Solinas at the University of Wellington, Victoria has produced research regarding blockchain regulation and the law ("Matteo Solinas - The Regulation of Distributed Ledgers," n.d.).

Private Sector Research

The private sector is increasingly interested in blockchain technology. Large financial institutions especially have led the charge on blockchain and produced research in advance of academic institutions.

Financial Institutions and Banks

A large number of banks and other financial service firms have expressed interest in blockchain technologies and have some kind of ongoing research. The list of institutions is very large, and many of the world's major

financial institutions are represented. Most of these institutions have partnered with R3CEV, a blockchain company that is attempting to create distributed ledgers for financial markets ("About R3," n.d.). They currently have at least 46 institutions as partners, and more seem to be joining regularly ("R3 (company)," 2016).

There are several good resources available for keeping track of this space. One is the "Financial Institution Involvement" list on the Blockchain page of law firm Davis Polk & Wardell LLP ("Blockchain | Blockchain Regulation Resources," n.d.). Additionally, the book *Blockchain Revolution* contains a section listing a number of financial institutions investigating the blockchain (Tapscott & Tapscott, 2016, p. 285). Finally, the Bitcoin magazine CoinDesk reports on the latest news regarding blockchain and institutional interest ("CoinDesk Bitcoin and Blockchain News," n.d.).

In terms of public facing research, Deloitte's report "Blockchain: Enigma. Paradox. Opportunity," is an excellent overview of many of the potential use cases that motivate institutional interest. These include (broadly): banking, insurance, the public sector, and media (*Deloitte-Blockchain-Enigma-Paradox-Opportunity.pdf*, 2016).

Governments

A number of governments have produced reports regarding Bitcoin and the blockchain in recent years. Within Canada, these include:

- "Digital Currency: You Can't Flip This Coin," from the Standing Committee on Banking, Trade and Commerce of the Canadian Senate (Standing Senate Committee on Banking, Trade and Finance, 2015).
- "A Bitcoin Standard: Lessons from the Gold Standard," from the Bank of Canada (Weber & others, 2016).
- "Cryptocurrencies: Bitcoins and Beyond," from Policy Horizons Canada

Other governments have produced the following:

- "Digital Currencies: Response to the Call for Information," from HM Treasury, UK. (Great Britain & Treasury, 2015).
- "Distributed Ledger Technology: Beyond Blockchain," from the Government Office for Science, UK ("Distributed ledger technology," n.d.).
- "Digital Currency – Game Changer or Bit Player," from the Senate Economics and References Committee of the Senate of Australia (Parliament of Australia, n.d.).
- "Blockchain Technology: Opportunities and Risks," from the State of Vermont (Sorrell, General, & General, 2016).
- "Discussion Paper – The Distributed Ledger Technology Applied to Securities Markets," from the European Securities and Markets Authority (European Securities and Markets Authority, 2016).
- "Blockchain Technology: Possibilities for the US Postal Service," from the Office of the Inspector General of the United States Postal Service (*Blockchain Technologies: Possibilities for the U.S. Postal Service*, n.d.).

Relevant Conferences

A number of academic conferences take place where blockchain research is of increasing interest. Annual conferences that have featured blockchain items include:

- New York Blockchain Workshop (associated with NYU) ("NYU Stern | Event | New York Blockchain Workshop," n.d.).
- Workshop on Bitcoin and Blockchain Research (3rd iteration in Barbados) ("3rd Workshop on Bitcoin and Blockchain Research," n.d.).
- Mediterranean Conference on Information Systems ("MCIS 2016," n.d.).

- Melbourne Money & Finance Conference ("Melbourne Money & Finance Conference 2016," 2016).
- International Conference on Enterprise Information Systems (ICEIS) ("ICEIS 2017 - Home," n.d.).
- Critical Legal Conference (Kent University) ("Call for Papers and Panels for Critical Legal Conference | Law News," n.d.).
- The Internet, Policy & Politics Conferences 2016 "The Platform Society" ("Call for Papers: IPP2016 'The Platform Society,'" n.d.).
- Proceedings on Privacy Enhancing Technologies Symposium ("PETs 2016 The 16th Privacy Enhancing Technologies Symposium," n.d.).
- International Conference of Financial Cryptography ("FC'16: Financial Cryptography 2016," n.d.).
- Applied Cryptography and Network Security Conference ("ACNS 2016" n.d.).
- Institute of Electrical and Electronics Engineers (IEEE) annual Conference ("IEEE Symposium on Security and Privacy 2016," n.d.).
- International Conference on Digital Preservation ("Welcome – iPRES 2016 - 13th International Conference on Digital Preservation," n.d.).
- Consensus Conference ("Consensus 2016," n.d.).
- Blockchain and financial markets technology; Perspectives from Law, Finance, and Computer Science ("Blockchain and financial markets technology," n.d.).
- The Sixth International Conference on Advanced Collaborative Networks, Systems and Applications ("COLLA 2016," n.d.).
- International Blockchain Week ("Ethereum Foundation and Wanxiang Blockchain Labs," 2016).
- Provable Security Conference in Nanjing, China ("ProvSec 2016," n.d.).

Due to the relative newness of the blockchain, a number of conferences have also been initiated recently. These include:

- Digital Currencies, Digital Finance and the Constitution of a New Financial Order: Challenges for the Legal System. An event run by UCL in Athens, Greece in 2016 ("Digital Currencies, Digital Finance and the Constitution of a New Financial Order: Challenges for the Legal System," n.d.).
- Controlling Cryptocurrencies at the University of Birmingham, UK ("Controlling Crypto-currencies," n.d.).
- Blockchain World Expo in 2016 in Toronto, Canada ("Fintech and Blockchain World Expo," n.d.).

Conclusion

Blockchain technology is beginning to be recognized as a major academic research area worldwide, although Canada lags considerably in dedicated academic blockchain research. The private sector fairs better, and Canada is home to a small number of blockchain initiatives, start-ups, and consultancies. Underlying favourable conditions, such as an educated workforce and a vibrant blockchain ecosystem, may allow Canada to forge ahead in the blockchain technoscape. Regardless of how Canada fairs, the United States especially houses the vast majority of ongoing blockchain research and activity, with the UK in second place. Several institutions elsewhere, like ETH Zurich in Switzerland, are producing a considerable amount of useful research on the subject. This survey attempts to document the nascent blockchain research space to provide a resource that scholars can use to contextualize new blockchain research and help them to make useful connections. It will prove especially vital to Canadian scholars, who are beginning in a relatively barren academic landscape and urgently need to begin making connections and forming a community to support blockchain research. Aside from Quinn DuPont's research at the University of Toronto, this survey also reveals the lack of blockchain research related to recordkeeping, a void that this project can move to fill with assurance. Regardless of whether blockchain technology fulfills the expansive hopes of some of its proponents, it certainly appears that the next few years will be a productive time for scholars with the abilities and interest to

pursue study of the blockchain.

References

3rd Workshop on Bitcoin and Blockchain Research. (n.d.). Retrieved from http://fc16.ifca.ai/bitcoin/
aaron-wright | Cardozo Law. (n.d.). Retrieved from http://www.cardozo.yu.edu/directory/aaron-wright
About R3. (n.d.). Retrieved from http://r3cev.com/about/
ABOUT US | UCL Blockchain. (n.d.). Retrieved from http://blockchain.cs.ucl.ac.uk/about-us/
About us | Imperial College London. (n.d.). Retrieved from http://www.imperial.ac.uk/cryptocurrency/about/
ACNS 2016 - 14th International Conference on Applied Cryptography and Network Security. (n.d.). Retrieved from http://acns2016.sccs.surrey.ac.uk/index.html
Ahmad, T. B. (n.d.). Blockchain Workshop Position Statement. Retrieved from https://www.w3.org/2016/04/blockchain-workshop/interest/ahmed.html
Andresen, G. (n.d.). Joining the MIT Media Lab Digital Currency Initiative. Retrieved from http://gavintech.blogspot.com/2015/04/joining-mit-media-lab-digital-currency.html
Andrew Miller phd@umd. (n.d.). Retrieved from https://www.cs.umd.edu/~amiller/
Angela Walch. (n.d.). Retrieved from https://law.stmarytx.edu/academics/faculty-and-staff/angela-walch/
Applied Cryptography Group | Stanford University. (n.d.). Retrieved from https://crypto.stanford.edu/
BAC to Appear Before Senate Banking, Trade and Commerce Committee | Bitcoin Alliance of Canada. (n.d.). Retrieved from http://bitcoinalliance.ca/2014/09/26/bac-to-appear-before-senate-banking-trade-and-commerce-committee/
Bitcoin Alliance of Canada | Promoting Bitcoin in Canada. (n.d.). Retrieved from http://bitcoinalliance.ca/
Bitcoin and beyond: Block chain, digital currencies and the construction of alternative economies at Coventry University on FindAPhD.com. (n.d.). Retrieved from https://www.findaphd.com/search/projectdetails.aspx?PJID=75041
Bitcoin Embassy - World's first Blockchain hub. (n.d.). Retrieved from http://bitcoinembassy.ca/
Blockchain | Blockchain Regulation Resources. (n.d.). Retrieved from https://www.blockchain-reg.com/blockchain#section-412
Blockchain Duhaime Law. (n.d.). Retrieved from http://www.duhaimelaw.com/category/blockchain/
Blockchain and financial markets technology: Perspectives from Law, Finance and Computer Science. (n.d.). Retrieved from http://www.systemicrisk.ac.uk/events/blockchain-and-financial-markets-technology-perspectives-law-finance-and-computer-science
Blockchain and Ripple Solutions | Bluzelle - We build solutions over Blockchain and Ripple. (n.d.). Retrieved from http://bluzelle.com
Blockchain for Creative Industries | Middlesex University London. (n.d.). Retrievedfrom http://www.mdx.ac.uk/our-research/research-groups/blockchain-for-creative-industries
Blockchain Technologies: Possibilities for the U.S. Postal Service. (n.d.). Retrieved from https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-001.pdf
Blockstack. (n.d.). Retrieved from https://blockstack.org/
Blockstream. (n.d.). Retrieved from https://www.blockstream.com/
Call for Papers and Panels for Critical Legal Conference | Law News. (n.d.). Retrieved from https://blogs.kent.ac.uk/law-news/2016/05/09/call-for-papers-and-panels-for-critical-legal-conference/
Call for Papers: IPP2016 "The Platform Society" | The Internet, Policy & Politics Conferences. (n.d.). Retrieved July 20, 2016, from http://ipp.oii.ox.ac.uk/2016/call-for-papers
Cambridge Centre for Alternative Finance. (n.d.). Retrieved from http://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/
CoinDesk Bitcoin and Blockchain News. (n.d.). Retrieved from http://www.coindesk.com/
COLLA 2016. (n.d.). Retrieved from http://www.iaria.org/conferences2016/COLLA16.html

Consensus 2016: Making Blockchain Real. (n.d.). Retrieved from http://www.coindesk.com/events/consensus-2016/
Controlling Crypto-currencies. (n.d.). Retrieved from https://controllingcryptocurrencies.wordpress.com/
Cryptiv. (n.d.). Retrieved from https://cryptiv.com/
Cryptocurrency Effects in Digital Transformations | Imperial College Business School. (n.d.). Retrieved from http://wwwf.imperial.ac.uk/business-school/research/innovation-and-entrepreneurship/ie-research/research-initiatives-and-themes/credit/
Cryptography, Security, and Privacy (CrySP) | SCS | UW. (n.d.). Retrieved from https://crysp.uwaterloo.ca/research/
Dan Boneh. (n.d.). Retrieved from http://crypto.stanford.edu/~dabo/
Decentral Consulting - Blockchain Consulting Services. (n.d.). Retrieved from http://decentral.ca/decentral-consulting/
Deloitte-Blockchain-Enigma-Paradox-Opportunity.pdf. (2016). Retrieved from http://bravenewcoin.com/assets/Industry-Reports-2016/Deloitte-Blockchain-Enigma-Paradox-Opportunity.pdf
Digital Certificates Project. (n.d.). Retrieved from http://certificates.media.mit.edu/
Digital Currencies, Digital Finance and the Constitution of a New Financial Order: Challenges for the Legal System. (n.d.). Retrieved from https://www.ucl.ac.uk/cles/research_initiatives/digital-currencies/events/material/digital-currencies-programme/
Digital Finance Initiative | Berkman Klein Center. (n.d.). Retrieved from https://cyber.law.harvard.edu/research/digital_currency#.
Distributed ledger technology: beyond block chain - Press releases - GOV.UK. (n.d.). Retrieved from https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain
Doguet, J. J. (2013). The Nature of the Form: Legal and Regulatory Issues Surrounding The Bitcoin Digital Currency Systems. *Lousiana Law Review*, *73*(4), 1119–153.
Dr. Debbie Maxwell - Publications - Research Database, The University of York. (n.d.). Retrieved from https://pure.york.ac.uk/portal/en/researchers/debbie-maxwell(5c60351c-3a8a-4fc4-86d1-4e6753962b5d)/publications.html
Dr. Gaby Dagher. (n.d.). Retrieved from http://cs.boisestate.edu/~gdagher/
DuPont, Q. (2014). The Politics of Cryptography: Bitcoin and The Ordering Machines » The Journal of Peer Production. *Journal of Peer Production*, (4). Retrieved from http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/
ECA, University of Edinburgh. (n.d.). Retrieved from http://www.designinaction.com/research/institution/eca/
Enigma. (n.d.). Retrieved from http://enigma.media.mit.edu/enigma_full.pdf.
Eskandari, S., Barrera, D., Stobert, E., & Clark, J. (n.d.). A First Look at the Usability of Bitcoin Key Management. Presented at the USEC 2015 Workshop, San Diego, CA: Internet Society. Retrieved from http://www.internetsociety.org/sites/default/files/05_3_3.pdf
Ethereum Foundation and Wanxiang Blockchain Labs announce a blockbuster event combining Devcon2 and the 2nd Global Blockchain Summit in Shanghai, September 19–24, 2016. (2016, April 5). Retrieved from https://blog.ethereum.org/2016/04/05/devcon2-and-blockchain-summit-shanghai-september2016/
European Securities and Markets Authority. (2016). *Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets* (pp. 1–34). Retrieved from https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf
Falcon - A Fast Bitcoin Backbone. (n.d.). Retrieved from http://www.falcon-net.org/
FC'16 : Financial Cryptography 2016. (n.d.). Retrieved from http://fc16.ifca.ai/
Fintech and Blockchain World Expo. (n.d.). Retrieved from http://www.fabexpo.ca/
Gipp, B., Meuschke, N., & Gernandt, A. (2015). Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. *arXiv Preprint arXiv:1502.04015*. Retrieved from http://arxiv.org/abs/1502.04015
Great Britain, & Treasury. (2015). *Digital currencies response to the call for information*. London: HM Treasury. Retrieved from

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf
Hanumanth K. Jayakumar | LinkedIn. (n.d.). Retrieved from https://www.linkedin.com/in/hanumanthk
Heilman, E., Baldimtsi, F., & Goldberg, S. (n.d.). Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. Retrieved from https://pdfs.semanticscholar.org/98a5/fb41d0842c3123268024682e43807291951a.pdf
Hengyi (Tony) Liu | LinkedIn. (n.d.). Retrieved from https://www.linkedin.com/in/hengyi-tony-liu-05242a76
Home of Aggelos Kiayias. (n.d.). Retrieved from http://www.cse.uconn.edu/~akiayias/Home_of_Aggelos_Kiayias/Home_of_Aggelos_Kiayias.html
IC3 About. (n.d.). Retrieved from http://www.initc3.org/about
IC3 Projects. (n.d.). Retrieved from http://www.initc3.org/projects
ICEIS 2017 - Home. (n.d.). Retrieved from http://www.iceis.org/
IEEE Symposium on Security and Privacy 2016. (n.d.). Retrieved from http://www.ieee-security.org/TC/SP2016/
Jeremy Clark. (n.d.). Retrieved from http://users.encs.concordia.ca/~clark/academic.php
Joseph Bonneau — index. (n.d.). Retrieved from http://jbonneau.com/
Kaitai Liang. (n.d.). Retrieved from http://users.ics.aalto.fi/ktliang/
Kalodner, H. (n.d.). Position Paper for W3C Blockchain Workshop. Retrieved from https://www.w3.org/2016/04/blockchain-workshop/interest/kalodner.html
Ledgers and Law in the Blockchain | King's Review – Magazine. (n.d.). Retrieved from http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain/
Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (n.d.). Making Smart Contracts Smarter. Retrieved from https://eprint.iacr.org/2016/633.pdf
Maryland Cybersecurity Center |. (n.d.). Retrieved from http://cyber.umd.edu/
Matteo Solinas - The Regulation of Distributed Ledgers. (n.d.). Retrieved from http://www.systemicrisk.ac.uk/sites/default/files/images/Matteo%20Solinas%20-%20RegulationDistributedLedger%20ok.pdf
MCIS 2016 – Mediterranean Conference on Information Systems. (n.d.). Retrieved from http://mcis2016.eu/
Media Lab Projects | Spring 2016. (n.d.). Retrieved from http://www.media.mit.edu/files/projects.pdf
MedRec. (2016, May 2). Retrieved from http://jods.mitpress.mit.edu/pub/medrec
Melbourne Money & Finance Conference 2016 - FinTech and Financial Innovation. (n.d.). Retrieved from https://business.monash.edu/acfs/events/melbourne-money-And-finance-conference-2016-fintech-and-financial-innovation
Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (n.d.). *Bitcoin and Cryptocurrency Technologies*. Retrieved from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf
NYU Stern - David Yermack - Albert Fingerhut Professor of Finance and Business Transformation. (n.d.). Retrieved from http://www.stern.nyu.edu/faculty/bio/david-yermack
NYU Stern | Event | New York Blockchain Workshop. (n.d.). Retrieved from http://www.stern.nyu.edu/experience-stern/news-events/new-york-blockchain-workshop
Open BlockChain. (n.d.). Retrieved from http://blockchain.open.ac.uk/
Parliament of Australia, (n.d.). Digital currency—game changer or bit player [text]. Retrieved from http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report
PETs 2016 The 16th Privacy Enhancing Technologies Symposium. (n.d.). Retrieved from https://petsymposium.org/
Philip Godsiff - University of Surrey - Guildford. (n.d.). Retrieved from http://www.surrey.ac.uk/sbs/people/philip_godsiff/
Prateek Saxena's Home Page. (n.d.). Retrieved from http://www.comp.nus.edu.sg/~prateeks/
Primavera De Filippi | Berkman Klein Center. (n.d.). Retrieved from https://cyber.law.harvard.edu/people/pdefilippi

Proceedings of the Standing Senate Committee on Banking, Trade and Commerce. (n.d.). Retrieved from http://www.parl.gc.ca/content/sen/committee/412/BANC/07EV-51307-E.HTM
ProvSec 2016. (n.d.). Retrieved from http://provsec2016.njue.edu.cn/
Quadriga to Launch First Canadian Blockchain R&D Lab | Business Wire. (2015, November 13). Retrieved http://www.businesswire.com/news/home/20151112006775/en/Quadriga-Launch-Canadian-Blockchain-Lab.
Quinn DuPont | Faculty of Information. (n.d.). Retrieved from http://current.ischool.utoronto.ca/students/quinn-dupont
R3 (company). (2016, July 18). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=R3_(company)&oldid=730365454
Research | Bill Maurer. (n.d.). Retrieved from http://faculty.sites.uci.edu/wmmaurer/research/
Research into Currencies | University of Cumbria. (n.d.). Retrieved from http://www.cumbria.ac.uk/research/centres/iflas/research-into-currencies/
Research : Steve Huckle : University of Sussex. (n.d.). Retrieved from http://www.sussex.ac.uk/profiles/307882/research
RUBIX - Build Great Decentralized Applications. (n.d.). Retrieved from http://rubixbydeloitte.com/applications.html
Saito, K. (n.d.). Position Statement by Kenji Saito. Retrieved from https://www.w3.org/2016/04/blockchain-workshop/interest/saito.html
Sarah Jane Hughes : Faculty and Staff of Indiana University Maurer School of Law. (n.d.). Retrieved from http://www.law.indiana.edu/about/people/bio.php?name=hughes-sarah-jane#profile-works
Security and Privacy of Bitcoin. (n.d.). Retrieved from http://www.syssec.ethz.ch/research/Bitcoin.html
Seed Funding 2016. (n.d.). Retrieved from http://networkedsociety.unimelb.edu.au/research/seed-funding-2016
Services - Ledger Labs. (n.d.). Retrieved from https://ledgerlabs.com/services/
Sorrell, W. H., General, A., & General, V. O. A. (2016). Blockchain Technology: Opportunities and Risks. Retrieved from http://bitcoin-reg.com/sites/default/files/blockchain_technology_opportunities_and_risks_0.pdf
Standing Senate Committee on Banking, Trade and Finance. (2015). *Digital Currency: You Can't Flip This Coin!* Retrieved from http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf
Student project: Bitcoin and block chain for physical computing : Department of Computer Science, University of Oxford: (n.d.). Retrieved from https://www.cs.ox.ac.uk/teaching/studentprojects/469.html
Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution*. Portfolio.
Technologies de confiance et société ouverte: blockchain, fab lab et badges numériques | LCA UQAM. (n.d.). Retrieved from http://www.lca.uqam.ca/2016/03/technologies-de-confiance-et-societe-ouverte-blockchain-fab-lab-et-badges-numeriques/
UCD Home: The UCD Centre for Innovation, Technology & Organisation. (n.d.). Retrieved from http://www.ucd.ie/cito/
UniHallers Win $5000 Grant | UniHall - UWA. (n.d.). Retrieved from http://www.unihall.uwa.edu.au/news/unihallers-win-5000-grant/
UTS: ICI Creative Clusters - Blockchain | University of Technology Sydney. (n.d.). Retrieved from http://www.uts.edu.au/about/faculty-law/events/uts-ici-creative-clusters-blockchain
Weber, W. E., & others. (2016). *A Bitcoin Standard: Lessons from the Gold Standard*. Bank of Canada. Retrieved from http://www.bankofcanada.ca/wp-content/uploads/2016/03/swp2016-14.pdf
Welcome – iPRES 2016 - 13th International Conference on Digital Preservation. (n.d.). Retrieved from http://www.ipres2016.ch/frontend/index.php?folder_id=349
Welcome to the MIT Media Lab, Gavin, Wlad and Cory — MIT Media Lab Digital Currency Initiative — Medium. (n.d.). Retrieved from https://medium.com/mit-media-lab-digital-currency-initiative/welcome-to-the-mit-media-lab-gavin-wlad-and-cory-977ae418c084#.2r2066woh
What we do – Digital Finance Institute. (n.d.). Retrieved from http://www.digitalfinanceinstitute.org/?page_id=892.
Willms, J. (2015, April 27). Canada Takes a Careful, Community-driven Approach to Bitcoin Regulation.

Retrieved from https://bitcoinmagazine.com/articles/canada-takes-careful-community-driven-approach-bitcoin-regulation-1430166629

Blockchain Technology for Recordkeeping

The Preservation of Digital Signatures on the Blockchain

A Background Paper "Blockchain Technology for Recordkeeping – Help or Hype?" a SSHRC Knowledge Synthesis Grant Study on "How can emerging technologies be leveraged to benefit Canadians?"

Prepared by: Stephen Thompson, Masters of Library Information Studies Student for Principal Investigator Dr. Victoria L. Lemieux

The University of British Columbia, Vancouver, BC, V6T 1Z1
Phone: 604 822 2404
E-Mail: vlemieux@mail.ubc.ca

Table of Contents

INTRODUCTION **79**
SOME DEFINITIONS **80**
WHAT ARE DIGITAL SIGNATURES? **80**
HOW DO DIGITAL SIGNATURES WORK? **81**
PUBLIC KEY INFRASTRUCTURES (PKIS) **81**
CERTIFICATION AUTHORITIES: THE TRUSTED THIRD PARTY **82**
CAVEATS WITH DIGITAL SIGNATURES ON PKIS **82**
HOW DOES THE BLOCKCHAIN PRESERVE DOCUMENTS? **83**
COMPARISONS BETWEEN THE BLOCKCHAIN AND PKIS **85**
CONCLUSION **86**
REFERENCES **86**

Introduction

The digitization of records has had a profound effect on the way in which records managers notarize and store them. In the paper records environment, the author of the record would state his ownership of the document, or an agreement articulated on the document, by signing his name to it. From the records manager's perspective, the document is the property of the person who signed it and its signature is synonymous with that

document.
With the advent of the digital record, we now have the "digital signature" and central to the concerns of the archivist is the preservation of these signatures. The process of creating them will be discussed later in this paper as will the advantages and limitations of the public key infrastructures (PKIs) that have been the established repository for the storage of the signatures. The paper will go on to compare them with the architecture around the blockchain's handling of the signatures. The ultimate question that this paper will ask is whether the blockchain is a sounder platform for the preservation of digital signatures than the PKIs.

Some Definitions

Given that this section is an analysis of signatures generated on the blockchain, it is correct to refer to them as "digital" signatures rather than "electronic". Zooming out to the level of records, this digital-only approach is informed by the new CGSB standard, on electronic records as documentary evidence, which distinguishes digital records from electronic records: electronic records refer to any machine-readable record whether it was created digitally or through analogue means, whereas digital records are those that consist of "discrete binary values aggregated into one or more bit stream" (CGSB 72.34-2015, 0.1). Returning to signatures, the electronic signatures are not necessarily encrypted. However, digital signatures are created in the digital environment to provide a layer of validation for public key encryption databases.
So, it is through the questions into the preservation of digital signatures that the blockchain comes into the discussion. But, first, it will be instructive to examine the academic discourse into digital signatures and then the preservation thereof during the period up until the advent of the blockchain.

What are Digital Signatures?

A digital signature is a mathematical calculation that validates and authenticates the bitstream of a document at a certain point in time. It is designed to guard against the tampering and forging of an identity in digital communications (Rouse, 2014a, para. 1).

The academic community has been discussing the methods and systems by which archival institutions can verify and authenticate the electronic records in their archive. They agree that the prime purpose of digital signatures is to ensure that the documents in question have been authenticated (Boudrez, 2007, p. 180); Blanchette, 2006, p. 70 & 2012, p. 1).

Digital signatures have these key characteristics:

- They are based on *public-key cryptography* (Blanchette, 2006, p. 72),
- They are accepted as *legal evidence* (Blanchette, 2012, p. 1),
- They provide *authenticity* for a document during its transfer from one digital space to another digital space (Blanchette, 2012, p. 5),
- Unlike written signatures, digital signatures do not prove the identity of the signatory. But they do provide authentication of the document's *bitstream* in that the sender has encrypted it with his public key and the receiver decrypts it with his private key (Boudrez, 2007, p. 183),

- Bitstream authentication supposes that *the individual and his private key are linked* (Blanchette, 2006, p.72 & 2012, p. 1; Boudrez, 2007, p. 184),

- They are *non-repudiable* because they not only preserve the integrity of the document but state that Alice and Bob were the only counterparties and that only they could have produced their respective signatures (Blanchette, 2006, p. 72; CGI, 2004, p. 11; Buldas et al., p. 4),

- The cryptographic signatures mitigate any attempts to alter the *integrity* of a document after it has been signed (Blanchette, 2006, p. 73; Boudrez, 2007, p. 180; Lemieux, 2016).

How do Digital Signatures Work?

In explaining how digital signatures work, we should draw attention to the fact that the counterparties sign a document directly. The structure differs from that of the blockchain where the counterparties sign a hash that represents the document.

We will refer to asymmetric or "public key" cryptography which involves an interaction between public and private keys. The public key is stored on a server accessible to other users on the network (more on that below) while the private key remains a secret.

Public key cryptography operates under a dual procedure on which signatures form a part. Assuming there are two parties, each party possesses a key pair: the public and private keys. To use Blanchette's crypto-couple analogy (2006, p. 1), Alice and Bob are fellow archivists about to manage the transmission of a document. Alice is about to send a document to Bob across the network. Before she does so, Alice encrypts the document with Bob's public key. Alice sends it across and, then, Bob decrypts the file with his private key. For the signature, the roles are reversed: Alice encrypts that same *document* with her private key and then sends it to Bob. Bob decrypts it with both his private key and Alice's public key. If he decrypts it successfully, Bob can then verify that Alice was the sender.

The resulting digital signature is intended to be available for anyone to verify the identity of the party that signed the document i.e. Alice. (In this first case, Bob and, in subsequent cases, by third parties such as a notary.) The document, standing as a new file, should state that it has been verified. From the point-of-view of an archivist, the signature is *genuine* in that it is what it claims to be, and it is *authentic* in that the elements that are required for that authenticity are present (Duranti, 1989, p. 17).

Public Key Infrastructures (PKIs)

PKIs can come in the form of key management servers or centralized directories. They combine software with a management process that, according to the CGI's 2004 White Paper (2004, p. 10-11) on public key encryption, covers the following operations:

- *the creation of the key pair* – Pedro (2015, p. 53) used the analogy of keys unlocking a safe. The private key unlocks the safe while the public key locks the safe. In order to decrypt Alice's document, Bob creates a private-public key pair by running a key generation algorithm from the PKI,
- *creation of digital certificates* – certificates verify the digital signature by displaying the link between Alice and her public key. In those systems that issue certificates, the signature is known as a "qualified digital signature". They produce the validity period, the signature algorithm, a serial number and the

name of the certification authority (Boudrez, 2007). These validity periods can be of a long duration and they also rely on the sustained readability and integrity of the signatures (Gladney, 2007, p. 170)

- *private key protection* – in key pairings, the private key is encrypted while mathematically linked to the public key which is unencrypted (Pedro, 2015, p. 53). Despite being linked, it is computationally infeasible to deduce the value of the private key from the value of the public key (Gladney, 2007, p. 168),
- *certificate revocation in the event of a compromised private key* – once a user's certificate has been revoked, the PKI must preserve the certificate on a database accessible to all users in the network so that it cannot be re-used. This attempts to deal with a problem that Kohnfelder (1978, p. 16) identified: a public file encryption function has a single point of failure. Once breached, the attacker can pass encryption functions that are bogus. He also stated that updating such a large system would be expensive and inefficient.
- *private key backup and recovery* – if the user loses his private key, any files encrypted with that key will be lost. So, the PKI needs a backup and recovery mechanism for lost private keys,
- *key and certificate update* – this is a mechanism for the renewal of expiring digital certificates. The PKI achieves this by carrying out the renewal automatically or notifying the user to carry out an operation that updates the certificate himself. Blanchette (2012, p. 77) stated that the idea behind fixed expiry dates is to mitigate against incremental damage to the network's integrity due to corrupted public keys,
- *key history management* – following a key update that generates new key pairs, history management makes it easier for the user to determine which private key to use for decrypting files,
- *certificate access* – the White Paper suggested an LDAP directory for convenient access to certificates.

One can see from here that PKIs require the preservation of at least three components: key pairs, active digital certificates and revoked digital certificates.

Certification Authorities: The Trusted Third Party

One operation within the PKI system which deserves a mention is the administration of the Certification Authority (CA). CAs are a type of "trusted third party" (TTP) which deliver validation authority for a PKI (Black & Layton, 2014, p. 13). PKIs assume the presence of CAs in that the users of the network store their public key with the CA which they recognise as a trusted third party that can vouchsafe the public key on its server. CAs verify the identity of each user and sign their public keys. So, in Alice and Bob's exchange of signatures, Alice is presenting her CA certificate, with the signature and public key both embedded, to Bob (Pedro, 2014, p. 55). So, what is meant by a TTP? TTPs have been defined as a "secure middle layer on (cloud) service transactions" (Stamou et al., 2013, p. 4976), they allow the secure, trustful, interaction between two parties (p. 4979). TTPs can be public sector organizations, such as the NSA and GCHQ, or they can originate from the private sector e.g. GlobalSign, Symantec and Comodo.

Caveats with digital signatures on PKIs

TTPs as a central point of failure

Users store their signatures with a TTP because they trust the integrity of the organization. Most of these TTPs are centralized. They stand as a "central point of failure" (Allen et al., 2015, p. 2) and therein lies many of the risks in storing signatures on a centralized platform owned by an organization:

- ownership of key pairs becomes ambiguous once entrusted to a TTP (Allen et al., 2015, p. 2);
- they are not bound to conform with national or international legislation (Stamou et al., 2012, p. 4981);

- neither are they obliged to enforce their own security policies (Stamou et al., 2012, p. 4981);
- leading on from that, it is difficult to control the internal governance of a TTP and to compel them to offer external ports in their systems or to submit accurate logs on a user's request (Stamou et al., 2012, p. 4981)

So, the users' digital signatures and key pairs rest on "trusted third parties" that operate under minimal legal enforcement.

Digital signatures validate and sign the bitstream of a document, not the document itself

(OCLC/RLG Working Group, 2002; Boudrez, 2007, p. 183)

As an example, a *fond* contains a video of an event in the 'wmv' format but the archivist converts it to an 'mp4' so it could be viewable across a wider range of platforms. The signature verifies the bitstream of the 'wmv'. However, should the archivist believe that the content of the video of the event had been digitally signed and proceeds with an attempt to authenticate the 'mp4' with the same signature that had come with the 'wmv' file, the authentication will fail.

Verification is not protection

The digital signature does not prove the integrity of the digital record. It only proves whether or not the digital document had been altered post-verification: verification does not prevent the alteration from taking place. This is why encryption is required when using digital signatures. Also, it only verifies a document at the point of transfer and not at any time thereafter (Boudrez, 2007, p. 183, citing National Archives Australia).

New signatures required for file conversions

With each data migration or file format conversion, a digital archivist will need to generate a new set of signatures to authenticate the digital transfer. The dilemma this creates for the archivist is whether to preserve only the originating signature set or to archive them as a validation chain in a parallel repository that can capture future signatures generated over time (Boudrez, 2007, p. 186-7). And, should the archivist decide to archive them, would he build it internally or would he migrate them to an external server? If he enacts the former solution, he will create an extra layer of digital archiving but would maintain control over the signatures. If he enacts the latter, he can upload them to a PKI solution but lose direct control.

How does the blockchain preserve documents?

The main archiving strength of the blockchain is that hash values generated will be preserved on the blockchain for as long as the blockchain continues to operate.

There are major differences between the purpose and application of signatures in a conventional, centralized, PKI and the purpose and application of signatures in the blockchain (a type of distributed PKI). In the blockchain, the document is one component while the hash value replaces the signature as the principal authenticating agent.

Hashing

There are two components to hashing:

- the *hash function* is a hexadecimal algorithm, such as SHA-2, that maps an input data of any size into a uniform, usually compressed, file size;
- the *hash value* is the output of a specific length that permanently identifies the input data (Pedro, 2015, p. 95).

The hash function is a one-way process: this means that the user can create the hash from input data but not use the hash to reveal the data. This is a key feature of proof-of-work (Pedro, 2015, p. 96). Should a records manager alter even one digit from the input data and then try to apply the same hash function, he will generate a completely different hash value (Pedro, 2015, p. 97).

This is a form of document authentication where, instead of digitally signing the document directly, a hash function generates a hash value to confirm that the authentication had taken place. Returning to our crypto-couple's document transfer, Alice authenticates the document not by signing it but by generating the hash

value. That hash value is broadcast to the blockchain so as to confirm that the transfer of the document had taken place. These hash values have a number of advantages:

- they can confirm the creation of content bundles such as datasets, degree certificates and ID management;
- they can authenticate that same document (as long as it has not been altered) at a time in the future (Lemieux, 2016). For example, should the document become an exhibit in a court of law;
- they can be stored privately and separately from the application that generated the hash value (Pedro, 2015, p. 99);
- the hash is a smaller file size than the input data and so can be stored more easily (Pedro, 2015, p. 99).

Proof-of-work

This refers to the computational problem-solving process that the 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 (Pedro, 2015, p. 102). Proof-of-work utilises 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, in our Alice and Bob transfer, is a proof-of-work that the document has been authenticated.

Proof-of-stake

The users prove their commitment to a transaction by "minting" i.e. publishing, blocks in proportion to the quantity of coins they hold, as opposed to mining them. This does not require nearly as much computational power as mining and so is more environmentally friendly than the proof-of-work function. Other advantages of proof-of-stake are that the activity is open to all stakeholders on the network and, because of the lower computational power required, the transaction fees are lower (Pedro, 2015, p. 235).

There is disagreement, however, about the risk of centralization. Pedro argued that as there is wider participation among the users, proof-of-stake is less susceptible to centralization. Bentov et al. (2014, p. 34) countered that proof-of-stake would place amateur minters in a conflict of interest against professionalized miners. Bentov expected the miners to prevail and then make centralizing moves to consolidate their control over the network.

Proof-of-concept

A *proof-of-concept* is a documentation of evidence that proves the viability of a project which is then hashed to the blockchain (Rouse, 2014b, para. 1). This proof-of-concept can come in the form of web traffic or transaction volumes. In the context of a blockchain project, the entrepreneur will build a solution, gather supporting datasets, then hash the sets and broadcast them to the blockchain.

In the context of digital preservation, Peter van Garderen stated that cryptographic hash functions are used for the production of proof of a digital action that is unique, which means there is no identical hash. In the action of hashing a document and then recording the hash to the blockchain, the archivist has created a *proof-of-concept* (Van Garderen, 2016).

Specialized signatures

The blockchain community have conceived an array of signatures that utilise the hashing process in a way that can solve various issues, mainly concerning space. I will run through those that would be most relevant to a records manager:

- *Elliptic Curve Digital Signature Algorithm (ECDSA)* – ECDSA combines elliptic curves (a public key family) with the DSA digital signature and, together, form the signature scheme used in Bitcoin (Pedro, 2015, p. 70). The feature that would be of interest to an archivist looking for an efficient preservation strategy is that there is no need to store the public key as it can be hashed repeatedly in the future (Lemieux, 2016).
- *Schnorr signatures* - this is an overriding signature that hashes a cluster of signatures in order to remedy file storage issues. So, if a *fond* contains thirty documents each with their own signature, the archivist can sign the entire *fond* with a Schnorr signature. He would reduce the filesize from 2400 bytes (80 bytes per signature) back to 80 bytes. The cryptography community approves of them because of their

speed, simplicity and strong security (van Wirdum, 2016, para. 14; Allen, 2015, para. 3). Some in the Bitcoin community have called for Schnorr signatures to become the standard (Pedro, 2015, p.58). This can be a useful signature and one that will be simple to preserve for new *fonds* that contain a large number of documents.

Timestamping

A timestamp proves that a certain dataset existed at a certain point in time (Pedro, 2015, p. 99). The blockchain method creates timestamped blocks through peer-to-peer technology, therefore disintermediating Time Stamping Authorities (TSAs). Miners on the Bitcoin blockchain timestamp each block which contains ten minutes' worth of transactions. The miners are, effectively, operating as a distributed TSA. This means that there is no need for periodic re-timestamping of signatures due to expiring keys. According to Guardtime, in the promotion of its new BLT algorithm, the time and integrity of the signature can be proven mathematically without reliance on the security of keys or of trusted parties (Guardtime, 2016).

The time it takes for a TSA to verify a transfer is measured in seconds whereas the blockchain's verification takes minutes (Amati, 2016, para. 23). Amati went on to state these key advantages that blockchain timestamping has over TSA timestamping:

- Long-term preservation can be achieved without the maintenance costs that come with a TSA-issued certificate (Amati, 2016, para. 24),
- Archivists can exploit the convenience of verifying the signature with the document and public key without having to safeguard the digital signature on a central server (Amati, 2016, para. 25).

Comparisons between the blockchain and PKIs

Above, we discussed how PKIs combine digital certificate administration with key management. The preservation of digital signatures on the blockchain network has a different architecture and a different purpose. It has been argued that the blockchain is gradually becoming recognized as a viable solution for the professional need for trusted digital records and public registration systems in general (Lemieux, 2016).

Certification – The Bitcoin blockchain is a PKI that neither issues digital certificates nor operates through a CA. Blockchain technology does not require a digital certificate for its users to trust the integrity of the network because the blockchain miners have already verified the transfer of digital value.

Decentralization – returning to the point about PKIs and the potentially serious issue of the 'single point of failure', the server room or the cloud can be seen as the 'single point of failure' that Kohnfelder was alluding to. The main advantage that a digital signature database on the blockchain network has over databases on centralized systems is the act of distributing a blockchain-based PKI infrastructure across a range of computers, or nodes. This decentralized structure enhances the longevity of the network because duplicates of the blocks, on which the signatures are stored, are so numerous (Findlay, 2015, para. 22). The decentralization of the blockchain gives it a further advantage in that no third party can alter or erase the transactions stored in the blocks without undoing the proof-of-work requirement that had verified them (Findlay, 2015, para. 13).

Distributed consensus – thousands of computers located around the world, known as 'nodes', verify each transaction by authenticating the digital signatures *en masse*: they reach consensus about the integrity of each transaction. This process is an element of the decentralized nature of the blockchain and some have argued that it gives the blockchain more integrity than authentication by a single CA (Lea, 2016). Amati stated three complementary positives of the blockchain's consensus on signatures:

- All agree on the latest signatures,
- We are seeing the same signatures,
- No-one can alter the signatures (Amati, 2016, para. 30).

So, instead of relying on a central authority to certify a document's authenticity, the blockchain can assert proof of its authenticity through cryptographic confirmation. This dynamic can empower many archive managers to establish their own records systems backed by the assurance and longevity of the distributed

blockchain network (Findlay, 2015, para. 14).
Notarization – a notary is a trusted authority that verifies or authenticates a transaction and the users in the network place trust in that notary that it will store, securely, the data in question (Economist, 2015, para. 7). A CA is a type of notary for key pairs. In the blockchain, a distributed consensus on the blockchain can take on notarial operations from trusted authorities (Li, 2016, para. 11).
Privacy – the encryption in the blockchain's distributed network offers strong security and privacy when verifying signatures. The way privacy differs on the blockchain from that of a PKI is that despite the public nature of the transactions and value balances, the counterparties behind the transactions remain private (Pedro, ch.13, p. 209). So, the blockchain record will say that Bitcoin address x sent a specified amount of digital value to Bitcoin address *y*. However, the more frequently they use the same Bitcoin addresses for future transactions, the further their privacy erodes. For example, an agent will be able to establish relationships between Bitcoin addresses. So, the question of privacy on the blockchain depends on the diligence of the counterparties to create new addresses per transaction. Pedro's chapter 13 (pp. 209-229) offers a full discussion about the privacy issue.
Independent of file format – a digital archive should ensure that its authentication system is neutral of file format. This reduces the problem of relying on applications that transfer data, proprietary or open-source, becoming obsolete (Findlay, 2005, para. 13).

Conclusion

This chapter has assessed public key infrastructures and then surveyed the features of the Bitcoin blockchain. The answer to the question as to whether a blockchain-powered PKI offers better signature preservation strategies than CA-controlled PKIs depends on what metadata the information professional selects for archival storage and the duration of the retention/disposition schedule. Boudrez (2007, p. 190) said that records of the validation metadata can replace that of the digital signature for those digitally-signed records which have a permanent retention period. So, blockchain adoption may be more advantageous to records with a permanent retention schedule. This is because the hash value, a feature particular to the blockchain, stands as validation metadata that would not require particular software for its future verification. Furthermore, the blockchain record does not require a centralized party, such as a CA, to notarize or validate the hashes – unless the records management utilises sidechains and third-party notaries such as Factum.
Developments in the Ethereum blockchain offer a point of entry for the information profession at a lower cost than the Bitcoin blockchain. The proof-of-stake versus proof-of-work conflict that I mentioned above will have a different outcome for decentralized networks. In the case of a large blockchain network such as Bitcoin where hashing power for block creation requires the corporatization of miners, Bentov's scenario of proof-of-work dominating the network is most likely to play out. However, in these emerging, decentralized blockchains where mining is still accessible to the user community, such as Ethereum, Pedro's optimism for the benefits of proof-of-stake can hold.
The blockchain offers exciting options for information professionals. In the case of metadata preservation, they will need to decide on what should be preserved: the digital signatures or the hashes. However, the library, archival or records management communities should wait before adopting blockchain systems now that the infrastructure is going through transitions. This is even more the case given that this July (2016) alone has seen the Halving and the hard fork on the Ethereum blockchain. The blockchain community has yet to see the consequences of these developments.

References

Allen, C. (2015, October 9). Schnorr signatures: An overview. *WebOfTrustInfo*. Retrieved from

https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/topics-and-advance-readings/Schnorr-Signatures--An-Overview.md.

Allen, C., Brock, A., Buterin, V., Callas, J., Dorje, D., Lundkvist, C., Kravchenko, P., Nelson, J., Reed, D., Sabadello, M., Slepak, G., Thorp, N. & Wood, H. T. (2015). *Decentralized public key infrastructure. A White Paper from Rebooting the Web of Trust*. Retrieved from https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf

Amati, F. (2016, January). Using the blockchain as a digital signature scheme. Medium blog. Retrieved from https://blog.bitcourt.com/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826#.a4i6eqmoz.

Anon. (2015, October 31). The trust machine: The promise of the blockchain. *The Economist*. Retrieved from http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

ANSI X9.95-2012. Trusted time stamp management and security. Retrieved from https://www.sec.gov/rules/proposed/s72703/iac120105.pdf.

Bentov, I., Lee, C., Rosenfeld, M. & Mizrahi, A. (2014). Proof of activity: Extending Bitcoin's proof-of-work via proof-of-stake. [Extended Abstract] *Performance Evaluation Review*, 42 93), 34-37.

Blanchette, Jean-François. (2012). *Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents*. Cambridge: The MIT Press.

Blanchette, Jean-François. (2006). The digital signature dilemma. *Annales des Telecommunications*, 61(7), pp. 908-923.

Bitcointalk.org. Retrieved from https://bitcointalk.org/index.php?topic=101514.0

Black, P. & Layton, R. (2014). *Be careful who you trust: Issues with the Public Key Infrastructure*. 2014 Fifth Cybercrime and Trustworthy Computing Conference. IEEE Computer Society. Retrieved from https://www.researchgate.net/publication/282936649_Be_careful_who_you_trust_Issues_with_the_public_key_infrastructure

Blockchain.info. Retrieved from https://blockchain.info.

BlockNotary. Retrieved from https://www.blocknotary.com/

Boudrez, F. (2007). Digital signatures and electronic records. *Archival science*, 7(2), pp. 179-193.

Buldas, A., Laanoja, R. & Truu, A. (2014). *Efficient implementation of keyless signatures with hash sequence authentication*. [Unpublished paper.] Retrieved from https://eprint.iacr.org/2014/689.pdf.

CGI (2004). *Public key encryption and digital signature: How do they work?* White Paper. Retrieved from www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf.

Clanchy, M. T. (2013). *From memory to written record: England 1066-1307*. Chichester, John Wiley & Sons Ltd.

CGSB 72.34-2015, 0.1. Electronic records as documentary evidence. Personal communication of draft by e-mail.

Cumming, K. & Findlay, C. (2016). Report on blockchain: Applications and implications. *Recordkeeping Roundtable*. Retrieved from https://rkroundtable.org/2016/04/03/report-on-blockchain-applications-and-implications/.

Curry, I. (2001, March). An introduction to cryptography and digital signatures. Entrust. Retrieved from https://www.entrust.com/wp-content/uploads/2013/05/cryptointro.pdf

Duranti, L. (1989). Diplomatics: New uses for an old science. *Archivaria*, 28, pp. 17-27.

Findlay, C. (2015). Decentralised and inviolate: the blockchain and digital archives. Retrieved from https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.

Garderen, P. van. (2016, May 17). Blockchain and digital preservation. Presentation at Simon Fraser University [Video file]. Retrieved from https://www.youtube.com/watch?v=S2N0m9YDgZw.

Gladney, H. (2007). *Preserving digital information*. Berlin, Heidelberg: Springer.

Guardtime. Retrieved from https://guardtime.com/blt-technology.

ISO 16363:2012. Space data and information transfer systems – Audit and certification of trustworthy digital repositories. Geneva: ISO. Retrieved from

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542.

ISO 15489-1:2016. Information and documentation – Records management – Part 1: Concepts and principles. Geneva: ISO. Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542.

ISO/TR 18492:2005. Long-term preservation of electronic document-based information. Geneva: ISO. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38716.

Kohnfelder, L. (1978). *Towards a practical public key cryptosystem.* Bachelor's degree thesis. Retrieved from http://groups.csail.mit.edu/cis/theses/kohnfelder-bs.pdf.

Lea, T. (2016). Introductory course – The power of the blockchain. What is blockchain? Retrieved from https://www.youtube.com/watch?v=KXC9hyB09pk

Lemieux, V. (2016). Trusting records: Is blockchain technology the answer? *Records Management Journal*, 26(2), pp. TBA.

Li, V. (2016, March). Bitcoin's useful backbone: Blockchain technology gains use in business, finance and contracts. *ABA Journal*, 102(3), p.31. Retrieved from http://www.abajournal.com/magazine/article/bitcoins_underlying_technology_blockchain_gains_use_in_business_finance_and

OCLC/RLG Working Group. (2002, June). *Preservation metadata and the OAIS Information Model: A metadata framework to support the preservation of digital objects*. Retrieved from http://www.oclc.org/content/dam/research/activities/pmwg/pm_framework.pdf.

Pedro, F. (2015). *Understanding Bitcoin: Cryptography, engineering and economics*. Chichester: John Wiley & Sons Ltd.

RFC 3161. (2001, August). Internet X.509 public key infrastructure time-stamp protocol (TSP). Retrieved from http://www.rfc-base.org/txt/rfc-3161.txt.

Rouse, M. (2014a). Digital signature. *SearchSecurity.TechTarget*. Retrieved from http://searchsecurity.techtarget.com/definition/digital-signature.

Rouse, M. (2014b). Proof of concept (POC). *SearchSecurity.TechTarget*. Retrieved from http://searchcio.techtarget.com/definition/proof-of-concept-POC.

Ruggieri, F. (2014). Security in digital data preservation. *Digital Evidence and Electronic Signature Law Review*, 11, pp. 100-106.

Stamou, K., Aubert, J., Gateau, B., Morin, J-H. (2012). *Preliminary requirements on trusted third parties for service transactions in cloud environments*. 2013 46th Hawaii International Conference on System Sciences. Institute of Electrical and Electronics Engineers, 4976-4983.

Wirdum, A. van. (2016, April 14). The power of Schnorr: The signature algorithm to increase Bitcoin's scale and privacy. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496

Blockchain Technology for Recordkeeping

Recordkeeping on the Blockchain

A Background Paper "Blockchain Technology for Recordkeeping – Help or Hype?" a SSHRC Knowledge Synthesis Grant Study on "How can emerging technologies be leveraged to benefit Canadians?"

Prepared by: Jessica Tung, Masters of Archival science and Library Information Studies Student for Principal Investigator Dr. Victoria L. Lemieux

The University of British Columbia, Vancouver, BC, V6T 1Z1
Phone: 604 822 2404
E-Mail: vlemieux@mail.ubc.ca

Table of Contents

INTRODUCTION **89**
METHODOLOGY AND APPROACH **90**
RECORDS AND RECORDKEEPING SYSTEMS **91**
THE BLOCKCHAIN **93**
PROPOSED AND CURRENT SERVICES **95**
RECORDS AND RECORDKEEPING ON THE BLOCKCHAIN **97**
CONCLUSION **99**
REFERENCES **100**

Introduction

An increasingly large fraction of our lives are lived out in the digital realm and it is a legitimate concern that facts are recorded and preserved in a manner that ensures not only their long-term security but also their accessibility. There has been much discussion concerning the Bitcoin network and its underlying technology, the blockchain, but little on the emerging projects that offer what would be considered traditional recordkeeping services. Due to its reputation as "trustless" and "immutable," early adopters are currently using the blockchain protocol in a range of circumstances – contract exchange, financial intermediation, or document verification— requiring digital interaction or exchange of data. The initial and now famous application of blockchain technology Bitcoin has given way to applications that rely upon Distributed Ledger Technologies (DLTs) and its decentralized network as their operating system. At the crux of this movement is

ultimately trusting the decentralized network of the blockchain, thus eliminating the need for any trusted third party to verify a transaction or any documentary by-products thereof. It is thus critical to examine the blockchain considering the central role of trust in recordkeeping systems and recognize that there remain risks to be contained and questions to be answered in relying upon this technology to secure records and to assert their integrity.

Ensuring that the records embedded on the blockchain are reliable and authentic is critical as they are primary means upon which current organizations base their blockchain services. As records are accepted in our society in the legal framework as evidence of an act (Bearman, 1993), and serve for the purpose of memory and accountability (MacNeil, 2001), there must be means to ensure that the recordkeeping system in which they are retained is trustworthy and will continue allowing access to those records to serve the needs of the people or organizations that created or received them. The blockchain's transparent, distributed ledger and its decentralized nature—with no central system or government regulating it—has given way to surprisingly innovative projects that rely heavily upon the trustworthiness of the system and of the records it holds and maintains.

For example, *Genecoin* offers to have your DNA sequenced, hashed, and embedded on the Bitcoin blockchain, proving that you exist and to "propogate your DNA far and wide" ("Genecoin.me," 2016, n.p.). A Brooklyn resident successfully used the Ethereum blockchain to sell excess green energy generated from home solar panels directly to his client (del Castillo, 2016). Last year, music artist Imogen Heap wrote about her decision to release her album through the blockchain in an endeavour to handle payments to collaborators and to receive instant artistic royalties for downloads (Resnikoff, 2015). Four banking companies and a distributed ledger company used *smart contracts* to execute successful credit swaps on the blockchain, demonstrating one of blockchain's most discussed potentials: the "ability to reduce costs of keeping track of securities" (Kar, 2016, para. 4). These are only a few examples of the new capabilities that blockchain technology is being tested for and why some enthusiasts are predicting it to be "the most disruptive force since the Internet" (Di Iorio, 2016, para. 2).

Methodology and Approach

This paper seeks to explore the possibilities of the blockchain as a recordkeeping system that creates and maintains trustworthy records. It offers a brief overview of the landscape surrounding blockchain solutions for record keeping issues and what companies are proposing for blockchain services. It begins with a discussion of trustworthy records and recordkeeping systems through an archival lens which will set the backdrop for a comparison of blockchain technologies and traditional recordkeeping services. Identifying the components of electronic records will provide a basis on which to recognize records that are made or received in recordkeeping systems, and will allow a means for discussing trustworthiness of those records.

The paper examines how organizations plan to offer blockchain services to counter the idea of a centralized system in favour of decentralized, distributed, and cryptographic systems. It will be followed with a consideration of how e-notary services are presented in order to illustrate how the concept of records and record-keeping is being affected by these blockchain services. In order to illustrate the potential that blockchain has to offer and its impact on trustworthy records, it is important to understand what the blockchain is, how the blockchain functions, and how it is promoted as a trustless and immutable technology. There remain risks to be examined and assuaged before blockchain technology can be relied upon to secure records.

Records and Recordkeeping Systems

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. 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 (Duranti, 2007). 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.

In archival science, a *record* is any document 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 (InterPARES 2 Terminology Database, 2016). In the electronic 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 intelligible 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 and ultimately determines if the record is probative, dispositive, narrative or supporting; *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.

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. *Trustworthiness* in archival theory encapsulates the concepts of accuracy, reliability and authenticity of a record and is intertwined with the concepts of identity, integrity and provenance. *Accuracy* points to the degree of precision and exactness of data in a record; *authenticity* refers to the quality of a record that it is what it purports to be and that it is free from tampering or corruption; and *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 (InterPARES 2 Terminology Database, 2016). *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. Provenance essentially dictates that records are to be understood with reference to their origins in activity, and thus is an indicator of the trustworthiness of the record (InterPARES 2 Terminology Database, 2016).

Recordkeeping systems and Trusted Digital Repositories are necessary for the preservation of and access to digital records. With the ubiquity of digital records in the 21st century, there is still room for development in the criteria against which the trustworthiness of a repository can be evaluated. These criteria for technology will evolve as the digital records become more dynamic and fluid, and their communities change. 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" (InterPARES 2 Terminology Database, 2016)· A *trusted recordkeeping system* can then be considered "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" (InterPARES 2 Terminology Database, 2016). Through an archival perspective and particularly in diplomatics, guaranteeing reliability is inextricably linked to methods of record creation while authenticity is linked to the record's mode, form and state of transmission, and to the manner of its preservation and custody (MacNeil, 2001).

A trusted recordkeeping system must be able to prove that its records meet the *authenticity requirement*—being able to establish complete elements of form and context that need to be preserved in order to maintain the authenticity of an electronic record. The results of IP2 led to the development of Principles for Records Creators, outlining recommendations for record creation in the digital environment in order that reliability, accuracy, and authenticity of digital records can be established and demonstrated over time, ultimately supporting accountability and evidentiary needs. Principle C6 notes that "every recordkeeping system should include in its design a recordkeeping metadata scheme, a classification scheme, a retention schedule, a registration system, a recordkeeping retrieval system, recordkeeping technological requirements, recordkeeping access privileges and procedures for maintaining accurate and authentic records" (Duranti & Preston, 2008, p. 34-35).

ISO 30300:2011 will also be useful in examining blockchain technology, specifying fundamentals and vocabulary concerning a Management Systems for Records (MSR). The standard defines *evidence* as documentation of a transaction (ISO 30300, 2011, 3.1.5), *record(s)* as information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business (ISO 30300, 2011, 3.1.7), and *records system* as an information system which captures, manages and provides access to records over time (ISO 30300, 2011, 3.4.4). ISO 30301:2011 follows with requirements a MSR must meet to support an organization in being accountable for and transparent with its records practices and ISO 30302:2015 provides guidelines for its implementation. These standards provide a methodology for a systematic approach to records creation and management, and establish the objectives for using record keeping systems. Effectively implemented and well-designed MSRs will ensure that authoritative and reliable information about, and evidence of, business activities are created, managed and made accessible to those who need it for as long as required.

If the blockchain is considered to serve a recordkeeping role in the accumulation and preservation of electronic records, the technology itself must be a "trusted custodian in a preservation environment that maintains the digital files, manages required migration, and records archivally relevant metadata" (Duranti & Franks, eds., 2015, p. 119). The blockchain must also be able to authenticate each record upon its introduction to the system (Duranti & Franks, eds., 2015). Standards such as ISO 30300:2011 and the IP2 guidelines will certainly pose limitations on the blockchain as a long-term solution for maintaining accessible trustworthy digital records. Furthermore, the blockchain, serving a recordkeeping purpose for certain organizations will be assessed for those specified requirements particularly when disputes arise concerning their records. The *Canada Evidence Act*, for example, requires proof of "the integrity of the electronic documents system by or in which the electronic document was recorded or stored" in order for e-records to be admissible as evidence (S. 31.2(1)(a) Canada Evidence Act, RSC 1985, c C-5). Ken Chasse (2014) argues that standards such as *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 are critical in assessing integrity of any electronic records management system, but since there is "no law of general application requiring institutional ERMS's be attained in compliance with [the standard], defects that can interfere with the existence, accessibility, and integrity of e-records are very numerous and very common" (p. 25). Indeed, in any recordkeeping and records-

creating system, the integrity of the records will depend entirely upon and requires proof of the record system's own integrity.

The Blockchain

The blockchain is a digital distributed transaction ledger made possible because thousands of different computers, called *nodes*, cooperate together as a system to store the sequences of bits that are encrypted as a single unit (a block), which are then chained together to form the blockchain. The Bitcoin blockchain establishes a distributed public ledger that contains the payment history of every bitcoin in circulation. The ledger is viewable by anyone participating in the blockchain and this ensures that there is proof of bitcoin ownership at any given juncture, avoiding the possibility of double-spending. "Bitcoin," with capitalization, is used when describing the concept of the entire network of Bitcoin, a technology. "bitcoin" however, is Bitcoin's cryptocurrency, and the blockchain is used as a public record of Bitcoin transactions in chronological order ("Vocabulary - Bitcoin," n.d.). In simplest terms the blockchain is a record of all transactions that have occurred on the Bitcoin network since its conception (Kelly, 2014). When people refer to transactions on the blockchain as being transparent, they are referring to the public ledger or list of all transactions which everyone on the blockchain network accepts as the authoritative record of ownership. This distributed database is only possible due to the nodes of the network that ultimately publish the anonymous yet verified transactions to the public ledger (Antonopoulos, 2014). There is no central authority; rather, there is an assemblage of nodes that deploy cryptographic hashes on the blockchain and validate previous transactions.

The blockchain is increasingly being considered as a solution to the challenges of trustworthy digital recordkeeping, particularly in the case of systematic records attestation. The interest in blockchain technologies has been widespread not only among technology enthusiasts but also among professional record keepers and governments as well. In April 2015, the European Commission launched a "5 Million EUR call aiming at the development of a distributed platform for decentralized data, identity management and bottom-up participatory innovation," ("EU call for proposals," 2016, n.p.) and this past April, the French government legalized the use of blockchain's distributed ledger technology, defining it and acknowledging it as a documentation tool to authenticate the transfer of ownership (Ngo, 2016). The statute is the first of its kind, and having blockchain defined in French law "as a shared electronic recording system allowing for authentication" is a significant step towards recognizing that blockchain technology has the potential to change the course that digital commerce will take and perhaps towards a more technology-based, decentralized economy ("Rapport au President de la Republique..." n.d., n.p.).

A force in decentralizing data governance, the blockchain was to be found primarily in the context of financial disintermediation with Bitcoin. However, with the power of the internet, blockchain technology is being used by organizations increasingly in verification services of records. Since these projects focus largely on the blockchain as distributed ledger technology in a recordkeeping role, defining electronic records and trust and identifying the components of a record will help establish reliability and authenticity of such records. Projects hoping to take advantage of blockchain technology mean new innovations and potential applications will affect a range of sectors in the economy and the social and everyday activities that previously required a centralized system or organizations to function as authoritative points of control (Antonopoulos, 2014). Ensuring the trustworthiness of both the blockchain system and the documented information contained therein is a crucial requirement if users are depending upon it to record and secure their digital interactions.

Blockchain technology is being explored for its recordkeeping potential particularly because it has the ability to create units of digital information that cannot be duplicated. Trusted records are particularly important given

enthusiasm for blockchain technology as a permanent distributed ledger of records of transactions and its promise for the attestation of any digital asset. Noting the high stakes for regulators, financial institutions, and governments, authors of *The Blockchain Revolution* proclaim that "for the first time ever, we have a platform that ensures trust in transactions and much recorded information no matter how the other party acts" (Tapscott & Tapscott, 2016, p. 33).

With so much being explored about blockchain as a trustless, secure technology, with its immutable blocks of recorded transactions, it is important how trusting in this technology comes about. In order to verify transactions across the blockchain network, the blockchain requires a consensus mechanism. For the Bitcoin blockchain, the consensus mechanism is "proof of work," when miners use computer power to solve a mathematical puzzle. The software code essentially gathers up all the transactions in a certain amount of time, which becomes a block, and broadcasts transactions to all computers on the network (Kelly, 2014). The successful miner is the one who solves the puzzle and then broadcasts its "proof-of-work" to the network. Other miners essentially compare the data from the underlying transactions to the hashed data within it so as to verify its legitimacy and check it against the history in the blockchain, creating an "inviolable realm of transparency" (Vigna & Casey, 2015, p. 220). The consensus mechanism is run and that block is added to the blockchain, and the miners restart their puzzle-solving again.

Ethereum is considering use of an alternative consensus method, called "proof of stake." It is an algorithm that depends upon cryptocurrency holdings of the node and not its computational resources. The validators place in a "security deposit" over which the protocol has direct control; if nodes on the network behave unpredictably in validating a transaction, they forfeit their deposit or "stake" (Zamfir, 2015). This gives incentive for miners to serve the consensus, and not to bet against it. Proof of stake is argued to be more sustainable and secure than proof of work, as transactions are confirmed based on current information of the nodes (Larimer, 2015). Mining is essentially the "main process of the decentralized clearinghouse, by which transactions are validated and cleared…[it] secures the [system] and enables the emergence of network-wide consensus without a central authority" (Antonopoulos, 2014, p. 176).

At the core of the blockchain technology is calculating cryptographic hash functions. *Hashing* is running a computing algorithm over any content file (a document, a GIF file, a video, a genome file) which results in a compressed string of alphanumeric characters that cannot be retroactively computed into the original contents. Because the blocks are always calculating hash functions that are unique, the code ensures that there are no changes to a transaction and any attempt to change what has already been published to the blockchain would be competing with a network of peer-to-peer nodes that are constantly updating. This is why the blockchain is considered to have an immutable chain of transactions—because each block is a referent to the previous block and to its hashes. There is an inevitable "cascade effect" which "ensures that once a block has many generations following it, it cannot be changed without forcing a recalculation of all subsequent blocks" (Antonopoulos, 2014, p. 162). A recalculation would be close to impossible due to the computation power it would require; the existence of innumerable transactions and blocks "makes the blockchain's deep history immutable...a key feature of bitcoin's security"(Antonopoulos, 2014, p. 162). It can be described as an "accumulate-only file system," writes Alan Morrison (2015), senior research fellow at PwC, Center for Technology and Innovation, who argues that blockchain technology is testament to the "rise of immutable stores of data"—a trend toward abandoning the traditional method of overwriting mutable files, a process found in relational databases.

The append-only feature of the blockchain translates to the ideas of security and permanence, and the proof of work and verification stages contribute to the verification of transactions. The blockchain's functionality is thus perceived as "a global ledger of truthful information [which] can help build integrity into all our institutions and create a more secure and trustworthy world" (Tapscott & Tapscott, 2016, p. 11). While traditionally society

relies upon intermediaries or organizations assuming to act with integrity, the blockchain can function to eliminate all trusted third parties during business transactions. Digital conglomerates and intermediaries such as Google, Apple, Visa, PayPal all power and drive online commerce but in a blockchain world, "trust derives from the network and even from objects on the network...the ledger itself is the foundation of trust" (Tapscott & Tapscott, 2016, p. 11).

Proposed and Current Services

The blockchain is attracting areas wherein a distributed consensus system is required, including fair voting systems, asset registration, stock ownership, and notarization. Land-title registration has already been attempted in Honduras using blockchain technology and an e-proxy voting system has been developed in Russia as well ("Russia's Securities Depository System..." 2016). Acronis is a Singapore-based data storage and security vendor that is testing blockchain technology for their data protection services, and in particular to "monitor data integrity and guarantee validity at all times" ("Acronis Blockchain Technology Initiative" 2016). Indeed, it seems possible that "[b]lockchain-based systems can infuse efficiency and integrity into document registries of all kinds and many other government processes" ((Tapscott & Tapscott, 2016, p. 205). Technological controls are clearly taking over areas where procedural controls for making and maintaining records were once commonplace, perhaps due to the powers of computers and of the internet, and the excess of information needing to be managed. However, employing the blockchain as with all systems necessarily involves risks surrounding organizational control, record reliability and authenticity, long-term digital preservation, and monetization.

The blockchain has also been considered a decentralized archive. It is being used as a site of data storage when digital assets are hashed and embedded upon the blockchain. A record of that hash can then be validated by running a search of the hash, using a blockchain explorer, any time in the future. Due to this capability, companies are leveraging the blockchain in order to verify that hashed record's existence. The blockchain thus is hailed as a revolutionary way by which organizations not only generate various types of digital records (by hashing them), but also by which these records can then be stored on the blockchain, securing them against hacking and fraud. Using digital signatures, hash functions, and relying public key cryptography, blockchain services allow users to transmit units of value, transact chunks of digital information, or sign contracts that are executed on the blockchain, all allegedly efficiently and securely. This in turn, generates new and different records directly on the blockchain. In effect, the blockchain is being proposed as a storage solution for any type of record.

If you are the first to make a product—whether it is artwork, software, or a line of poetry—you can embed its hash on the blockchain and you will have proof of it because it is considered registered, and stored on the blockchain. Organizations adopting the blockchain hope to offer trustworthy registration and verification services for a user's intellectual property; a user can create a hash of any digital asset, anchor it onto the blockchain and have a timestamp affixed to it. In this way the blockchain is used analogous to Copyright, which requires—when disputes surface—documentary proof of creator and date of creation. Blockchain companies providing this service essentially provide users with a certificate that acts as proof that the hash of their digital asset is embedded onto the blockchain and affixed with a timestamp. Companies *Proof of Existence* and *Blocksign* are only two examples among various others that utilize this functionality of registration on the blockchain. The services use time-stamped, hashed data to maintain confidentiality for various applications. They use the capacity of a cryptographic hash to be inserted into a transaction, which is then mined into a block, and the block timestamp becomes the document's timestamp. Via the hash the record's content essentially is encoded into the blockchain, where its blockchain's network members act as witnesses. These services allow users to prove exact contents of a digital asset at a certain time through comparison of the original hashes of a digital asset (The LTB Network, youtube).

Furthermore, much of the hype of blockchain applications also converges on its ability for a certification of authenticity. However, to be *legally authentic* a document must be attested by an appropriate authority. Thus, it is legally authentic in that its *validity* is confirmed. The blockchain is being used as a substitute for notarization services. Notarization services establish the authenticity of an asset by verifying the identity of the person signing it. This process of signing and establishing authenticity are how blockchain companies are leveraging the technology's reputation as a trustworthy ledger. A *notary* or *notary public* as defined by Black's Law Dictionary as "a person authorized by a state to administer oaths, certify documents, attest to the authenticity of signatures, and perform official acts in commercial matters, such as protesting negotiable instruments" (*Black's Law Dictionary* 7th ed., 1999, p. 867). Although many services claim to replace the function of the public notary, many of the e-notary companies using the blockchain explicitly state that their jurisdictions have not yet recognized their services as legally authorized to notarize 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. VN's aim is to "provide a digital, neutral, dispassionate witness for recording online facts and conveying them to third parties in a trustworthy manner" (Sirer, n.d.), allowing users to demonstrate that they possessed a specific document, picture or recording at a certain date. Without storing files, VN simply provides a cryptographically protected certificate that attests to the file's contents at the moment of submission. It is a virtual notary service for various file types: documents, web pages, twitter feeds, stock prices. You can examine existing certificates, which contain full details so that "the provenance of the data can be traced back to the original source" (Sirer, n.d.). However, VN's website fully admits that it is not recognized in any jurisdiction by the legal system as a notary public, but emphasizes that its certificates can serve as trustworthy evidence in the same capacity.

Blockchain services such as the above take advantage of the blockchain's ability to use cryptographic hashes as a "permanent" and public way to record and store information. In the future users can find what they have previously stored by providing the blockchain with a reference point, or with a block explorer and a blockchain address pointer. The blockchain is perceived by these services as a budding universal central repository, where core functionality is its ability to verify a digital asset via a public general ledger, distributed on computers across the world. A general consensus among blockchain enthusiasts is that the technology "offers a way of recording transactions of any digital interaction in a way that is designed to be secure, transparent, and highly resistant to outages, auditable, and efficient" (Schatsky & Muraskin, 2015). The argument goes that if the proof of signature is not controlled by any single entity, the blockchain services and its records can be trusted. The positions of these organizations is that "[a] few thousand blocks back...and the blockchain is settled history" (Antonopolous, 2014, p. 162), and privacy too is ensured since the data placed in it is in the form of a one-way hash and indecipherable. Nodes and miners act as public notaries who confirm the users' uploads and these blockchain-based notary systems are deemed as solutions to an expensive and ineffective infrastructure for notarization and transferring documentation. Notably, the UK government is already looking into the use of the blockchain in the maintenance of digital records, and for maintaining integrity of these records (Spaven, 2015).

The blockchain can also be used to "combine supply chain management with the Internet of Things to tag a new piece of equipment with a smart chip that communicates its provenance, ownership, warranties, or special information" (Tapscott & Tapscott, 2016, p. 205). It is unsurprising then that the concept of provenance is embraced by blockchain enthusiasts due to the hype surrounding the distributed ledger's transparency and openness. *Provenance.org* is a noteworthy platform using the blockchain to offer services that build a reputation for clients. By tracing the origins of products and providing reliable customer information for their manufacture, *Provenance* hopes to resolve product traceability issues through the blockchain's "transparency movement." 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 ("Provenance For Non-Profits," n.d.). "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 ("How Provenance is Channeling..." 2015).

Furthermore, at the crux of many of these blockchain services is the concept that *smart contracts* can replace the legal system as being the ultimate trusted third-party. Smart contracts are event-driven programs that are attached to a transaction and stored on the blockchain; they are coded directly on a transaction specifying the use, timing and parties in the transaction (Kelly, 2014). As part of the growing blockchain ecosystem, smart contracts would mean that no law firm has to draft a written agreement to be enforced by a judge; the execution of any obligations of the first party is automated by software and leverages the distributed software, and the criteria for doing so is verified by the decentralized blockchain. The idea is that any certification of ownership, such as deeds, titles, tangible or intangible assets can be put into digital form, hashed, and then acted upon by software. These assets become "smart property" whose ownership can be both established and then stored on the blockchain for future verification and validation (Kelly, 2014, p. 157). Smart contracts allow for the automatic transfer of ownership of these electronic records once contractual obligations are met, and efficiency is achieved with blockchain-approved transfers.

Ethereum, "the world's second most valuable cryptocurrency network after Bitcoin" (Seaman, 2016) is making headlines while it makes changes to the blockchain architecture through the deployment of these smart contracts. Ethereum is developing a blockchain and a language that hopes to allow any user to build smart contract applications that will execute on its platform (Antonopolous, 2014). Using a built-in currency called *ether*, Ethereum is developing to be like an "app store" of the digital world (Kelly, 2014, p.156), aiming to decentralize existing services and systems altogether. With Ethereum, you would be able to control accounts, money, and do operations like any program; the critical selling point of Ethereum seems to be that they do operations autonomously, allowing everyday people who are not coding experts to use the blockchain to facilitate peer-to-peer exchanges, distributing and decentralizing assets into communities. Ethereum highlights how the applications that run on its blockchain will always execute reliably without the need for a trusted third party.

Records and Recordkeeping on the Blockchain

There is little discussion of the recordkeeping capacity of the blockchain. Electronic records must have their integrity intact so they can be consulted as evidence of the transactions they document. Electronic records are kept precisely because they not only contain useful information as evidence of a transaction, and with proper recordkeeping systems these records can also be maintained as evidence over time (Bearman, 1993). With blockchain services drawing upon records for their evidentiary and documentary value, a review of the blockchain as a trusted recordkeeping system will be important. Traditional electronic recordkeeping systems are typically dependent for functioning on the hardware and software in which they were implemented (Bearman, 1993), which makes the distributed ledger system of the blockchain unique. However, we have to consider who writes the codes that run on the platforms, what rules are being executed without an operator, and with whom does accountability lie when disputes arise concerning the records registered or created on the blockchain.

As the recent DAO "hack" on the Ethereum blockchain exemplifies, the trusted technology and smart contracts are not so much immutable but calls the security and trustworthiness of the blockchain into question. The attacker(s), who drained an account of its entire ether fund, simply "exploited software vulnerability" ("Understanding The DAO Hack," 2016, n.p.). It is a reminder that the security of the system is wholly dependent upon the network of users in conjunction with the strength of the written code that underlies the technology. The rules of the technology and thus any accountability are baked directly into the code that the blockchain executes. Andreas Antonopoulos, Bitcoin and blockchain expert, admits that "[a] decentralized system like bitcoin pushes the responsibility and control to the users" (Antonopolous, 2014, p. 233). "Users" include not only users in the network, but the coders and miners who run the consensus mechanism. The security system the

blockchain is built upon depends heavily upon the consensus mechanism and not access controls. It is the miners who ultimately decide which direction to take with the distributed ledger, which also challenges the suggestions made of democracy on the blockchain.

IP2 's Principle C6 suggests that recordkeeping systems should be designed to include:a recordkeeping metadata scheme, a classification scheme, a retention schedule, a registration system, a recordkeeping retrieval system, recordkeeping technological requirements, recordkeeping access privileges and procedures for maintaining accurate and authentic records (Duranti & Preston, 2008). Taking into consideration the IP2 principles, the blockchain falls short in more than one area, which is problematic as a trusted recordkeeping system should be used to maintain records that can be presumed accurate and authentic. To increase the probability of a record's trustworthiness, we have to look to the procedural controls exercised during the recordkeeping process on the blockchain: classification, registration, imposition of access privileges, maintenance of audit trails, use of continuous monitoring, and perpetual assessment (Macneil, 2004). In terms of records creation, the hash of the record becomes a referent of the data being embedded onto the blockchain. *Integrity*, which is the quality of being complete and unaltered in all essential respects, along with *identity*, are components of the authenticity of a record (InterPARES 2 Terminology Database, 2016). Record integrity is established and maintained through identifying the responsibility for the record through time by "naming the handling person or office(s) and the trusted records officer or the recordkeeping office, identifying access privileges and access restrictions and indicating any annotations or any modifications (technical or otherwise) made to the record by the persons having access to it" (Duranti & Preston, 2008, Principle C4). Metadata describe context, content, and structure of records and their management through time and are necessary in assessing authenticity of records (ISO 1549-1, 2001, definitions 3.12). In terms of metadata, the structure of the blocks comprising the blockchain does capture transaction metadata, particularly in the block header. Examples of what is captured include a reference to the previous block hash, information regarding the mining competition: *difficulty*, *timestamp*, and *nonce*, an also a hash of the merkle tree root (Antonopolous, 2014). IP2's essential metadata includes *identity metadata,* which includes among others, the names of the persons involved in the creation of the digital materials, a subject or title, documentary form, and digital presentation—all integral to maintaining and assessing trustworthiness of records. Also essential are *integrity metadata*, including names of the handling person or office, access restriction or privilege code(s), and planned disposition. It is unlikely that the block identifiers, including block header hash and block height are sufficient to meet these essential metadata standards, especially given the size limits placed on blocks. Also, it is unclear whether it is possible to locate a record using this metadata through the available block explorers, and whether protocols can be designed to capture more useful metadata without increasing block size, while retaining privacy, and without compromising security.

Blocks are data containers of aggregate transactions, and since they are explicitly ordered by reference to previous block hashes (Antonopolous, 2014), the concept of the archival bond could be said to be reasonably expressed by the records on the blockchain in the sense that transaction order is captured. However, it is unclear how a classification scheme could be implemented, how classification of records belonging in the same aggregation would be carried out by the blockchain, or how a record's network of relationships could be reflected in the unique hash that is embedded (Antonopolous, 2014). Furthermore, without the ability to classify groups of records belonging to the same aggregate, it is retention schedules become problematic. Perhaps with smart contracts certain records transactions can execute autonomously, but as a "permanent" storage mechanism the blockchain does not allow for disposition. What it does allow for, as previously discussed, is registration of a digital asset. However, hash algorithms are one-way and irreversible; it is not possible to decipher the original contents of the record from a hash or to remove them from a block. Blockchain services can effectively provide record registration, time-stamping, and verification services, but the data itself as unintelligible without the original file, document, or asset—thus functions solely as a referent for the original. Moreover, retrieval of the records embedded on the blockchain will need further exploration. Block explorers can provide information on blocks, addresses, and transactions, but there seems to be no easy way to navigate hashes unless you have either the original block hash, the age of the transaction, the block height,

the address of the sender or receiver, or some other useful statistical information that uniquely identifies the block you are searching for. Records cannot be easily retrieved, and it remains to be seen how powerful block explorers can be, what features they will offer in terms of privacy and access privileges and restrictions, how they are designed, and who will lead their development. This leads to the question of whether the blockchain is a sustainable storage solution for these hashes of data. Companies claim to use blockchain technology and hashing algorithms to establish "archival" permanence but the significant cost of computational power is not compensated by the system, and for the distributed ledger to remain truly "distributed," users will increasingly need significant amounts of memory on their computers in order to own a copy of the current blockchain. This issue is often referred to as blockchain "bloat" (Wagner, 2014), when the size of the network grows so large with its transactions that the ledger may not be sustained by every user. Due to the computation power or cryptocurrency required for the verification process— the potential for digital preservation, long-term storage, and even "immutability"—will always be dependent upon and relative to this computer power and the availability of miners on the network. We have to consider if the recordkeeping technological requirements outlined in IP2 principles are met and if computational power or proof-of-stake consensus affects auditability and registration times, and examine if and how the records will be securely accessible over time.

Blockchain Revolution discusses that "the blockchain technology functions well as a regulator in as itself" (Tapscott & Tapscott, 2016, p. 13) and that "we need institutions that act with integrity, security, privacy, inclusion, rights protection, and distributed power" (p. 308). However, the incentive to confirm transactions on blockchains will be problematic in ensuring trustworthiness of records. What is the incentive for network miners to verify transactions that they are not part of? What will be the consensus mechanism that helps blocks aggregate transactions and embeds data on to the blockchain? The consensus protocols require trusting the peer-to-peer network and the code written to run the blockchain, and users who decide to upload their personal data are essentially agreeing to the rules of the network rather than the law. If the blockchain is to be considered a trusted custodian for records its protocols must be able to establish maximum degree of control with regard to the maintenance and use of records. It must be evaluated with standards such as ISO 30300:2011 to measure the level of business risk of having inadequate records controls, if the blockchain meets legislative regulatory, and accountability requirements, and will it provide protection and support in litigation, including the management of risks associated with the existence of or lack of evidence of organizational activity.

While transactions are highly irrevocable on the blockchain, which increases the probability that records are complete and reliable, the irreversibility has implications for recordkeeping. Even without a central host and resistant to outages through a central server, the distributed nature of the ledger and append-only feature of the blockchain also means that any personal data contained on the blockchain cannot be removed. Ownership and creatorship too is not proven; the registration functionality that the blockchain is being used for does not discriminate and means there could be an arms race: the first to upload and embed a certain hash is ultimately the first to register and "authenticate" it as theirs on the blockchain. This cannot be undone and it remains to be seen if the platform can balance privacy and control unauthorized access to information—with the ideas of transparency and usability.

Conclusion

At a minimum, electronic recordkeeping systems create, store, disseminate, and retrieve records (Bearman, 1993). Recordkeeping systems provide organizations with evidence of business transactions where non-record information systems store information in discrete chunks that can be recombined and reused without reference to their documentary context (Bearman, 1993). In this sense perhaps the "ledger of things" (Tapscott & Tapscott, 2016, p. 152-159) functions analogously to a powerful database to which people across the globe contribute data via different services and applications. The distributing power of blockchain technology, however, comes with the issues of obfuscation on the blockchain and being able to extract intelligible and trustworthy

information in order to put it to good use. The current lack of interoperability of the different blockchain platforms will be of concern in the future since users will have to choose which system through which to embed their data. Interoperability also raises concerns data integration and being able to monitor the information when there is a lack of blockchain and data management standards. Though, there is optimism that the energetic "adoption of blockchain technology [could] actually become an accelerator in the ISO adoption process" ("Blockchain: Infrastructure, Protocol, Content - Blog," n.d., n.p.) and lead to agreements for a data governance metadata framework.

Momentum is certainly growing for the adoption of blockchain services. While the technology promises to combat the reliance on centralized services, it is still certainly the case that users may eventually need to rely back on centralized services, such as the court, for disputes. Digital currency regulation will continue to be controversial and the possibility of regulation is stifled by what makes the blockchain so popular and strong: the fact that its existence is owed to the millions of computers that are distributed across local and international borders (Kelly, 2014). And while the dream of a self-regulated market rests on the agreed-upon defined mathematical code and consensus system that runs the system, the blockchain surely cannot "address the problem of human greed and deceit" (Kelly, 2014, p. 139). Thus, the promises of the blockchain in reducing costs, removing centralization, transforming auditability, and promoting transparency—will be supported by those who trust in the technology and the codes written to run it. Blockchains and platform software will not only need to be designed with privacy in mind, but they will also need to weigh in on accountability with the longevity of the platform, and its significant dependencies upon miners, consensus validation, and computation power to create useable, reliable and ultimately trustworthy records.

References

Acronis Blockchain Technology Initiative. (n.d.). Retrieved from http://www.acronis.com/en-us/business/blockchain-notary/

Anthony Di Iorio. (n.d.) "The Blockchain Is Transforming Finance." *The Blockchain Is Transforming Finance - Industry and Business*. Retrieved from http://www.industryandbusiness.ca/development-and-innovation/the-blockchain-is-transforming-finance.

Antonopoulos, Andreas M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc.

ARMA International Standards Development Committee. (2007) "Glossary of Records and Information Management Terms." *US, ARMA International*.

Bearman, D. A. (1993). Record-keeping systems. *Archivaria*, *1*(36).

Black's Law Dictionary 7th ed. (1999), Bryan A. Garner, editor. West Group.

"Blockchain: Infrastructure, Protocol, Content - Blog." (n.d.). *Sapient Global Markets*. Retrieved from https://www.sapientglobalmarkets.com/blog/blockchain-infrastructure-protocol-content.

"BlockSign." (n.d.). Retrieved July 8, 2016 from https://blocksign.com/.

Chasse, Ken. (2007). "Electronic Records as Documentary Evidence." *Canadian Journal of Law and Technology* 6: 141.

Chasse, Ken. (2014). "Electronic Records as Evidence." Retrieved from http://ssrn.com/abstract=2438350

del Castillo, Michael. (April 11, 2016). "Ethereum Used for 'First' Paid Energy Trade Using Blockchain Tech." *CoinDesk*. Retrieved from http://www.coindesk.com/ethereum-used-first-paid-energy-trade-using-blockchain-technology/.

Di Iorio, Anthony. (2016). "Blockchain? What you need to know." Retrieved from http://www.pressreader.com/canada/national-post-latest-edition/20160623/282510067863814

Duranti, Luciana & Franks, Patricia C. eds. (2015). *Encyclopedia of Archival science*. Rowman & Littlefield.

Duranti, Luciana. (2002). "The concept of electronic record." *Preservation of the integrity of electronic records*, pp. 9-22. Springer Netherlands.

Duranti, L. and Preston, R. (2008). *International research on permanent authentic records in electronic systems*

(InterPARES) 2: Experiential, interactive and dynamic records (pp. 34-35). CLEUP.
Duranti, Luciana. (2002). "The Reliability and Authenticity of Electronic Records." *Preservation of the Integrity of Electronic Records*, pp. 23-30. Springer Netherlands.
"EU call for proposals for developing blockchains and decentralised data architectures." (n.d.). Retrieved from http://ec.europa.eu/newsroom/itemdetail.cfm?item_id=28275.
"Genecoin." (n.d.). Retrieved July 8, 2016 from http://www.genecoin.me.
"How Provenance Is Channeling the Blockchain for Social Good." (n.d.). *CoinDesk*. Retrieved from http://www.coindesk.com/provenance-channeling-blockchain-social-good/.
InterPARES 2 Terminology Database. http://www.interpares.org/ip2/ip2_terminology_db.cfm
Kar, Ian. (n.d.). "The DTCC and 4 Top Banks Used Blockchain Tech to Trade Credit Swaps." *Quartz*. Retrieved from http://qz.com/656959/the-dtcc-and-4-top-banks-used-blockchain-tech-to-trade-credit-swaps/.
Kelly, Brian. (2014). *The Bitcoin Big Bang: How alternative currencies are about to change the world*. John Wiley & Sons.
Larimer, Daniel.(August 8, 2015). "Review of Casper, Ethereum's Proposed Proof of Stake Algorithm." *Bytemaster's Blog*. Retrieved from http://bytemaster.github.io/2015/08/08/Review-of-Casper-Ethereums-proposed-Proof-of-Stake-Algorithm/.
MacNeil, H. (2001). Trusting records in a postmodern world. *Archivaria*, 36-47.
Morrison, Alan. PricewaterhouseCoopers. (n.d.). Technology Forecast: The rise of immutable data stores. Retrieved from http://www.pwc.com/us/en/technology-forecast/2015/remapping-database-landscape/immutable-data-stores--rise.html
Ngo, Diana. (n.d.). "France Issues New Ruling for Mini-Bonds Trading on Blockchain Platforms." Retrieved from https://btcmanager.com/news/finance/france-issues-new-ruling-for-mini-bonds-trading-on-blockchain-platforms/.
"Proof of Existence."(n.d.). Retrieved July 8, 2016 from https://proofofexistence.com/about.
"Provenance | Building Trust in Great Businesses and Products." (n.d.). *Provenance*. Retrieved from https://www.provenance.org/.
Rapport au Président de la République relatif à l'ordonnance no 2016-520 du 28 avril 2016 relative aux bons de caisse. https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000032465510
Resnikoff, Paul. (October 5, 2015). "I'm Imogen Heap. And This Is Why I'm Releasing My Music on Blockchain." *Digital Music News*. Retrieved from http://www.digitalmusicnews.com/2015/10/05/im-imogen-heap-and-this-is-why-im-releasing-my-music-on-blockchain/.
"Russias Securities Depository Successfully Tests Blockchain-Based E-Proxy Voting System." (April 29, 2016) *EconoTimes*. Retrieved from http://www.econotimes.com/Russias-Securities-Depository-Successfully-Tests-Blockchain-Based-E-Proxy-Voting-System-202270.
Schatsky, David & Muraskin, Craig. (December 7, 2015). "Beyond Bitcoin: Blockchain Is Coming to Disrupt Your Industry." *Deloitte University Press*. Retrieved July 8, 2016 from http://dupress.com/articles/trends-blockchain-bitcoin-security-transparency/.
Seaman, David. (July6, 2016). "Why Corporations Love Ethereum." *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/david-seaman/why-corporations-love-eth_b_10849632.html
Spaven, Emily. (September 1, 2015). "UK Government Exploring Use of Blockchain Recordkeeping." *CoinDesk*. Retrieved from http://www.coindesk.com/uk-government-exploring-use-of-blockchain-recordkeeping/.
Tapscott, Don, & Tapscott, Alex. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.
The LTB Network. (December 12, 2013). *Block-Chain Notary Service, ProofOfExistence.com*. Retrieved from https://www.youtube.com/watch?v=6YHiuZeWyrE.
Vigna, Paul & Casey, Michael J. (2015). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*. St. Martin's Press.
"Vocabulary - Bitcoin." (n.d.). Retrieved from https://bitcoin.org/en/vocabulary.
Wagner, Andrew. (November 6, 2014). "Ensuring Network Scalibility: How to Fight Blockchain Bloat." *Bitcoin*

Magazine. Retrieved from https://bitcoinmagazine.com/articles/how-to-ensure-network-scalibility-fighting-blockchain-bloat-1415304056.

Zamfir, Vlad. (August 1, 2015). "Introducing Casper 'the Friendly Ghost.'" *Ethereum Blog*. Retrieved from https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.

Appendix B – Blockchain Terminology

TRUSTER Preservation Model (EU31)

Proposal of the blockchain-related terminology for the InterPARES Trust Terminology database

This draft terminology report is based on the analysis of the final consultation draft of the project "Blockchain Technology for Recordkeeping: Help or Hype?", a SSHRC Knowledge Synthesis Grant Competition on "How can emerging technologies be leveraged to benefit Canadians?" led by principal investigator Victoria L. Lemieux, and other relevant literature.

Date submitted:		10 October 2016
Author:		InterPARES Trust Project
Writer(s):		Ph.D. Hrvoje Stancic, assoc. prof. GRAs: Andro Babic, Nikola Bonic, Magdalena Kules, Ira Volarevic PhD students: Vladimir Bralic, Anabela Lendic, Ivan Slade Silovic Faculty of Humanities and Social Sciences, University of Zagreb, Croatia

Document Control

Version history			
Version	Date	By	Version notes
0.1	10 October 2016	Ph.D. Hrvoje Stancic, assoc. prof.	draft for consideration

Contents

BITCOIN 106
BLOCKCHAIN RECORDKEEPING 107
CERTIFICATION AUTHORITY 108
CRYPTOCURRENCY 109
CRYPTOGRAPHIC HASH FUNCTION 110
DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO) 111
DIGITAL MONEY 112
DISTRIBUTED CONSENSUS 114
DISTRIBUTED LEDGER 115
ELECTRONIC EVIDENCE 116
ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) 117
ETHEREUM 118
EVERLEDGER 119
FACTOM 120
FORK 121
HARD FORK 122
INSTITUTIONAL-BASED TRUST 123
MINER 124
MULTISIGNATURE 125
NODE 126
NOTARIZATION 127
PEER-TO-PEER PAYMENT 128
PROOF-OF-CONCEPT (POC) 129
PROOF OF STAKE 130
SCHNORR SIGNATURES 131
SIDECHAIN 133
SMART CONTRACT 134
SMART PROBATE 136
SOFT FORK 137

TIMESTAMP **138**
TRUSTED THIRD PARTY (TTP) **139**
TRUSTLESS TRANSFER **140**
VIRTUAL CURRENCY **141**

BITCOIN

Syndetic Relationships
RT: cryptocurrency
RT: blockchain
RT: distributed ledger
RT: virtual currency
RT: digital money

InterPARES Definition
n. ~ a (→) cryptocurrency based on (→) distributed ledger technology.

General notes
–

Citations
Parliament of Australia 2015, p. 12: Launched in 2009, Bitcoin was the first decentralised convertible digital currency and the first cryptocurrency.
http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report
Grewal-Carr, Marshall 2016, p. 6: In his original Bitcoin white paper, Satoshi Nakamoto defined an electronic coin – the Bitcoin – as "a chain of digital signatures" known as the 'blockchain'. The blockchain enables each coin owner to transfer an amount of currency directly to any other party connected to the same network without the need for a financial institution to mediate the exchange.
http://bravenewcoin.com/assets/Industry-Reports-2016/Deloitte-Blockchain-Enigma-Paradox-Opportunity.pdf

BLOCKCHAIN RECORDKEEPING

Syndetic Relationships
RT: recordkeeping system

InterPARES Definition
n. ~ the use of blockchain as a technology to store records of hashes such as ledger entries

General Notes
With its origins as a cryptocurrency, it may not be obvious that blockchain technology is fundamentally about recordkeeping as well. However literature synthesis confirmed the original supposition that it is, indeed, a recordkeeping technology by nature.

Citations
Deery 2016: 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
http://www.the-blockchain.com/2016/05/07/blockchain-future-business-records-brian-deery-chief-scientist-factom-inc

CERTIFICATION AUTHORITY

Syndetic Relationships
RT: TTP (trusted third party)
RT: PKI (Public Key Infrasctructure)

InterPARES Definition
n. ~ a type of "trusted third party" (TTP) which delivers validation authority for a PKI; responsible for verification of the identity of a user and signing of his/her public keys.

General Notes
One operation within the PKI system which deserves a mention is the administration of the Certification Authority (CA). CAs are a type of "trusted third party" (TTP) which deliver validation authority for a PKI (Black & Layton, 2014, p. 13). PKIs assume the presence of CAs in that the users of the network store their public key with the CA which they recognise as a trusted third party that can vouchsafe the public key on its server. CAs verify the identity of each user and sign their public keys. So, in Alice and Bob's exchange of signatures, Alice is presenting her CA certificate, with the signature and public key both embedded, to Bob (Pedro, 2014, p. 55).

Citations
Black, P. & Layton, R. (2014). *Be careful who you trust: Issues with the Public Key Infrastructure*. 2014 Fifth Cybercrime and Trustworthy Computing Conference. IEEE Computer Society. Retrieved from https://www.researchgate.net/publication/282936649_Be_careful_who_you_trust_Issues_with_the_public_key_infrastructure
Pedro, F. (2015). *Understanding Bitcoin: Cryptography, engineering and economics*. Chichester: John Wiley & Sons Ltd.

CRYPTOCURRENCY

Syndetic Relationships
BT: virtual currency
RT: cryptography
RT: BitCoin
BT: digital money

InterPARES Definition
n. ~ a decentralized form of digital currency which relies on cryptographic techniques for generation of units and/or transaction security.

General notes
Usually thought of as a subset of (→) virtual currency, the term cryptocurrency implies use of encryption techniques in its creation or operation. All virtual currencies based on (→) blockchains, such as (→) BitCoin, are cryptocurrencies.

Citations
Gerstein, Hervieux-Payette 2015, p. 3: A cryptocurrency is one in which users come to an agreement about changes in the transactions ledger using cryptographic techniques. In the case of Bitcoin, the unique private key associated with every Bitcoin transaction is encrypted.
http://www.bankofcanada.ca/wp-content/uploads/2016/03/swp2016-14.pdf
Webber et al 2016, p. 6): Cryptocurrencies are a new medium of exchange. In their most basic form, they are a communications technology that offers peer-to-peer (P2P) transactions, eliminating the need for a third-party (ie. a bank) to carry out and authorize the transaction.
http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf

CRYPTOGRAPHIC HASH FUNCTION

Syndetic Relationships
RT: Hash

InterPARES Definition
n. ~ a mathematical algorithm that maps data into a bit string.

General Notes
In blockchains, cryptographic hashes serve to enable transparency without exposing content. A small change in the data input drastically changes the bit string, a simple comparison shows proof of data input change.

Citations
Schneier 2004: One-way hash functions are a cryptographic construct used in many applications. They are used with public-key algorithms for both encryption and digital signatures. They are used in integrity checking. They are used in authentication. They have all sorts of applications in a great many different protocols. Much more than encryption algorithms, one-way hash functions are the workhorses of modern cryptography. https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5.html

DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)

Syndetic Relationships
RT: Decentralized Autonomous Corporation (DAC)

InterPARES Definition
n. ~ an organization that is run through rules encoded as computer algorithms called (→) smart contracts

General Notes
Open-source investor-directed venture capital fund application autonomously running on top of the Ethereum blockchain.
(daohub.org, 2016) The DAO - the first Decentralized Autonomous Organization on the Ethereum blockchain which was developed by German programmer, Christoph Jentzsch, and was launched in 2016.
(wikipedia, 2016) A decentralized autonomous organization (DAO), sometimes labeled a decentralized autonomous corporation (DAC), is an organization that is run through rules encoded as computer programs called smart contracts. A DAO's financial transaction record and program rules are maintained on a blockchain. There are several examples of this business model. The precise legal status of this type of business organization is unclear.

Citations
Popper, 2015: One of the biggest companies in the field of smart contracts is the DAO, an open-source investor-directed venture capital fund application running on top of the Ethereum blockchain that was developed by German programmer, Christoph Jentzsch, and was launched in 2016. Many industry experts and observers, as well as the mainstream media, have had difficulty to fully describe what it is that the DAO does or offers, although, it has generated a lot of excitement and has managed to raise over $150 million from investors through crowdfunding, making it the most successful crowdfunded venture ever - this popularity also speaks to the attractiveness of POS because users actually have a stake in the system.
Popper, Nathaniel. (August 28, 2015).“Bitcoin Technology Piques Interest on Wall St.” *The New York Times*. Retrieved from http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html
del Castillo, 2016: One way of describing the DAO and what it does is that it is a collection of Ethereum-based smart contracts that, when taken collectively, amount to a series of by-laws and other founding documents that determine how its constituency - anyone who has bought DAO tokens with ethers - votes on decisions, allocates resources, and, thereby, creates a return on investment from the projects the DAO helps fund.Unlike a traditional company that has a designated managerial structure, the DAO is run and owned by everyone who has purchased a DAO token, although, on top of this structure exists a group of Curators who are there to provide a failsafe mechanism and security from attacks and fraud. The Curators do not add centralization to the DAO, as they are nominated by investors and can be fired at any time, for any reason.
del Castillo, Michael. (April 11, 2016). “Ethereum Used for ‘First’ Paid Energy Trade Using Blockchain Tech.” *CoinDesk*. Retrieved from http://www.coindesk.com/ethereum-used-first-paid-energy-trade-using-blockchain-technology/

DIGITAL MONEY

Sin.: digital currency

Syndetic Relationships
NT: cryptocurrency
RT: BitCoin
NT: virtual currency

InterPARES Definition
n. ~ a digital form of currency that allows for instantaneous transactions and borderless transfer-of-ownership.

General notes
The term digital money is often thought synonymous with digital currency, (→) virtual currency and (→) cryptocurrency but this is true only in the first case. Both (→) virtual currency and (→) cryptocurrency are much narrower terms. Digital money may refer to any digital medium of exchange and is sometimes even used to describe physical money in a digital state (such as money in a bank account).

Citations
Parliament of Australia 2015, p. 11: [A] digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. 'real currency', 'real money', or 'national currency'), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.[6]
http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report
Webber et al. 2016, p. 18: …it may include electronic forms of a state-issued currency, such as prepaid access cards and wire transfers. Similarly, the Bank of Canada stated that the term may include online credit card transactions, Interac transactions sent by email, online bill payments and the cashing of cheques with a smartphone's camera. The Bank also indicated that individuals often use terms such as "e-money," "e-cash," "digital money," "digital currency" and "virtual currency" interchangeably, erroneously believing that they have the same meaning. The Bitcoin Alliance of Canada suggested that a "virtual currency" is based on a ledger, a "digital currency" only exists digitally, and a "cryptocurrency" is based on cryptography. It identified cryptocurrencies as a subset of digital currencies, which are a subset of virtual currencies. The Department of Finance said that it considers a digital currency to have four characteristics:
its value can be held and exchanged without the use of banknotes or coins;
it is not the official currency of a country;

[6] FATF, *Virtual Currencies—Key Definitions and Potential AML/CFT Risks*, 2014, p. 4. http://www.fatfgafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-amlcft-risk.html; see also Attorney General's Department, *Submission 42*, p. 5. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

it has the intended purpose of being exchanged for real or virtual goods and services; and
its units can be transferred between individuals, between businesses, and between individuals and businesses.
http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf

DISTRIBUTED CONSENSUS

Syndetic Relationships
RT: Ttransaction
RT: Blockchain
RT: Authentication

InterPARES Definition
n. ~ a consensus about the integrity of a transaction reached by thousands of computers located around the world (→ node), in the process of verification of the transaction.

General Notes
Distributed consensus – thousands of computers located around the world, known as 'nodes', verify each transaction by authenticating the digital signatures en masse: they reach consensus about the integrity of each transaction. This process is an element of the decentralized nature of the blockchain and some have argued that it gives the blockchain more integrity than authentication by a single CA (Lea, 2016). Amati stated three complementary positives of the blockchain's consensus on signatures:

- All agree on the latest signatures,
- We are seeing the same signatures,
- No-one can alter the signatures (Amati, 2016, para. 30).

So, instead of relying on a central authority to certify a document's authenticity, the blockchain can assert proof of its authenticity through cryptographic confirmation. This dynamic can empower many archive managers to establish their own records systems backed by the assurance and longevity of the distributed blockchain network (Findlay, 2015, para. 14).

Citations
Lea, T. (2016). *Introductory course – The power of the blockchain*. What is blockchain? Retrieved from https://www.youtube.com/watch?v=KXC9hyB09pk

DISTRIBUTED LEDGER

Syndetic Relationships
RT: blockchain

InterPARES Definition
n. ~ a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions.

General notes
A distributed ledger is a digital record of ownership, but without a central administrator of the ledger and a central data store. Instead, the ledger is replicated among many different nodes in a peer-to-peer network, and a consensus algorithm ensures that each node's copy of the ledger is identical to every other node's copy. Asset owners must use cryptographic signature to debit their account and credit another's, so a distributed ledger is unforgeable.
A blockchain is just one type of distributed ledger. The bitcoin blockchain, which uses 'Proof-of-Work Mining', is the most publicly proven method used to achieve distributed consensus. However, other forms of distributed ledger consensus exist such as Ethereum, Ripple, Hyperledger, MultiChain, Eris, and other private enterprise solutions.

Citations
DuPont and Maurer, 2014: The core qualities new enterprises like Ethereum exploit all have to do with underlying features of blockchains as records-keeping devices, and peculiar ones, at that. A blockchain is a database or ledger that is distributed among all the nodes in the network running it (at least in theory). Each node has a complete copy of the entire database (again, at least in theory). Modifications to the database have to be verified by enough of the other nodes to warrant that modification's validity. Bitcoin uses a lottery-like proof of work system to effect this, but other systems can do it differently. Regardless, the key characteristics of a blockchain that make it a special kind of ledger and that are particularly appealing to developers and proponents are that it is: distributed, decentralized, public or transparent, time-stamped, persistent, and verifiable.
Dupont, Quinn & Maurers, Bill. (2014). Ledgers and the Law in Blockchain. The King's Review. Retrieved from http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain/

European Securities and Markets Authority, 2016: Distributed ledgers - sometimes known as 'Blockchains' in the case of virtual currencies - are essentially records, or ledgers, of electronic transactions, very similar to accounting ledgers. Their uniqueness lies in the fact that they are maintained by a shared or 'distributed' network of participants (so-called 'nodes') and not by a centralized entity, meaning that there is no central validation system. Another important feature of distributed ledgers is the extensive use of cryptography, i.e. computer-based encryption techniques such as public/private keys and hash functions, to store assets and validate transactions.
European Securities and Markets Authority. (2016). *Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets* (pp. 1–34). Retrieved from https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

ELECTRONIC EVIDENCE

Syndetic Relationships
BT: evidence

InterPARES Definition
n. ~ an rvidence that is handled by a computer or a computer system.

General Notes
–

Citations
Schafer & Mason 2012, p. 27: Electronic evidence [is] data (comprising the output of analogue devices or data in digital format) that is manipulated, stored, or communicated by any man-made device, computer, or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be with the evidence.
Burkhard Schafer & Mason, Stephen. 'The characteristics of electronic evidence in digital fomat' in Stephen Mason (eds) Electronic Evidence (LexisNexis, 2012) 23-70

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

Syndetic Relationships
RT: Blockchain
RT: Hashing
RT: Public key
RT: Bitcoin
RT: DSA digital signature

InterPARES Definition
n. ~ a signature scheme which combines elliptic curves (a public key family) with the DSA digital signature; used in Bitcoin.

General Notes
Specialized signatures
The blockchain community have conceived an array of signatures that utilise the hashing process in a way that can solve various issues, mainly concerning space. I will run through those that would be most relevant to a records manager:

- Elliptic Curve Digital Signature Algorithm (ECDSA) – ECDSA combines elliptic curves (a public key family) with the DSA digital signature and, together, form the signature scheme used in Bitcoin (Pedro, 2015, p. 70). The feature that would be of interest to an archivist looking for an efficient preservation strategy is that there is no need to store the public key as it can be hashed repeatedly in the future (Lemieux, 2016).
- Schnorr signatures - this is an overriding signature that hashes a cluster of signatures in order to remedy file storage issues. So, if a fond contains thirty documents each with their own signature, the archivist can sign the entire fond with a Schnorr signature. He would reduce the filesize from 2400 bytes (80 bytes per signature) back to 80 bytes. The cryptography community approves of them because of their speed, simplicity and strong security (van Wirdum, 2016, para. 14; Allen, 2015, para. 3). Some in the Bitcoin community have called for Schnorr signatures to become the standard (Pedro, 2015, p.58). This can be a useful signature and one that will be simple to preserve for new fonds that contain a large number of documents.

Citations
Pedro, F. (2015). *Understanding Bitcoin: Cryptography, engineering and economics*. Chichester: John Wiley & Sons Ltd.
Lemieux, V. (2016). *Trusting records: Is blockchain technology the answer?* Records Management Journal, 26(2)

ETHEREUM

Syndetic Relationships
RT: ether
RT: Ethereum Project

InterPARES Definition
n. ~ a public blockchain platform which provides a decentralized virtual machine that can execute (→) smart contracts using a cryptocurrency called *ether*.

General Notes
(wikipedia, 2016) Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality.It provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), that can execute peer-to-peer contracts using a cryptocurrency called ether
(ethereum.org, 2016): Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference

Citations
Pangburn, (2015), para. 5: Ethereum is a public blockchain that allows developers to easily deploy decentralized applications. What is notable about the Ethereum blockchain is that it offers more flexibility than the Bitcoin blockchain in terms of the applications that can run on it. This is because the Ethereum blockchain's programming language is Turing complete, meaning it is a system "in which a program can be written to find an answer - or to execute a smart contract that can buy something, sell something, or do something," while the Bitcoin blockchain scripting language is more restrictive, limited, and less user-friendly.
Pangburn, DJ. (June 19, 2015). "The Humans Who Dream of Companies That Won't Need Us." *Fast Company*, Retrieved from http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them.

EVERLEDGER

Syndetic Relationships
RT: distributed ledger

InterPARES Definition
n. ~ a digital, permanent, global ledger that tracks and protects items of value by using the Bitcoin blockchain as a platform for provenance

General Notes
dia barcelona, 2016: Everledger is a digital, permanent, global ledger that tracks and protects items of value by using the Bitcoin blockchain as a platform for provenance and combating insurance fraud.

Citations
Patel, 2015: One UK company that has been in the news a lot in this regard is Everledger, who is using blockchain technology to help the insurance industry solve diamond theft and fraud. Founded in 2015 by Leanne Kemp, Everledger uses the Bitcoin blockchain as a platform for creating a permanent ledger registry for diamond certification and related transaction history, which helps insurance companies, law enforcement and other interested parties to verify ownership. In conjunction with certified diamond laboratories a multi-layered digital fingerprint is created and imprinted on a given diamond and also recorded on the blockchain: "by using the immutable public blockchain for holding such data Everledger aims to provide transparency around all diamonds, reveal their origin, trail of ownership, the processes they might have undergone".
Patel, Kam. (September 15, 2015). "Everledger: putting bling on the blockchain." *FusionWire*. Retrieved from http://www.fusionwire.net/innovators/everledger-putting-bling-on-the-blockchain/

FACTOM

Syndetic Relationships
RT: Intrinio
RT: tieron

InterPARES Definition
n. ~ an open-source distributed, decentralized protocol running on top of the Bitcoin blockchain that collects, packages, and secures data into the Bitcoin blockchain through hashes and a network of federated servers, whom delegate responsibility in the system

General Notes
(factom.com, 2016) Factom stores the world's data on a decentralized system. Using blockchain technology for smart contracts, digital assets and database integrity.

Citations
Bitcoinist.net, 2015: *Factom* was developed in 2014 by the Texas Bitcoin Conference founder Paul Snow, investment and tech specialists Peter Kirby and David Johnston, all of whom still run Factom. Factom is an open-source distributed, decentralized protocol running on top of the Bitcoin blockchain that collects, packages, and secures data into the Bitcoin blockchain through hashes and a network of Federated servers, whom delegate responsibility in the system, Notably, no "single server is ever in control of the whole system, and no server is permanently in control of any part of the system; the responsibility for each part of the system cycles among the servers each minute".
Bitcoinist.net. (June 1, 2015). "The Factom Protocol - A Technical Overview." *Inside Bitcoins*. Retrieved from http://insidebitcoins.com/news/the-factom-protocol-a-technical-overview/32872
Lemieux, 2016, p. 15:.Factom is about proof of publication, proof of process, and proof of audit ("Factom - FAQs," n.d.). Factom publishes a hash of a document, or a digital fingerprint of a document, which lets you validate and verify a document without revealing any private information. This hash is then secured into the Bitcoin Blockchain where it remains immutable. To reiterate an earlier point, obviously, these hashes are not the actual records themselves, and the hashes are only used to authenticate the original records, but only if those originals have been exactly preserved so as to produce the same hashes as on the blockchain, since a blockchain hash cannot be reverse engineered.
"FAQs." (n.d.). Retrieved from https://www.factom.com/faqs/
Lemieux, V. (2016). Trusting records: Is blockchain technology the answer? *Records Management Journal*, 26(2)

FORK

Syndetic Relationships
RT: blockchain
NT: hard fork
NT: soft fork

InterPARES Definition
n. ~ a split in a blockchain which appears when two or more blocks have the same block height. Typically occurs when two or more miners find blocks at nearly the same time, but can also happen as part of an attack.

General notes
The word 'fork' in this context originates from open source software. The development of software like this would allow to draw trees: each time the code is copied separately, a new branch is created. This would be called 'forking', since the same code would then develop in two parallel directions.
If two miners find a new block at the exact same second, they will both have valid and legitimate blocks, and neither will have a reason to toss it out. Both blocks are linked to the last one, but the block after will have to be linked to one of these two. Technically, this is a fork in the blockchain.

Citations
Danova, 2015: What happens when the blockchain forks? It's actually quite simple: you get two chains with a shared genesis and are identical up until the forking point, after which they exist exclusively in parallel (unless one is completely abandoned), creating two separate networks.
Danova, Helga (2015), What is Bitcoin Fork? Retrieved from https://blog.cex.io/bitcoin-dictionary/what-is-bitcoin-fork-14622

HARD FORK

Syndetic Relationships
BT: fork
RT: blockchain
RT: soft fork

InterPARES Definition
n. ~ a permanent divergence in the block chain caused by non-upgraded nodes not following new consensus rules.

General notes
Hard fork is a change of the Bitcoin protocol that is not backwards-compatible; i.e., older client versions would not accept blocks created by the updated client, considering them invalid. This can create a blockchain fork when nodes running the new version create a separate blockchain incompatible with the older software. Hard forks ease block acceptance rules making previously invalid blocks valid in the new version. This is not forward compatible as older versions will not accept the new blocks, causing the users of the old paradigm to remain on their own blockchain-fork indefinitely. To implement a hard fork, without a blockchain-fork, all users must switch to the new protocol consensually.

Citations
Wong and Kar, 2016: That leaves a hard fork, where the core developers of Ethereum unilaterally make the decision to essentially create a new version of the network with different rules than the original. Then, miners, exchanges, and other major apps that are built on it need to decide if they want to a part of the new version of Ethereum or the original. Hence, the idea of a fork.
Wong, Joon Ian & Ian Kar, Ian. (2016, July 18). Everthing you need to know about the Ethereum "hard fork". *Quartz*. Retrieved from http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/
Amsel, 2016: A hard fork suggested by EthCore will replace the previously immutable contract known as TheDAO and perhaps any other attacked contracts. It will also directly transfer ether from attacker contracts back to the original DAO.
Amsel, Alex (2016). Understanding Proposed Ethereum Forks. Retrieved from https://medium.com/ownage/understanding-proposed-ethereum-forks-6abd63a478fc#.h7c6umbbb
Smith and Atlas, 2016: A hard consensus fork occurs when blocks that would have previously been considered invalid are now valid. Any Bitcoin user, miner, exchanger, etc. who wants to stay in consensus with the network must upgrade his software during a hard consensus fork; otherwise, some new block that the network accepts will appear as invalid to him.
Smith, Peter & Atlas, Kristov (2016). A Brief History of Bitcoin Forks. Retrieved from https://blog.blockchain.com/2016/02/26/a-brief-history-of-bitcoin-forks/

INSTITUTIONAL-BASED TRUST

sin. institutional trust, system trust

Syndetic Relationships

–

InterPARES Definition

n. ~ a belief that a certain institution has met all needed criteria and conditions are in place so that it can lead to situational success.

General notes

Institutional-based trust assures a person, institution or any other user of the services provided by a certain party, that the party providing these services has met all the safeguards and conditions to be trusted on a level needed to successfully complete a certain task or operation.

Citations

F. B. Cross, F. B., 2004. "Law and Trust." *Geo. Law Journal* 93: 1484.

MINER

Syntetic Relationships
RT: blockchain
RT: hash

Definition
n. ~ a network (→) node that finds valid proof of work for new blocks, by repeated hashing.

General Notes
The word "mining" is somewhat misleading. By evoking the extraction of precious metals, it focuses our attention on the reward for mining, the new bitcoins in each block. Although mining is incentivized by this reward, the primary purpose of mining is not the reward or the generation of new coins. If you view mining only as the process by which coins are created, you are mistaking the means (incentives) as a goal of the process. Mining is the main process of the decentralized clearinghouse, by which transactions are validated and cleared. Mining secures the bitcoin system and enables the emergence of network-wide consensus without a central authority. Mining is the invention that makes bitcoin special, a decentralized security mechanism that is the basis for peer-to-peer digital cash.

Citations
Antonopoulos, Andreas M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc.

MULTISIGNATURE

Syndetic Relationships
RT: Schnorr signatures
RT: Cryptography

InterPARES Definition
n. ~ an aggregation of more than one signature into a single, new signature.

General Notes
Wirdum 2016:
Schnorr
So what, then, are Schnorr signatures?
Schnorr, named after its inventor Claus-Peter Schnorr, is a signature scheme: the series of mathematical rules that link the private key, public key and signature together. Many cryptographers consider Schnorr signatures the best in the field, as they offer a strong level of correctness, do not suffer from malleability, are relatively fast to verify, and – importantly – support multisignature: several signatures can be aggregated into a single, new signature.
However, until now it has not been possible to utilize Schnorr in Bitcoin. Another type of signature scheme, Elliptic Curve Digital Signature Algorithm (ECDSA), is baked into the Bitcoin protocol, and changing that would require a hard fork.
That's where Segregated Witness comes in.
With Segregated Witness, all signature data is moved to a separate part of the transaction: the witness, which is not embedded in the "old" Bitcoin protocol. And thanks to script versioning, almost any rule applied in the witness can be changed through a soft fork. Including the type of signature scheme used.
This opens the door for Schnorr.

Citations
Wirdum, A. van. (2016, April 14). The power of Schnorr: The signature algorithm to increase Bitcoin's scale and privacy. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496

NODE

Syndetic Relationships
RT: Honest node

InterPARES Definition
n. ~ a. a single unit (computer) within a network; b. a single unit (computer) within a decentralized blockchain system which holds a copy of the blockchain and expends CPU power to build the blockchain.

General Notes
Because blockchains rely on nodes to form distributed ledgers and store their copies, blockchain integrity depends on the nodes. In order to keep a blockchain secure from outside interference, the amount of CPU power produced by honest nodes must exceed the amount produced by potential destabilizing nodes.

Citations
Nakamoto 2008: The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof of work as proof of what happened while they were gone. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf

NOTARIZATION

Syndetic Relationships
RT: virtual notary

InterPARES Definition
n. ~ the act of attesting to a documents' authenticity.

General Notes
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).

Citations
Prisco 2016: According to Vavilov, the blockchain will be used as a notary service. In November, Bitcoin Magazine covered the plans of the Estonian government for another official blockchain-based notarization service
https://bitcoinmagazine.com/articles/bitfury-announces-blockchain-land-titling-project-with-the-republic-of-georgia-and-economist-hernando-de-soto-1461769012

PEER-TO-PEER PAYMENT

Syndetic Relationships
RT: cryptocurrency
RT: BitCoin
RT: digital money
RT: virtual currency

InterPARES Definition
n. ~ a transaction using a (→) cryptocurrency between two parties which does not rely on a third party (such as a bank) to conduct the transaction.

General notes
Peer-to-peer communication is a common term in computer technologies, especially networks. It assumes direct communication between two equal parties (peers) without any special servers or services which enable it. Peer-to-peer payment is a similar term but it replaces the lack of need for an intermediary technology with a lack of need for an institution to conduct the (digital) payment (most often a bank).

Citations
No citation found. The term is rarely used and authors may consider it self-explanatory.

PROOF-OF-CONCEPT (POC)

Syndetic Relationships
RT: Blockchain
RT: Hashing

InterPARES Definition
n. ~ a documented evidence that a potential product or service can be successful.

General Notes
A *proof-of-concept* is a documentation of evidence that proves the viability of a project which is then hashed to the blockchain (Rouse, 2014b, para. 1). This proof-of-concept can come in the form of web traffic or transaction volumes. In the context of a blockchain project, the entrepreneur will build a solution, gather supporting datasets, then hash the sets and broadcast them to the blockchain.
In the context of digital preservation, Peter van Garderen stated that cryptographic hash functions are used for the production of proof of a digital action that is unique, which means there is no identical hash. In the action of hashing a document and then recording the hash to the blockchain, the archivist has created a *proof-of-concept* (Van Garderen, 2016).

Citations
Rouse 2014: Proof of concept (POC) is documented evidence that a potential product or service can be successful.
Developing a proof of concept can help a product owner to identify potential technical and logistical issues that might interfere with success. It also provides the opportunity for an organization to solicit internal feedback about a promising product or service, while reducing unnecessary risk and exposure and providing the opportunity for stakeholders to assess design choices early on in the development cycle.
A proof of concept plan should address how the proposed product or service will support business goals. It should include clearly defined criteria for success, documentation for how the proof of concept will be carried out, an evaluation component and a proposal for how to move forward should the POC prove to be successful. Developing such a plan is an important step in determining how an envisioned product or service will ultimately be delivered to users with the fewest number of flaws.
Rouse, M. (2014). Digital signature. *SearchSecurity.TechTarget*. Retreived on September 4, 2016, from http://searchsecurity.techtarget.com/definition/digital-signature
Garderen, P. van. 2016: In the action of hashing a document and then recording the hash to the blockchain, the archivist has created a *proof-of-concept*.
Garderen, P. van. (2016, May 17). Blockchain and digital preservation. Presentation at Simon Fraser University [Video file]. Retrieved from https://www.youtube.com/watch?v=S2N0m9YDgZw

PROOF OF STAKE

Syntetic Relationships
RT: blockchain
RT: Ethereum

Definition
n. ~ an algorithm that depends upon cryptocurrency holdings of the node and not its computational resources. The validators place in a "security deposit" over which the protocol has direct control; if nodes on the network behave unpredictably in validating a transaction, they forfeit their deposit or "stake".

General Notes
Ethereum and other blockchains use an alternative consensus method, called "proof of stake." It is an algorithm that depends upon cryptocurrency holdings of the node and not its computational resources. The validators place in a "security deposit" over which the protocol has direct control; if nodes on the network behave unpredictably in validating a transaction, they forfeit their deposit or "stake" (Zamfir, 2015). This gives incentive for miners to serve the consensus, and not to bet against it. Proof of stake is argued to be more sustainable and secure than proof of work, as transactions are confirmed based on current information of the nodes (Larimer, 2015). Mining is essentially the "main process of the decentralized clearinghouse, by which transactions are validated and cleared…[it] secures the [system] and enables the emergence of network-wide consensus without a central authority" (Antonopoulos, 2014, p. 176).

Citations
Zamfir, Vlad. (August 1, 2015). "Introducing Casper 'the Friendly Ghost.'" *Ethereum Blog*. Retrieved from https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/
Antonopoulos, Andreas M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc. p. 176
Larimer, Daniel.(August 8, 2015). "Review of Casper, Ethereum's Proposed Proof of Stake Algorithm." *Bytemaster's Blog*. Retrieved from http://bytemaster.github.io/2015/08/08/Review-of-Casper-Ethereums-proposed-Proof-of-Stake-Algorithm/

SCHNORR SIGNATURES

Syndetic Relationships
RT: Hashing
RT: Fond
RT: Criyptography
RT: Bitcoin

InterPARES Definition
n. ~ a. A signature scheme comprising of series of mathematical rules for linking private key, public key and signature together. It offers a strong level of correctness, do not suffer from malleability, are relatively fast to verify, and support multisignature; b. An overriding signature that hashes a cluster of signatures in order to remedy file storage issues.

General Notes
Specialized signatures
The blockchain community have conceived an array of signatures that utilise the hashing process in a way that can solve various issues, mainly concerning space. I will run through those that would be most relevant to a records manager:

- Elliptic Curve Digital Signature Algorithm (ECDSA) – ECDSA combines elliptic curves (a public key family) with the DSA digital signature and, together, form the signature scheme used in Bitcoin (Pedro, 2015, p. 70). The feature that would be of interest to an archivist looking for an efficient preservation strategy is that there is no need to store the public key as it can be hashed repeatedly in the future (Lemieux, 2016).
- Schnorr signatures - this is an overriding signature that hashes a cluster of signatures in order to remedy file storage issues. So, if a fond contains thirty documents each with their own signature, the archivist can sign the entire fond with a Schnorr signature. He would reduce the filesize from 2400 bytes (80 bytes per signature) back to 80 bytes. The cryptography community approves of them because of their speed, simplicity and strong security (van Wirdum, 2016, para. 14; Allen, 2015, para. 3). Some in the Bitcoin community have called for Schnorr signatures to become the standard (Pedro, 2015, p.58). This can be a useful signature and one that will be simple to preserve for new fonds that contain a large number of documents.

Citations
Wirdum 2016:
Schnorr
So what, then, are Schnorr signatures?
Schnorr, named after its inventor Claus-Peter Schnorr, is a signature scheme: the series of mathematical rules that link the private key, public key and signature together. Many cryptographers consider Schnorr signatures the best in the field, as they offer a strong level of correctness, do not suffer from malleability, are relatively fast

to verify, and – importantly – support multisignature: several signatures can be aggregated into a single, new signature.
However, until now it has not been possible to utilize Schnorr in Bitcoin. Another type of signature scheme, Elliptic Curve Digital Signature Algorithm (ECDSA), is baked into the Bitcoin protocol, and changing that would require a hard fork.
That's where Segregated Witness comes in.
With Segregated Witness, all signature data is moved to a separate part of the transaction: the witness, which is not embedded in the "old" Bitcoin protocol. And thanks to script versioning, almost any rule applied in the witness can be changed through a soft fork. Including the type of signature scheme used.
This opens the door for Schnorr.
Wirdum, A. van. (2016, April 14). The power of Schnorr: The signature algorithm to increase Bitcoin's scale and privacy. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496

SIDECHAIN

Syndetic Relationships
RT: blockchain
RT: distributed ledger
RT: BitCoin

InterPARES Definition
n. ~ a blockchain which relies on another blockchain to validate data.

General notes
Rarely used term, most authors use blockchain in places where sidechain would be appropriate.

Citations
Blockstream: Sidechains are blockchains that are interoperable with each other and with Bitcoin, avoiding liquidity shortages, market fluctuations, fragmentation, security breaches and outright fraud associated with alternative crypto-currencies.
https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf
Back et al. 2014, p. 8):[7] A sidechain is a blockchain that validates data from other blockchains.
https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

[7] Paper not referenced directly, referenced in Narayanan et al 2016: Bitcoin and Cryptocurrency Technologies

SMART CONTRACT

Syndetic Relationships
RT: blockchain

InterPARES Definition
n. ~ a self-executing computer algorithm which embeds the terms and conditions of a contract as source code that is compiled into executable computer code

General Notes
Smart contracts are stored on 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.
Smart contracts are computer protocols that embed the terms and conditions of a contract as source code that are compiled into executable computer code that can run on a network, thus, many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing or both, making contractual processes more efficient and faster.
(wikipedia, 2016) Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts usually also have a user interface and often emulate the logic of contractual clauses. Proponents of smart contracts claim that many kinds of contractual clauses may thus be made partially or fully self-executing, self-enforcing, or both. Smart contracts aim to provide security superior to traditional contract law and to reduce other transaction costs associated with contracting.

Citations
von Haller Gronbaek 2016: This article explores the use of blockchain technology for applications other than cryptocurrency (blockchain 2.0). Among these applications are smart contracts. Entries into the ledger may consist of computer code that executes the terms and conditions of a contract between parties. Such parties will usually be parties to contracts, private individuals, corporate entities, public institutions or other entities. The more sophisticated the code, the more automated, self-executing, and "smarter" the contract.
von Haller Gronbaek, Martin. (June 16, 2016). "Blockchain 2.0, smart contracts and challenges." *Bird & Bird*. Retrieved from http://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges
von Haller Gronbaek, 2016: Smart contracts are computer protocols that embed the terms and conditions of a contract as source code that are compiled into executable computer code that can run on a network, thus, many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing or both, making contractual processes more efficient and faster. 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 a database that cannot be forged or tampered with. With blockchain-based smart contracts there is no longer a need for a third party for recordkeeping or enforcement, and should, technically, eliminate ambiguity.
von Haller Gronbaek, Martin. (June 16, 2016). "Blockchain 2.0, smart contracts and challenges." *Bird & Bird*. Retrieved from http://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges

Blockchain Technology for Recordkeeping

SMART PROBATE

Syndetic Relationships
RT: Smart Contract

InterPARES Definition
n. ~ a will or probate that would function in a similar way as a (→) smart contract; once a set of pre-established conditions are met the probate would execute.

General notes
This implementation could streamline the probate process but it does not eliminate the need for courts to get to their findings in a faster way.

Citations
Howard, 2015: The blockchain cannot eliminate [...legal challenges to a will] or the factual basis for them," says Dixon. That is important because a common attack on the smart contract concept is premised on the fear that technology (through the blockchain) would remove a person's 'due process right' to have his or her day in court. "What the blockchain can do," continued Dixon, "is make it much easier for a genuine will to be upheld, for a bogus challenge to be dismissed, and for courts to come to factual findings much more quickly".

SOFT FORK

Syndetic Relationships
BT: fork
RT: blockchain
RT: hard fork

InterPARES Definition
n. ~ a temporary fork in the blockchain which commonly occurs when miners using non-upgraded nodes violate a new consensus rule their nodes don't know about.

General notes
Soft forks restrict block acceptance rules in comparison to earlier versions.
The new rules allow a subset of the previous valid blocks, therefore all blocks considered valid by the newer version are also valid in the old version. If at least 51% of the mining power shifts to the new version, the system self-corrects: blocks created by old versions of Bitcoin Core that are invalid under the new paradigm might commence a short-term "old-only blockchain-fork", but eventually, they would be overtaken by the chain fork created under the new paradigm, as the hashing power working on the old paradigm would be smaller ("only old versions") than on the new paradigm ("accepted by all versions").
However, if less than 51% of the hashing power switches to the new version, it behaves like a hard fork, and the blockchain-fork will not mend, as the chain created under the old rules has more hashing power and is incompatible to the new rules.

Citations
Amsel, 2016: A soft fork is an optional flag that miners can elect to run on their node. The suggested fork is to allow breathing room only (to quote Jeff) to prevent any DAO contract, including child DAOs, from reducing their ether balance. This buys time for a real solution before more damage can be done by this or other exploits.
Amsel, Alex (2016). Understanding Proposed Ethereum Forks. Retrieved from https://medium.com/ownage/understanding-proposed-ethereum-forks-6abd63a478fc#.h7c6umbbb
Smith and Atlas, 2016: A soft consensus fork occurs when blocks that would have previously been considered valid are now invalid. Upgrading software during a consensus soft fork is forever optional to a Bitcoin user, miner or exchanger, with the following caveats:

- If the soft fork introduces a new feature that you want to use as either the sender or recipient, you must upgrade in order to use it.
- At least 51% of miners must upgrade to adopt the soft fork; otherwise, it will forever appear as the shortest chain and get orphaned by the network.
- Refusal to accept the soft fork can reduce your security. As you would normally consider soft forked transactions invalid, Bitcoin developers use various tricks to make these transactions appear valid to you while reducing your client's capacity to process exactly why they are valid.

Smith, Peter & Atlas, Kristov (2016). A Brief History of Bitcoin Forks. Retrieved from https://blog.blockchain.com/2016/02/26/a-brief-history-of-bitcoin-forks/

TIMESTAMP

Syndetic Relationships
RT: Timestamping

InterPARES Definition
n. ~ current time of an event that is recorded by a computer

General Notes
(wikipedia, 2016) A timestamp is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. The term derives from rubber stamps used in offices to stamp the current date, and sometimes time, in ink on paper documents, to record when the document was received. Common examples of this type of timestamp are a postmark on a letter or the "in" and "out" times on a time card.

Citations
Parker, "Timestamping" 2015: Timestamping is the process of securely keeping track of the creation and modification time of a document, allowing vested parties to know with certainty that a document existed at a particular date and time. Timestamping is a business tool seemingly well-suited for blockchain technology because by design a blockchain transaction includes date and time that is secured by the blockchain through a hash that can later certify the existence of data.

TRUSTED THIRD PARTY (TTP)

Syndetic Relationships
RT: Certification Authority
RT: PKI (Public Key Infrastructure)
RT: Public Key

InterPARES Definition
n. ~
1. Secure middle layer on (cloud) service transactions
2. Public or private sector organizations that allow the secure, trustful, interaction between two parties.

General Notes
TTPs have been defined as a "secure middle layer on (cloud) service transactions" (Stamou et al., 2013, p. 4976), they allow the secure, trustful, interaction between two parties (p. 4979). TTPs can be public sector organizations, such as the NSA and GCHQ, or they can originate from the private sector e.g. GlobalSign, Symantec and Comodo.

Citations
Stamou, K., Aubert, J., Gateau, B., Morin, J-H. (2012). *Preliminary requirements on trusted third parties for service transactions in cloud environments*. 2013 46th Hawaii International Conference on System Sciences. Institute of Electrical and Electronics Engineers, 4976-4983.

TRUSTLESS TRANSFER

Syndetic Relationships
–

InterPARES Definition
n. ~ a system where record rights are administered and mediated by a technology, excluding a trusted institution or third party.

General Notes
This system does not actually move us beyond the need for trusted third parties, nor does it remove the enormity of the law in preserving rights and ensuring public trust. As Victoria Lemieux explains, at least with regards to systems where the records themselves are created and maintained outside of the blockchain: "Does using the Bitcoin Blockchain ensure the trustworthiness of the records? No. Trustworthiness is only guaranteed if the records are both reliable and authentic. Blockchain solutions do not address the reliability of records, and there are many features of the Bitcoin Blockchain that may negatively affect the authenticity of information as well."

Citations
Baker, Edward D. (2015). "Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange." Southwestern Law Review 45: 341–433.

VIRTUAL CURRENCY

Syndetic Relationships
NT: cryptocurrency
RT: BitCoin
BT: digital money

InterPARES Definition
n. ~ a digital medium of exchange, usually Internet based and independent of any physical currency or governing body such as a central state bank; may be convertible into real currency or it may not be in which case it is specifically designed to be used inside a closed system.

General notes
Refers to a type of (→) digital money which is designed specifically for use on the Internet or another digital closed system.

Citations
European Central Bank 2012, p. 6: A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.
European Central Bank (2012). Virtual Currency Schemes. Retrieved from http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
Gerstein & Hervieux-Payette 2015, p. 18: …it may include electronic forms of a state-issued currency, such as prepaid access cards and wire transfers. Similarly, the Bank of Canada stated that the term may include online credit card transactions, Interac transactions sent by email, online bill payments and the cashing of cheques with a smartphone's camera. The Bank also indicated that individuals often use terms such as "e-money," "e-cash," "digital money," "digital currency" and "virtual currency" interchangeably, erroneously believing that they have the same meaning. The Bitcoin Alliance of Canada suggested that a "virtual currency" is based on a ledger, a "digital currency" only exists digitally, and a "cryptocurrency" is based on cryptography. It identified cryptocurrencies as a subset of digital currencies, which are a subset of virtual currencies. The Department of Finance said that it considers a digital currency to have four characteristics:

- its value can be held and exchanged without the use of banknotes or coins;
- it is not the official currency of a country;
- it has the intended purpose of being exchanged for real or virtual goods and services; and
- its units can be transferred between individuals, between businesses, and between individuals and businesses.

Gerstein, Irving R. & Hervieux-Payette, Céline (2015). Digital Currency: You Can't Flip This Coin! Report of the Standing Senate Committee on Banking, Trade and Commerce. Canada. Retrieved from http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf

Appendix C – Blockchain Campanies

NAME	GEOGRAPHIC LOCATION	USE CASE CLASSIFICATION CATEGORY	BLOCKCHAIN PLATFORM	VALUE PROPOSITION	FOUNDED	SOURCE
Acronis Blockchain Technology Initiative	USA/ Singapore	Data protection and notarization	Ethereum	data storage and file sync & share solutions	2016	http://www.acronis.com/en-us/business/blockchain-notary/
Appii	UK	Job recruitment	Ethereum	Appii has developed a blockchain-based solution to register and verify the experience and qualifications of students, and those already in the workforce.	2016	http://www.appii.io/
Applied Blockchain	UK	Blockchain Applications & Storage	Private/Ethereum		2015	http://appliedblockchain.com/
Ascribe	USA	Attribution and Registration service for artists and creators	Bitcoin	Lock in attribution, securely share and trace where your digital work spreads.	2014	https://www.ascribe.io/
Bazaar Blockchain Technologies	UK	Market Maker for BTC liquidity	Bitcoin	IT solutions for fast and reliable integration with existing financial systems via API and FIX.	2014	http://www.bazaarbt.com/index.html
BigChainDB	Germany	Blockchain Applications & Storage	RethinkDB (*database)	Bigchain DB is database-style decentralized storage: a blockchain database. BigchainDB combines the key benefits of distributed DBs and traditional blockchains, with an emphasis on scale.	2016	https://www.bigchaindb.com/
Bitcoin	International	Open-source cryptocurrency, digital asset and payment system	Bitcoin	Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen.	2009	https://bitcoin.org/en/
BitCourt	Argentina	Digital signatures and document notarization	Bitcoin	BitCourt is a contract and transparency platform using blockchain technology where	2015	https://signatura.co/

				parties can sign and notarize contracts, resolve disputes, manage calls for tenders and many more custom-made solutions. BitCourt allows you to notarize any document, linking it to your personal or corporate identity, signing, timestamping and creating a publicly verifiable proof of its authenticity without exposing its contents.		
Bitfiniex	Hong Kong	Cryptocurrencies exchange	In-house platform	Bitfinex is a trading platform for Bitcoin, Litecoin and Ether with many advanced features including margin trading, exchange and margin funding.	2013	https://www.bitfinex.com/
Bitfury	USA & Netherlands	Security & infrastructure provider; Bitcoin mining	Bitcoin	BitFury offers a both hardware and software allowing businesses and governments to operate on the public blockchain including the following software offerings: digital assets PaaS, data analytics, voting, property rights registration; and hardware solutions: semiconductors and microelectronics, servers, datacenter construction.	2011	http://bitfury.com/
Bitland	Ghana	Land registration	Bitcoin & BitShares	Bitland is an experimental platform using decentralized, trustless models such as Bitcoin's blockchain to bridge the gap between the government and the undocumented areas for land registry and title services.	2013	http://www.bitland.world/

BITNATION	International	Government administration	Bitcoin	BITNATION is designed to disrupt the nation state oligopoly through offering more convenient, secure and cost-efficient Do-It-Yourself Governance services including security and dispute resolution. BITNATION offers a full range of services traditionally done by governments. We provide a cryptographically secure ID system, blockchain based dispute resolution, marriage and divorce, land registery, education, insurance, security, diplomacy, and more through a fully distributed platform.	2014	https://bitnation.co/
BlockApps STRATO	USA	Ethereum blockchain applicaitons.	Ethereum	for rapid development, deployment and management of enterprise blockchain applications.	2015	http://www.blockapps.net/
Blockchain Tech Ltd	Canada/UK	Blockchain platforms for finance and DAM	private	develops easy to use and intuitive platforms built on blockchain, enabling businesses to increase efficiency (first technology platform is a remittance business called Interbit)	2015	http://btl.co/
BlockCrushr Labs	Canada	Social & Welfare Services	Ethereum	Feeding homeless people using blockchain to anonymously load "digital food wallets".		https://www.blockcrushr.com/wp-content/uploads/2016/05/Ending-Homeless-Hunger-With-The-Blockchain-First-Draft.pdf
Blocksign	USA	Document signing and verifying	Bitcoin	a service for legally signing any document, contract or agreement.	2014	https://blocksign.com/

Blockstack Labs	USA	Decentralized services for Identity, naming, storage and authentication.	Bitcoin	A Global Naming and Storage System Secured by Blockchains" A large deployment of a decentralized PKI service built on top of the Namecoin blockchain; Build decentralized, server-less apps by plugging into Blockstack's services for identity, naming, storage, and authentication.	2013	https://blockstack.org
Blockstream	USA	Bitcoin applications	Bitcoin	Developing bitcoin applications specifically sidechains, as well as other applications to accelerate innovation in crypto currencies, open assets and smart contracts.	2014	https://www.blockstream.com/
BlockTech	USA	Blockchain-based Archival and Library services	Bitcoin and Litecoin	Blockchain-based archival application that offers an open source, censorship-resistant, peer-to-peer library for art, history, and culture.	2014	https://blocktech.com/
Bluzelle	Canada	Finance	Ripple	Creating blockchain financial products centered on the foreign exchange market using the Ripple protocol.	2015	http://bluzelle.com/
Chromaway	Sweden	Finance & smart contracts	Bitcoin	Chromaway provides a platform for smart contracts and issuing and transferring assets through a blockchain, mainly using colored coins.	2014	http://chromaway.com/
Chronicled	USA		Ethereum	Eliminating conterfeits from the market by providing an authenticated platform for collecting/transferring collectible and vintage sneakers	2015	http://www.chronicled.com/

Coin Sciences	UK	Public and private blockchain suite and services development	In-house platform - Multichain	Developing the MultiChain platform for private blockchains. MultiChain (www.multichain.com) includes features such as permissions management, native asset support, simple configuration and deployment, and backwards compatibility with bitcoin. Other products previously developed include CoinSpark (coinspark.org), a rich protocol for enhancing bitcoin transactions with third-party assets and messaging, and Coin Secrets (coinsecrets.org) which shows recent metadata embedded in the bitcoin blockchain.	2014	https://coinspark.org/about-coin-sciences-ltd/
Colored Coins	USA	Protocol specification for issuing and transacting digital assets on top of the Bitcoin Blockchain	Bitcoin	An open source bitcoin 2.0 protocol that enables developers to create digital assets on top of bitcoin Blockchain utilizing its functionalities beyond currency.	2015	http://coloredcoins.org/
ConsenSys	USA	Ethereum blockchain applicaitons.	Ethereum	a venture production studio building decentralized applications and various developer and end-user tools for blockchain ecosystems, focusing primarily on Ethereum.	2015	https://consensys.net/
Counterparty (XCP)	USA	Bitcoin applications powering finance	Bitcoin	Open Source protocol enabling users to write smart contracts	2014	http://counterparty.io/
Cryptiv	Canada	Digital asset management system	Multiple protocols	Cryptiv will facilitate seamless, currency agnostic transactions using digital currencies over the internet and across social	2014	https://cryptiv.com/

				media.		
decentral	Canada	Blockchain technology consultants	N/A	decentral offers blockchain consulting services, fintech expertise and software development, as well as Toronto's first two-way Bitcoin ATM. We organize community-driven events that bring together enthusiasts in finance and fintech, blockchain, cryptocurrencies and decentralized technologies.	2014	http://decentral.ca/
Digital Asset Holdings	USA	settlement and ledger services for financial assets	maps applications onto both public and private blockchains	software company that builds distributed, encrypted straight through processing tools	2014	https://digitalasset.com/
Enigio Time	Sweden	Authentication, Digital notary services	Bitcoin as a referenced blockchain, but use own blockchain Enigio as a Blockchain Aggregator	Solutions for qualified electronic time stamping, traceability and E-archives.	2012	https://enigio.com/
Eris	USA	Smart Contract application platform	Ethereum, eris:db	a platform for building, testing, maintaining, and operating applications with a blockchain backend.	2014	https://erisindustries.com/
Ethcore	UK	Ethereum browser "Parity"	Ethereum	Develop software solutions for enterprises and industries using blockchain technologies	2014	https://ethcore.io/
Ethereum	Switzerland	Public blockchain platform	Ethereum	a public blockchain-based distributed computing platform, featuring smart contract functionality.	2013	https://www.ethereum.org/
Everledger	UK	Asset verification, Certification, or tracker	combined private blockchain based on the Eris stack with Bitcoin, but will deployed to Ethereum later	fraud detection system; a premanent ledger for diamond certification and verification for insurance companies, owners, claimats,	2015	http://www.everledger.io/

				and law enforcement		
Factom	USA	Timestamping service for business	Bitcoin	A scalable data layer for Blockchain to power a remarkable range of applications, including audit systems, medical records, supply chain management, voting systems, property titles, legal applications, and financial systems.	2014	http://factom.org/
Filament	USA	Communication platform builder	Bitcoin	To develop ad-hoc mesh networks of smart sensors for industrial applications, operating on the blockchain.	2015	https://filament.com/
Filecoin	USA	Distributed file service for storing data	Bitcoin	a data storage network and electronic currency based on Bitcoin.	2014	http://filecoin.io/
Fluent	USA	Financial network and payment platform	custom-built, federated blockchain where the nodes are hosted both with big buyers and the financial institutions on the network.	provides a real-time, low-cost, simple and secure invoicing and payments system for global supply chains based upon blockchain technology and is targeted for use by banks, financial institutions and their global enterprise customers.	2014	https://fluent.network/
Hashkloud Pty	Australia	Digital Commerce & Payments platform	Bitcoin	technology company developing Fintech solutions	2015	http://www.hashkloud.com/
Hawk	USA	Privacy-preserving blockchain and smart contracts	Ethereum and Zcash	a system of smart contracts that can be layered on top of any existing blockchain to hide not only a transaction's counterparty, but the amount of the transaction itself.	2016	https://eprint.iacr.org/2015/675.pdf
Hyperledger	USA	Blockchain platform	Hyperledger	cross-industry collaborative effort to support blockchain-based distributed ledgers.	2015	https://www.hyperledger.org/
IBM Blockchain	USA	Platform as a service (PaaS)	Private	Bluemix platform as a service	2014	http://www.ibm.com/blockchain/inde

				(PaaS) provides convenient ways to test an IBM Blockchain network on the cloud; this service is built on top of the Linux Foundations's Hyperledger Project open source code.		x.html
IPFS (InterPlanetary File System)	USA	Content Addressed, Versioned, P2P File sharing system	private and Ethereum	a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.	2014	https://ipfs.io/
Ledger Labs	Canada	Blockchain consulting	N/A	Ledger Labs is a Toronto-based consulting and development firm applying decentralized systems and principles to the fields of security, finance, and governance. Packed with unparalleled blockchain expertise, we aim to be a national and global leader in understanding and interpreting this new science.	2015	https://ledgerlabs.com/
Litecoin	USA	Open-source P2P digital currency	Litecoin	The Litecoin blockchain is capable of handling higher transaction volume than its counterpart - Bitcoin. Due to more frequent block generation, the network supports more transactions without a need to modify the software in the future. As a result, merchants get faster confirmation times, while still having ability to wait for more confirmations when selling bigger ticket items.	2011	https://litecoin.org/

MaidSafe	Scotland	SAFE (Secure Access For Everyone) network that manages and secures data	own version of a block chain, which it calls the 'transaction manager'.	a new platform to improve Internet security.	2006	http://maidsafe.net/
Mediachain Labs	USA	Asset registration, identifying, and tracking	Bitcoin	a protocol for registering, identifying, and tracking creative works online.	2016	https://blog.mediachain.io/how-mediachain-works-5a5ccc1c3210#.8azprwea4 https://blog.mediachain.io/introducing-mediachain-a696f8fd2035#.tnsxosfkn
MedVault	Ireland	Medical	Bitcoin & Colu	MedVault allows patients to securely record medical information on the bitcoin blockchain while creating rules to control who can access it. Currently in proof-of-concept stage.	2015	http://www.coindesk.com/medvault-wins-e5000-at-deloitte-sponsored-blockchain-hackathon/
Monograph	USA	A content monetization platform — Monegraph Everywhere. Digital Asset Management	Bitcoin	a platform that makes it easy for digital creators of all kinds to construct licenses for the commercial use of their digital work.	2015	https://monegraph.com
Namecoin	International	domain name registration (.bit)	Bitcoin	software is used to register names and store associated values in the blockchain	2011	https://namecoin.info/docs/faq/
Omni Layer (formerly Mastercoin)	USA	Digital currency and communications protocol	Bitcoin	Second-Generation Protocol on the Bitcoin Blockchain; seeks to create an entirely new network of currencies, commodities and securities	2013	http://www.omnilayer.org/
PeerTracks	USA	Music streaming and retail services	MUSE	PeerTracks is a music streaming, music retail (download), talent discovery and fan engagement platform that allows everyone – content creators and consumers - to make a living from music. The game changer lies in the underlying Peer-to-Peer network (called MUSE) we use to simplify, automate and remove much of		http://peertracks.com/

				the costly overhead.		
Proof of Existence	USA	Data certification and notarization	Bitcoin	establish proof-of-existence on the bitcoin blockchain	2013	https://www.proofofexistence.com/
Provenance	UK	Supply Chains, trust and transparency	Ethereum and Bitcoin	Creating and fostering open and accessible information about products	2013	https://www.provenance.org/
Quadriga Fintech Solutions	Canada	Fintech	Bitcoin	The company provides a wide range of innovative products and services, including Canada's longest-running Bitcoin trading platform, a digital currency merchant payment processing platform and a peer-to-peer remittance service via which users can send secure funds to recipients worldwide., including Bitcoin ATMs.	2013	http://quadrigafs.com/
R3CEV	USA	Finance	Microsoft Azure	Leads a consortium of major financial companies in research and development of blockchain usage in the financial system.	2014	https://r3cev.com/
Ripple Labs	USA	Finance	Private in-house platform	Ripple's distributed financial technology allows for banks around the world to directly transact with each other without the need for a central counterparty or correspondent.	2012	https://ripple.com/
Rubix	Canada	Blockchain platform for enterprise solutions	Private in-house platform & Ethereum	Rubix is a software platform that allows Deloitte teams and clients to build their own customized blockchain-based and smart contract applications for any use case. Some examples include: decentralized capital markets systems; peer-to-	2014	http://rubixbydeloitte.com/index.html

				peer payments; and health data management.		
ShoCard	USA	Digital identity and authentication	Bitcoin	ShoCard is a digital identity and authentication platform built on a public blockchain data layer, using public/private key encryption and data hashing to safely store and exchange identity data, which includes biometrics such as fingerprint, facial, iris and voice.	2015	https://shocard.com/
Skuchain	USA	Finance & commerce	Bitcoin	To create a new era of collaborative commerce based on a new type of trust - a smart contract that governs all phases of a typical trade agreement from order, shipment and invoice to final payment. A blockchain model connecting together new realms of commerce where financiers in developed economies can provide loans down the supply chain to clients in emerging and developing economies, even though they have no history of trade or data with these firms.	2014	https://www.skuchain.com/
Stampery	USA/SPAIN	Data certification and notarization	Bitcoin & Ethereum	Uses Blockchain Timestamping Architecture (BTA) to generate a proof for each individual dataset	2015	https://stampery.com/
Symbiont	USA	Smart contract system, trading platform called Smart Securities	Bitcoin	Symbiont will be using Counterparty and other blockchain-based technology to solve specific, identified issues in several segments of the multi-trillion dollar securities	2015	http://symbiont.io/

				market.		
Tallysticks	UK	Business operations	Private	Using blockchain (distibuted ledger) technology for invoice management.	2015	http://tallysticks.io/
The DAO	"Stateless"	Venture capital fund	Ethereum	To provide a new decentralized business model for organizing both commercial and non-profit enterprises.	2016	https://daohub.org
Tierion	USA	Cloud platform for data collection, registration, and verification	Bitcoin	cloud platform capable of recording millions of records in the Bitcoin blockchain.	2015	https://tierion.com/
TransActive Grid	USA	Energy	Ethereum	To develop an energy exchange on a microgrid using blockchain technology.		https://consensys.net/static/TransactiveGridRelease.pdf
Ubitquity	USA	Real Estate, Notary services	Bitcoin	Securely recording, tracking, and transferring of title. Increase transparency, reduce search time & fraud with our revolutionary Software-as-a-Service (SaaS) Platform.	2015	https://www.ubitquity.io/home/index.html
Uproov	Australia	Photo and video registration and authentication service	Bitcoin	A creation of LedgerAssets Pty Ltd	2015	https://uproov.com/
Virtual Notary	USA	Document Notarization	Bitcoin	Certifying factoids and issues cryptographically-signed certificate that attests to that factoid. We can optionally record the certificate on the Bitcoin blockchain.	2013	http://virtual-notary.org/
Wave	Israel	Trade	In-house platform	WAVE connects all members of the supply chain to a decentralized network and allows them a direct exchange of documents. WAVE's application manages ownership of documents on the blockchain eliminating	2014	http://wavebl.com/

				disputes, forgeries and unnecessary risks.		

1Appendix D – Blockchain Research Initiatives

University or Organiz-ation	Country of Origin	Project Name(s)	Sub-projects	Notes	Link
MIT	USA	The Media Lab Digital Currency Initiative		Bitcoin focused by notes blockchain in summary	https://www.media.mit.edu/research/highlights/media-lab-digital-currency-initiative
			MedRec	A medical records project using blockchain as its technological base. Describes itself as a "decentralized record management system for EMRs that uses blockchain technology to manage authentication, confidentiality, accountability, and data sharing." Uses Ethereum. Most interestingly, it turns medical records into anonymized data that researchers can access.	http://jods.mitpress.mit.edu/pub/medrec
			Enigma	A private P2P data computation service. Uses blockchain to control the network, primarily because it is a "tamper proof log"	http://enigma.media.mit.edu/
			Media Lab Digital Certificates	Uses blockchain to "store and manage digital credentials." Claims to be tamper proof.	http://www.media.mit.edu/files/projects.pdf
University College London	UK	Digital Currencies, Digital Finance and the Constitution of a New Financial Order		Part of UCL's Centre for Law, Economics and Society (CLES). Broad focus. Also has a Research centre for blockchain technology http://blockchain.cs.ucl.ac.uk/	https://www.ucl.ac.uk/cles/research_initiatives/digital-currencies
		UCL Centre for Blockchain Technologies		Aims to produce blockchain research in the three key areas of science and technology, economics and finance, and regulation and law	http://blockchain.cs.ucl.ac.uk/
Cornell	USA	IC3 - INITIATIVE FOR CRYPTOCURRENCIES & CONTRACTS		Initiative of Cornell University, Cornell Tech, and UC Berkeley. Smart contracts focusis relevant to our research	http://www.initc3.org/
			Solidus	A centralized cryptocurrency for use by banks, etc.	http://www.initc3.org/projects.html
			Bitcoin-NG	Improves bitcoin transaction throughput	http://www.initc3.org/projects.html
			Miniature World	Blockchain emulation testbed	http://www.initc3.org/projects.html
			Fruit Chain	Project to learn more about and discourage bitcoin frauds	http://www.initc3.org/projects.html
			Falcon Network	"Wide Area Interconnect" for Blockchain	http://www.initc3.org/projects.html
			FLAC	Security tool	http://www.initc3.org/projects.html
			Virtual Notary	Blockchain notary. Iissues both freestanding certificates as well as immutable records on the Bitcoin blockchain."	http://www.initc3.org/projects.html
			Etherscrape	Tool to read/understand smart contracts	http://www.initc3.org/projects.html
			Hawk	Smart contract system. This system had some crossover with University of Maryland via two researchers, Ahmed E. Kosba, Andrew Miller, and Babis Papamanthou	http://www.initc3.org/projects.html
			Gyges	Smart contract programming frameworks	http://www.initc3.org/projects.html

			Town Crier	Integration of "trustworthy" authenticated data feeds into smart contracts	http://www.initc3.org/projects.html
			Theoretical Foundations for Secure Decentralized Systems	Research into the security of decentralized systems.	http://www.initc3.org/projects.html
University of Pittsburgh	USA	Ledger		This is an open access journal about crypto-currencies. No articles have yet been published.	http://ledger.pitt.edu/ojs/index.php/ledger
Imperial College London	UK	Centre for Cryptocurrency Research and Engineering		Focused on engineering, novel applications of blockchain, and financial applications.	http://www.imperial.ac.uk/cryptocurrency/about/
		Cryptocurrency Effects in Digital Transformations		In conjunction with Surrey University. Focused on economic impacts of distributed ledgers.	http://wwwf.imperial.ac.uk/business-school/research/innovation-and-entrepreneurship/ie-research/research-initiatives-and-themes/credit/
University of Waterloo	CA	Cryptography, Security, and Privacy	Cryptocurrencies	Responsibiliy of prof. Sergey Gorbunov. Not terribly blockchain focused.	https://crysp.uwaterloo.ca/research/
Universite de Quebeca Montreal	CA			Requires a french speaker to determine value	http://www.lca.uqam.ca/2016/03/technologies-de-confiance-et-societe-ouverte-blockchain-fab-lab-et-badges-numeriques/
University of Melbourne	AU	Melbourne Networked Society Institute (MNSI)		Blockchain is identified as research area under the "Financial" category, which is a 2016 Focus Area. This is a funding programme seeking innovative interdisciplinary research. Something may result? There is currently nothing concrete, but something to keep an eye on.	
University of Western Australia	AU	?		Student project that designed a blockchain based voting system.	http://www.unihall.uwa.edu.au/news/unihallers-win-5000-grant/
Coventry University	UK	BITCOIN AND BEYOND: BLOCK CHAIN, DIGITAL CURRENCIES AND THE CONSTRUCTION OF ALTERNATIVE ECONOMIES		Blockchain from a societal approach. It's a research project/academic program.	http://www.coventry.ac.uk/research/research-students/research-studentships/bitcoin-and-beyond-block-chain-digital-currencies-and-the-construction-of-alternative-economies/?theme=main
University of Cumbria	UK	Research on alternative currencies and exchange systems		Focused on sustainability; not blockchain focused. Bitcoin. Part of Institute for Leadership and Sustainability	http://www.cumbria.ac.uk/Courses/SubjectAreas/IFLAS/ResearchAlt.aspx
University of Edinburgh	UK	Design in Action		Has produced two papers on blockchain, one on visualizing it, another on "narrative" and blockchain.	
Middlesex University London	UK	Blockchain for Creative Industries		Investigating applications of blockchain to creative industries.	http://www.mdx.ac.uk/our-research/research-groups/blockchain-for-creative-industries
Oxford University	UK	Bitcoin and block chain for physical computing		A student project/research group. For students to produce research.	http://www.cs.ox.ac.uk/teaching/studentprojects/469.html
National Institute of Informa	JP	??		Very unclear, but there are interested researchers.	https://www.ideals.illinois.edu/bitstream/handle/2142/73770/478_ready.pdf

tics					
University of Louisville	USA	Bitcoin Messaging Protocol - Preserving and Validating Messages Through the BTC Blockchain		Not a project, just a presentation, but maybe relevant	http://louisville.edu/speed/computer/seminars/bitcoin-messaging-protocol-preserving-and-validating-messages-through-the-btc-blockchain
Harvard	USA	Berkman Center for Internet and Society	Digital Finance Initiative	Collaboration with MIT. Not much going on here yet it seems. But major collaborator Primavera De Fillipi has a number of publications	https://cyber.law.harvard.edu/research/digital_currency#
University of Maryland	USA	Maryland Cybersecurity Center (MC2)	(SEE CORNELL)	Associated with Cornell Hawk project. No specific blockchain research on website	http://www.cyber.umd.edu/
ETH Zurich	CH	Institute of Information Security	Security and Privacy of Bitcoin	Bitcoin in title but it seems equally applicable to blockchain. Several publications already	http://www.syssec.ethz.ch/research/Bitcoin.html
			Tampering with the Delivery of Blocks and Transactions in Bitcoin	Intersection of scailability and security	http://www.syssec.ethz.ch/research/Bitcoin.html
			Quantifying Location Privacy Leakage from Transaction Prices	Examines "impact that the prices from consumers' purchase histories have on the consumers' location privacy"	http://www.syssec.ethz.ch/research/Bitcoin.html
			Misbehavior in Bitcoin: A Study of Double-Spending and Accountability	Analyze[s] "the conditions for performing successful double-spending attacks against fast payments in Bitcoin, where the time between the exchange of currency and goods is short (in the order of a minute)"	http://www.syssec.ethz.ch/research/Bitcoin.html
			On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients	Examines "privacy of SPV clients"	http://www.syssec.ethz.ch/research/Bitcoin.html
			Is Bitcoin a Decentralized Currency?	Examines limits of decentralization	http://www.syssec.ethz.ch/research/Bitcoin.html
			Double-spending Attacks on Fast Payments in Bitcoin	Security of bitcoin in fast-payment situations	http://www.syssec.ethz.ch/research/Bitcoin.html
			Evaluating User Privacy in Bitcoin	Examines privacy issues	http://www.syssec.ethz.ch/research/Bitcoin.html
Princeton	USA			Associated with a startup something called Blockstack Labs. Also this guy Harry Kolodner https://www.w3.org/2016/04/blockchain-workshop/interest/kalodner.html	https://blockstack.org/blockstack.pdf
Carleton	CA	HotSoft		Elizabeth Stobert wrote a paper on bitcoin and has since moved to ETH Zurich. Otherwise, an undergraduate did a project called "Minimally Viable Blockchain" that won an award in winter 2016.	http://hotsoft.carleton.ca/hotsoft/
University of Technology, Sydney	AU	Finance Discipline Group		Contributed to AUS Senate report on bitcoin. Pg 20 bitcoins found to be for investments more than exchange.	
University of British	CA	iSchool research project			

Columbia					
Stanford University	USA	Applied Cryptography Group		Minor bitcoin and blockchain research	https://crypto.stanford.edu/
Cambridge University	UK	Center for Alternative Finance		Currently no dedicated blockchain of cryptocurrency research noted.	https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/
Open University	UK	Open Blockchain		Application of Blockchains to higher education.	http://blockchain.open.ac.uk/
National University of Singapore	SG	Security Research Cluster		Research on smart contracts	http://compsec.comp.nus.edu.sg/

Appendix E – Consultation Collaborators

Kuldar Aas, Deputy Digital Archivist at the National Archives of Estonia

Jason Baron, Counsel, Drinker Biddle & Reath LLP; Co-Chair of the Information Governance Initiative, USA

Nicolas Connizzo, Digital Archivist at the Vermont State Archives and Records Administration, USA

Luciana Duranti, Professor of Archival Science at the University of British Columbia, Canada

Barbara Endicott-Popovsky, Executive Director for the Center of Information Assurance and Cybersecurity at the University of Washington, USA

David Fricker, Executive Director at the National Archives of Australia, Australia

Natasha Khramtsovsky, Senior Expert at Electronic Office Systems LLP, Russian Federation

Richard Marciano, Professor, College of Information Studies, the University of Maryland, USA

John McDonald, Information Management Consultant and Educator, Canada

Chris Prom, Andrew S. G. Turyn Professor and Archivist, University of Illinios Urbana-Champagne, USA

Hrvoje Stancic, Associate Professor at Faculty of Humanities and Social Sciences, University of Zagreb, Croatia

Mats Stengärd, Partner and Chief Operating Officer, EnigioTime, Sweden

Peter van Garderen, Information Management Consultant, Canada

Ethan Wilding, Co-founder, Head of Strategy and Partnerships; Co-founder, Blockchain Canada, Canada

Angela Walch, Associate Professor of Law, St. Mary's University, USA

Appendix F – Dissemination Coverage

Peter. B. Nichol, "The Next Generation of Health IT," CIO from IDG,
http://www.cio.com/article/3090143/security/highlights-from-the-w3c-blockchain-workshop-at-mit.html

"**Archival bond**
This concept is primarily associated with Luciana Duranti, a professor of archival science at the School of Library, Archival and Information Studies at the University of British Columbia, Canada, who first proposed the concept and Heather MacNeil. MacNeil conducted research into the integrity of electronic records, with her 1996 paper, The Protection of the Integrity of Electronic Records.

The archival bond is a concept in archival theory referring to the relationship that each archival record has with the other records produced as part of the same transaction and located within the same grouping.
When we applying this concept, records would not be on the blockchain, but rather, only the hashes would reside on the blockchain (or related links or mappings). Does this mean library science and archival studies will be rising educational majors? Will the "Chief Archival Officer" be the newest wave to enter the c-suite?"

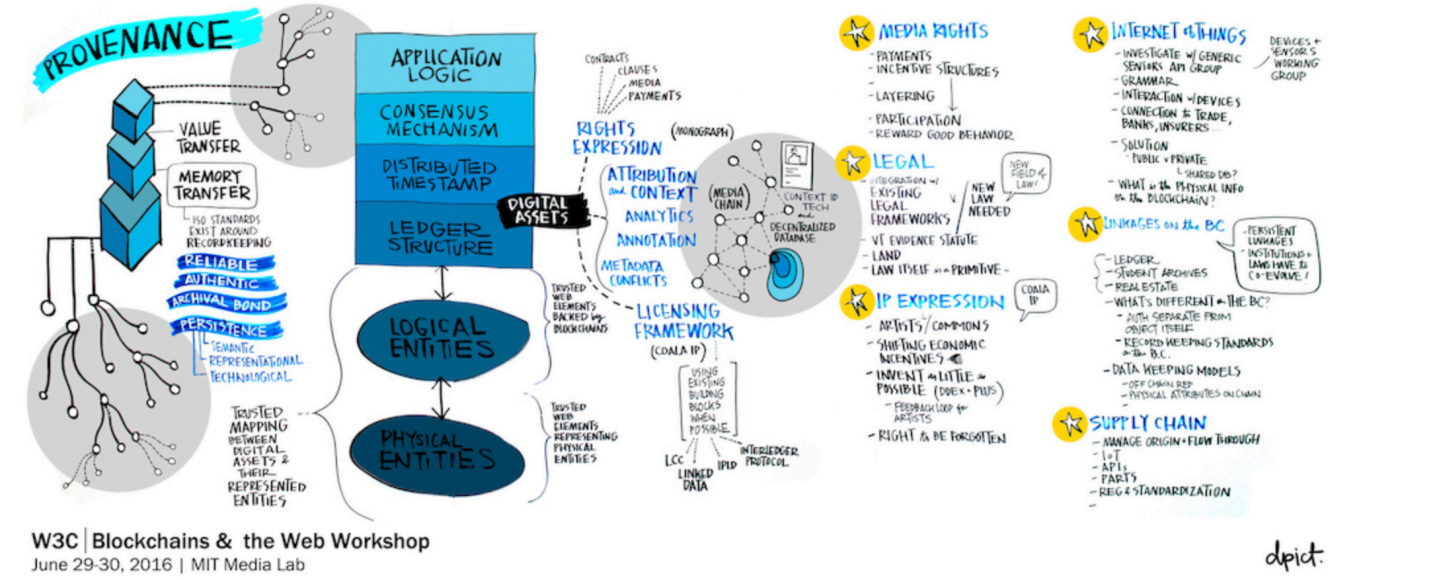

Figure 1: Visual Summary of Session on Provenance held at the W3C Blockchains & the Web Workshop. Note references to "Memory Transfer", "Archival Bond"; and "Preservation".

Appendix G – A Primer on Records and Recordkeeping

Key international and Canadian standards applicable to blockchain technology for recordkeeping

- ***ISO 14721: 2012.*** *Space Data and Information Transfer Systems—Open Archival Information System (OAIS) —Reference Model*
- ***ISO 15489: 2016.*** *Information and documentation* ***-*** *Records Management*
- ***ISO 16175-1: 2010.*** *Information and Documentation—Principles and Functional Requirements for Records in Electronic Office Environments—Part 1: Overview and Statement of Principles*
- ***ISO 16175-2: 2011.*** *Information and Documentation—Principles and Functional Requirements for Records in Electronic Office Environments—Part 2: Guidelines and Functional Requirements for Digital Records Management Systems*
- ***ISO 16175-3: 2010.*** *Information and Documentation—Principles and Functional Requirements for Records in Electronic Office Environments—Part 3: Guidelines and Functional Requirements for Records in Business Systems*
- ***ISO/IEC 18014-3: 2009***. Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens
- ***ISO 23081-1: 2006*** Information *and Documentation—Records Management Processes—Metadata for Records - Part 1: Principles*
- ***ISO 30300: 2011.*** *Information and Documentation—Management Systems for Records—Fundamentals and Vocabulary*
- ***National standard of Canada; CAN/CGSB-72.34-2005****. Electronic records as documentary evidence.*

This section of the primer is reprinted with permission from Hurley, G., Léveillé, V., and McDonald, J. (2016) *Managing Records of Citizen Engagement Initiatives: A Primer*. Vancouver: InterPARES Trust. Retrieved October 10, 2016 from https://interparestrust.org/trust/research_dissemination.

The authenticity, reliability, integrity and usability of records and their ability to serve their multiple roles for as long as they are required will also be dependent upon the quality of the records management infrastructure established by a given records-creating organization.

The components of the infrastructure for managing records are little different from those established for the management of other valued assets within a given organization, such as human resources and financial resources. All are based on asset management principles and all are dedicated to supporting the effective management of the objectives, goals, and functions of the organization. In the case of records management, the components of the infrastructure are as follows:

Laws and policies that assign accountability for the activities associated with the capture and management of records;

Standards and practices that enable the management of records as 'records';

Systems and technologies that support the capability to capture, organize, retain, make available and otherwise manage records throughout their life cycle;

People who have the required knowledge and abilities to plan, design, implement and maintain the infrastructure for managing records;

A **management and governance structure** that allocates and controls the resources for managing records; and

A level of **awareness** among all of those involved in creating, capturing and managing records about the importance of records and their responsibility for their proper management.

Ideally, while part of the infrastructure will reside in a central office, such as a records management office, other parts will be integrated in the infrastructures supporting the administrative and operational programs of the organization - for example, a program manager hiring and managing staff according to human resources policies and rules, or a program manager capturing and storing records locally in accordance with records management rules.

3.3 Configuration of the Records Management Infrastructure

Similar to the infrastructures for managing human and financial resources, the management of an infrastructure for managing records typically exists at the level of the organization. An example is a records management office located in a central 'corporate' area of the organization such as 'administration', an 'information management' department, or a 'corporate secretariat'. This enables the achievement of a number of organizational goals, such as the ability to respond to legal obligations, the opportunity to exchange information across the organization and maximize its value e.g. through policies and the application of standards, and the potential to reduce costs and achieve economies of scale.

While the infrastructure may be established at the whole-of-organization or at a corporate level, it is normally configured to support the requirements of the individual business lines or programs of the organization. For instance, just as human and financial resources are configured to support the communications function of an organization and its role in disseminating information to a given community, so too should the records management infrastructure be configured to capture and manage the records resulting from the dissemination activity. Similarly, it should be configured to support the capture and management of the activities associated with a consultation, or with undertaking a collaboration, or empowering a given community organization to carry out tasks normally associated with a given government organization.

The infrastructure may also extend beyond a single organization. For instance, . . . it may extend to embrace one or several government organizations and/or one or several community organizations. The specific configuration of the extended infrastructure, however, will be influenced by the nature of the . . . initiative. In 'inform', 'consult' and 'involve' engagements for instance, the infrastructures in each of the given government and community organizations may be distinct even though they are supporting the same joint activity. In an 'inform' engagement, for instance, the government may support a distinct infrastructure for disseminating information while the community organization may support its own distinct infrastructure for receiving information. Typically there would be little if any overlap between the infrastructures. Similarly, in an 'empower'

engagement, the government's records management infrastructure might be used to manage the records documenting the empowerment while the records management infrastructure in the community organization might be used to manage the records documenting document the empowered activity - for example, the development of a specific chapter of a national strategy on water resources management that would be accepted by the government. The potential for overlap may increase in 'involve' and 'consult' engagements as the government organization and community organization interact more closely to achieve common goals such as the development of methods for consulting a given community or managing a shared consultation process. In cases such as these where the capture and maintenance of a documentary record of the entire activity may be important, the records management infrastructures of both the government and community organizations may overlap. In a 'collaboration', an entirely new infrastructure for managing records may be established. One part may reside with the participating government organization(s), another with the participating community organization(s) and a third with the secretariat or similar governance and management structure established for the 'collaboration'. If it is important that a complete record of the collaboration be captured and maintained then it follows that the records management infrastructures of all three entities (government, community, secretariat) may be required to overlap.

Regardless of the type of engagement or the configuration of the records management infrastructure supporting a given engagement, the quality and integrity of the records will be dependent on the quality and integrity of the infrastructure. At a broader level, the quality and integrity of the records management infrastructure will be dependent upon the overall infrastructure for managing the GCE initiative itself. If there are weaknesses in the policies, procedures, standards, technologies, and governance/management structures supporting the management of the GCE initiative then it follows that the quality and integrity of the supporting records management infrastructure may be placed at risk.

Appendix H – A Primer on the Blockchain and how it operates

Terminology – See Appendix B.

General introduction to blockchain technology

- Tapscott, D. and Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World.*
- Tapscott, D. *Ted Talk - How the blockchain is changing money and business*
- Blockchain Canada learning resources - www.BlockchainCanada.org/learn

This section of the primer is reprinted with permission from Lemieux, V. (2016) Trusting Records: Is Blockchain Technology the Answer?. *Records Management Journal* 26 (2), http://www.emeraldinsight.com/doi/abs/10.1108/RMJ-12-2015-0042.

How does the technology work? Bitcoin Blockchain technology essentially establishes a distributed public ledger that contains the payment history of every Bitcoin in circulation, providing proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers - Bitcoin's nodes - around the world and is publicly available (The Economist 2015, 3). For purposes of more easily comparing the operation of native Blockchain to the case study implementation using Factom's proposed solution for the Honduran land registry system, discussion of the specifics of how the technology works will be divided into three parts: 1) recording transactions, 2) validating transactions and 3) updating a public ledger and authenticating transactions. An overview of the entire process using the Bitcoin Blockchain is provided as Table 1. Box 1 summarizes three critical FAQs for records professionals to understand about the Bitcoin Blockchain.

Table 1. Overview of how Bitcoin creates and updates a distributed public ledger

START – Bitcoin wallet A proposes the transfer of Bitcoin to another wallet B
2 - The Bitcoin distributed "mesh" network checks the public ledger that sufficient Bitcoin exists in wallet A
3 - If there is sufficient Bitcoin, specialized nodes called miners will bundle the proposal with other reputable transactions to create a new block for the Blockchain
4 - The blocks are cryptographically "hashed"; that is, they are used as input to an algorithm that converts then into a fixed-size alphanumeric string, which is called the hash value (sometimes also called a message digest, a digital fingerprint, a digest or a checksum).
5 - That hash is put, along with some other data (e.g., a nonce), into the header of the proposed block. See Appendix A

6 - This header then becomes the basis for the "proof of work" performed by the miner nodes on the Bitcoin network
7 - When a miner node arrives at a solution to the proof of work, other nodes check it and then each node that confirms the solution updates the Blockchain with the hash of the header of the proposed block. This becomes the new block's identifying string, now part of the distributed ledger in the Blockchain.
END – Wallet A's payment to Wallet B's transaction, and all the other transactions the block contains, are confirmed

5.1 Recording transactions

Blockchain technology works by using the Blockchain – made up of an electronic chain of hashes of digital signatures (see Figure 3). Digital signatures are a form of asymmetric cryptography (i.e., they use one private key and one public key) for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (i.e., it is authentic), that the sender cannot deny having sent the message (i.e., it is non-repudiable), and that the message was not altered in transit (i.e., that it has integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

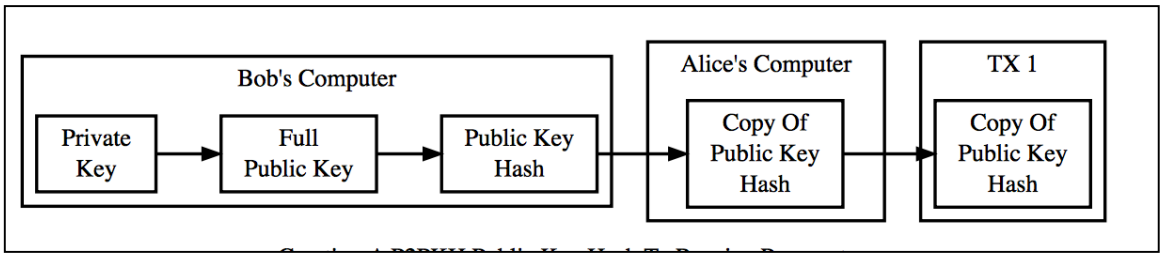

Figure 3. Bitcoin digital signature generation [Source: Nakamoto 2009]

Each party completes a transaction, for example, sale of a Bitcoin or other asset, by digitally signing (with their private key) a hash of the previous transaction and the public key of the next owner and adding these to the end of the hash chain. The receiving party (e.g., a payee) can verify the signatures to verify the chain of ownership (Nakamoto 2009; Bitcoin.org 2015). See Figure 4. To complete this process, Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256k1 curve. Secp256k1 private keys are 256 bits of random data. A copy of that private key data is computationally transformed into a secp256k1 public key, which avoids the need for a central authority (called a Certificate Authority) to generate and hold the public keys as is typical of Public Key Infrastructure (PKI) cryptography. (Bitcoin.org 2015).

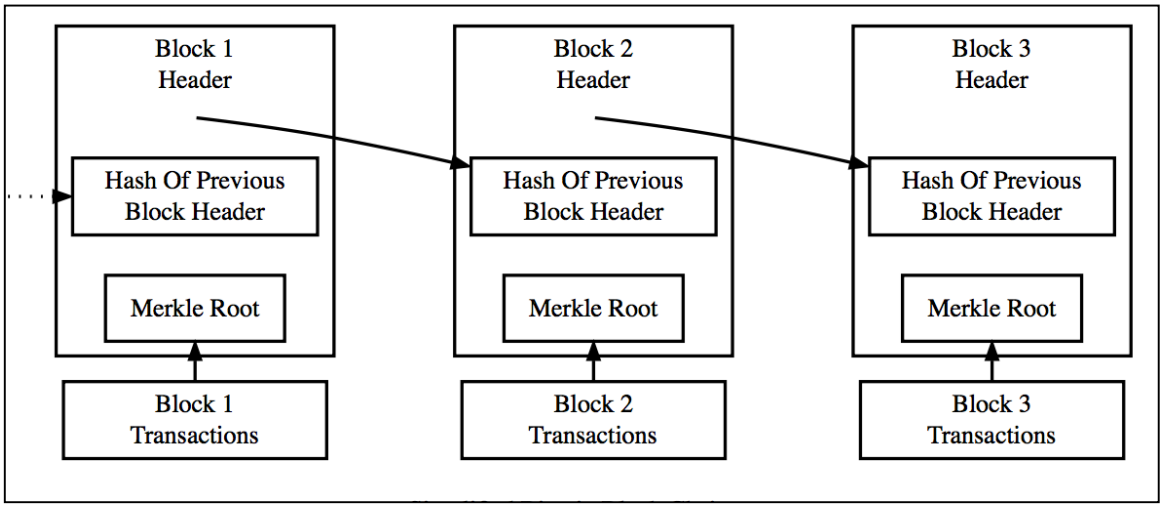

Figure 4. Simplified Blockchain [Source Bitcoin.org 2015].

5.2 Validating transactions

In order to avoid a situation wherein a party could transfer an asset twice (the problem of 'double-spending' in Bitcoin terms), the transactions are broadcast out to a distributed network of nodes to agree and approve the order of the transactions. Nodes in the network collect the broadcasts of the transactions into blocks, which are then hashed, and receive a timestamp. As explained,

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post . . . The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it (Nakamoto 2009).

To achieve this, the system uses the Hashcash proof of work function; the Hashcash algorithm requires the following parameters: a service string, a nonce (a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks), and a counter. In Bitcoin the service string is encoded in the block header data structure, and includes a version field, the hash of the previous block, the root hash of the Merkle tree[8] of all transactions in the block, the current time, and the difficulty (Bitcoinwiki) 2015). Proof of work, also called mining in Bitcoin parlance, occurs when a computer in the network scans for a value that when hashed begins with a required number of zero bits.

5.3 Updating a public ledger

When a computer finds the proof, it broadcasts the block to all nodes (see Appendix A for an example of the content of a Bitcoin block). Nodes accept the block only if all transactions in it are valid. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. Nodes work on a consensus system; that is, together with little coordination. Their behaviour is such that they do not need to be identified, can leave and rejoin the network at will, accept the proof-of-work chain as proof of what happened while they were gone and express their acceptance of valid blocks by working on extending them and can reject invalid blocks by refusing to work on them (Nakamoto,

[8] An important feature of the system in terms of saving disk space is that once the latest transaction has enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

2009). This process ultimately establishes a single, but distributed, agreed history for each transaction (a trusted chain of transactions, or Blockchain) and creates a way for the receiver of an asset to know that the previous owners did not sign any earlier transactions (or double spend) (Nakamoto 2009). Advocates argue that trust is increased among the parties because there no possibility for abuse by a node in a dominant position, as there can be when a system relies upon a single trusted third party that may be breached or turned rogue (Wild, Arnold and Stafford 2015). According to Bitcoin's inventor, the system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes because "in order to modify a past block, an attacker would have to redo the proof-of-work of the block *and all blocks after it* [emphasis added] and then catch up with and surpass the work of the honest nodes" (Nakamoto, 2009, 3).

Box 1. Three Key FAQs about the Bitcoin Blockchain [Source: Author's own analysis]

1. Does the Bitcoin Blockchain function as a decentralized archive, storing original records from which records can be accessed? No [in general]. Original records are not stored on the Bitcoin Blockchain, only hashes of original records.
2. Is it possible to reproduce an original record from the hash of the record stored on the Bitcoin Blockchain? No. It is not possible to reverse engineer a hash to reproduce a record.
3. Does using the Bitcoin Blockchain ensure the trustworthiness of the records? No. Trustworthiness is only guaranteed if the records are both reliable and authentic. Blockchain solutions do not address the reliability of records, and there are many features of the Bitcoin Blockchain that may negatively affect the authenticity of information as well.