ARMA INTERNATIONAL EDUCATIONAL FOUNDATION
RESEARCH • EDUCATION • SCHOLARSHIP

Blockchain Technology & Recordkeeping

Victoria L. Lemieux, Ph.D; Darra Hofman, JD, MSLS; Danielle Batista, B.A.R.M, MIS; and Alysha Joo, MASLIS

Project Underwritten by: ARMA Canada Region

May 30, 2019

www.armaedfoundation.org

Table of Contents

Preface

Information professionals are no strangers to changes in technologies used to create and keep records. In the past few decades, there have been several such changes, leading both to new forms of records, such as web or social media records, and recordkeeping solutions, such as electronic records management systems and cloud-based software services. Blockchains, which may be defined as ledgers with entries organized in an append-only, sequential chain using cryptographic links and distributed out and stored on a peer-to-peer computer network, are an emerging recordkeeping technology producing new forms of records, and new modalities of recordkeeping with which records and information professionals will need to engage.

Practically every country in the world is now considering or already using blockchain technology for recordkeeping.[1] Examples abound. The government of Georgia, for example, piloted the registration of land titles using a private blockchain in 2016 and has plans to expand the service to sales and purchases of land titles, mortgages, rentals, new land title registration, property demolition and notary services.[2] The Swedish land registry authority, Lantmäteriet, has been testing a way to record property transactions on a blockchain.[3] A pilot of an application of blockchain technology to land transfer registration in the municipality of Pelotas in Brazil was conducted by the local real estate registration authority in 2017.[4]

Recording of land transactions is by no means the only recordkeeping use case. Many jurisdictions, such as Estonia, are already using blockchain to securely keep medical records and a host of other types of government records as well.[5] The UK National Archives has been experimenting with the use of blockchains in digital preservation.[6] Recent reports issued by the US National Archives and Records Administration and Deep Analysis outline a growing array of blockchain projects and solutions.[7] In this study, our aim is to provide an overview of blockchain technology that offers information professionals knowledge that they will find useful to address the challenge of effectively managing records in these emerging recordkeeping environments.

The chapters in this report respond to and are structured according to an initial set of questions from the ARMA International Education Foundation's call for proposals for a study on blockchain and records and information management, viz: 1) Because blockchain executes a checksum at various distribution points, where is the actual record?; 2) What retention concerns are raised here? (Keeping as an active record, an archived record and e-discovery?); 3) How is destruction defined and executed?; 4) Who owns the record?; 5) Are there defined life cycles?; and 6) What are current standards and best practices? Do they differ by industry? There are certainly many more questions about this technology that need answers, but this list provides a good starting point.

As blockchain technology is still emerging, and technical changes to how it operates can be expected, we remain humble about our knowledge of this complex technology and its implications for records and information professionals. Nevertheless, it is our sincere hope that by sharing the current state of our understanding, we can help to prepare records and information professionals for the future of recordkeeping in a blockchain world.

Victoria L. Lemieux, Darra Hofman, Danielle Batista, and Alysha Joo

March 2019

Chapter 1: An Overview of Blockchain Technology

This chapter provides an overview of blockchain technology, beginning with a description of how it operates as a "technology of trust" and then delving into its technical aspects in greater detail. In general, in this chapter and throughout this report we will take the position that blockchains are a type of distributed ledger comprised of confirmed and validated blocks cryptographically chained together.[8] For convenience, however, we use the term blockchain to encompass both blockchains and distributed ledgers, pointing out differences between the two technologies only when needed for accuracy or clarity.

Blockchain as a Technology of Trust

Trust, it has been said, is "the bond of society," and society would hardly be able to function without it.[9] According to Duranti and Rogers, "Trust has been defined in many ways. In business, trust involves confidence of one party in another, based on an alignment of value systems with respect to specific benefits in a relationship of equals. In jurisprudence, trust is usually described as a relationship of vulnerability, dependence and reliance in which we participate voluntarily. In substance, trust means having the confidence to act without the full knowledge needed to act."[10] Setting aside differing views about the nature of trust, there is a growing global consensus that there exists, nowadays, a crisis of trust.[11] We no longer trust our institutions, our information systems, nor the information they contain. Moreover, many people increasingly mistrust centralized authorities in any form.[12] As an example, Cheney et al. observe: "historically, databases . . . were trusted because they were under centralized control: it was

assumed that trustworthy and knowledgeable people were responsible for the integrity of the data."[13] Collomosse et al. note that trust in archival institutions, traditionally seen as places that could be trusted to preserve the long-term integrity and authenticity of records, has eroded.[14] This erosion of trust is because, in many contexts, those in control of centralized systems have proven to be untrustworthy, manipulating the records which they were supposed to be protecting.[15] Nor has decentralization been the answer up until now: data originating from the web or social media have proven to be quite untrustworthy in many cases. We have lacked a comprehensive solution to these problems.

Now, however, blockchain technology has been advanced as a solution to the global crisis of trust. Indeed, blockchain's unique capabilities, some argue, circumvent the need for trust, which is why it is sometimes called a "trustless" technology.[16] In practice, however, blockchain technology really does not obviate the need for trust. Instead, it offers a new way to substitute the information one does not have from other sources in order to place confidence in something or someone (i.e., to trust) and, by extension, take action on the basis of having that trust.[17] It purportedly serves to replace more traditional, and often very inefficient or flawed means of obtaining this information and establishing trust (e.g., long-term social ties, traditional legal contracts, or information supplied by "trusted" intermediaries) with a new, more efficient source of information as a basis for trust.

The substitution of information necessary for trust is achieved in blockchain systems by: 1) incentive mechanisms: blockchain technology is designed to incentivize social actors to behave properly (e.g., via cryptocurrency-based reward mechanisms in some blockchains); interacting parties know this and therefore have the confidence to act without full knowledge of one another, 2) records creation and keeping: blockchain technology is meant to produce final, definitive and immutable records, using cryptography, thereby establishing tamper-resistant proof of actions that have taken place and 3) decentralization: blockchain technology operates as a distributed peer-to-peer network in which participants usually do not operate under any centralized authority; rather, participants are autonomous, though operating in a coordinated fashion because they are incentivized to do so. It is because they are autonomous, which makes collusion difficult, that the records generated in these systems can be trusted. These unique features provide a basis to assert claims without contestation (e.g., "I created this art work") or to prevent bad actors from repudiating their actions (e.g., for fraudulent purposes or to avoid

accountability). Blockchains use cryptographic recordkeeping, consensus and principles of distribution in an effort (not always guaranteed) of finality, completeness and immutability of records entered into the ledger as a basis for trust.

Blockchain's Interacting Trust Layers

Figure 1. Three-layer trust model of blockchain technology (Source: Lemieux, rendered by Hoda Hamouda).

It is a unique intertwining of social design and engineering, recordkeeping design and engineering, and technical design and engineering (see Figure 1) that enables blockchains to operate as a system of trust. Thus, the design of blockchains can be said to rely upon three interacting "trust layers": a *social layer*, the layer at which social actors interact with one another and determine how much information they need, and in what form (e.g., by social convention, how much from the blockchain system and how much from other sources external to the system) in order to be able to trust and take action on the basis of trust; a *records layer* that supplies the information that social actors have decided they need to obtain from the blockchain system to give them confidence to act; and a *technical layer*, the technical means by which social actors interact and create, store and obtain information about those interactions as tamper-resistant and non-repudiable proof of facts about acts (see Figure 1). Each of these layers interoperates with the goal of achieving trusted transactions. Due to their capacity to alter existing technical, records, and social trust relations, blockchains hold the potential to disrupt a myriad of social, political, and economic domains.

The primary focus of this study is on the records layer; however, to understand this layer, and the means by which blockchain-based records can be managed effectively, it is important to understand the other two layers and, to some extent, how the layers interact with one another in the design and operation of blockchain systems. As information professionals will likely understand the technical layer of blockchain systems least well because of the emerging nature of this technology, the remainder of this chapter discusses technical aspects of blockchain systems in broad terms, referring as appropriate, to aspects of the social and records layers that interact with, and are shaped by, the technical layer.[18]

How blockchain transactions are executed

When individuals want to undertake a transaction on a blockchain network, such as transferring a unit of cryptocurrency or ownership of a piece of property to someone else, they transfer control of the asset by transferring the blockchain representation of it (sometimes called a token) using asymmetric (or PKI) cryptography – a type of cryptography that relies upon use of a public key and a private key – from their blockchain address to the other person's blockchain address. An address is denoted by the hash of a public key and some additional data and functions somewhat like a zip or postal code indicating the destination of a particular transfer of value. For each public key there is a matched private key. The individual uses their private key to digitally sign the transaction (see Figure 2) to authorize and make the transaction happen.[19] The digitally signed transaction (rendered as a transaction output hash) is then bundled together with other digitally signed transactions, and then validated, confirmed, and entered into the ledger, thereby making an entry to indicate that the transaction has occurred in the copy (called replica) of the ledger usually held by all computers forming the blockchain network.

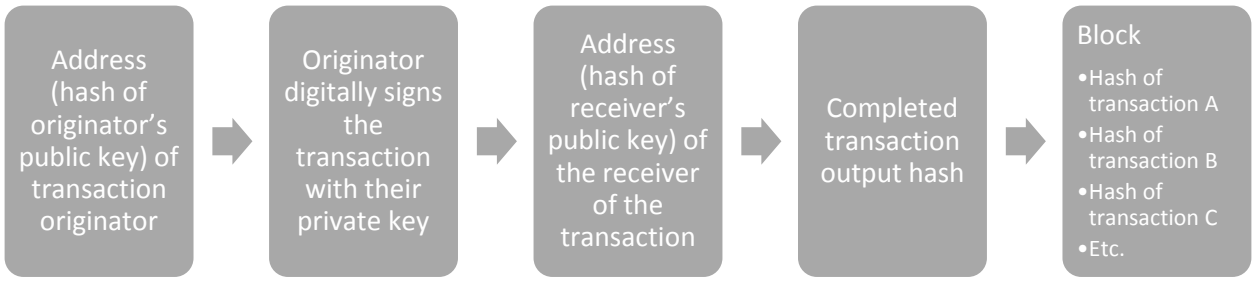


Figure 2. Transaction processing using public-private key pairs on the blockchain (Source: *Lemieux, 2017).*[20]

Blockchain Technical Features

From a technical perspective, blockchains have three important features that renders them worthy of trust. The first is that blockchains operate as distributed systems – a system in which the technical components of the ledger are distributed across a network of computers comprised of equal peers (called nodes) that function in a shared and synchronized manner (see Figure 3).[21] In practice, this means that full or partial copies of the ledger exist on two or more nodes.[22] The distribution of copies of the ledger across nodes, often under independent control and in diverse locations, provides redundancy, protecting from loss of the ledger, and also makes it difficult to manipulate ledger entries, since a number of nodes would have to simultaneously collude in order to alter the record. In theory, the higher the number of nodes participating in the network, the more difficult this type of manipulation is to carry out.

Some blockchains may exhibit a more centralized network and storage topography. The IOTA blockchain, the "Tangle," for example, currently incorporates "Permanodes," though there are plans to eliminate these over time, which act as super-nodes of special importance because they store full replicas of the blockchain ledger. This makes such blockchains less resilient since these super-nodes can present single points of failure and might be less tamper resistant. It is possible to alter the ledger by changing one or a few of the super-nodes rather than having to alter ledger replicas stored on all nodes.[23] On the other hand, such a design makes the blockchain better suited to cases that require high transaction with short-term evidential value scalability

(e.g., often the case with 'Internet of Things' use cases where there will be a high number of communications between devices).

In some cases, designers of blockchain systems compensate for the greater vulnerability of less distributed networks and storage topographies by incorporating compensating controls, such as allowing only authorized and trusted nodes to participate in the blockchain network (i.e., operating a "permissioned" blockchain; see *infra*). In this way, greater information about transacting parties provides some of the information needed to achieve trust. Such design considerations are taken at the level of the social layer of blockchains, typically by core developers or founding parties who establish the governance and technical protocols that determine how a given blockchain system will be configured to operate.[24] This is one example of how design considerations and trade-offs involve considerations that must achieve a delicate balance of social, recordkeeping, and technical features that deliver presumptions of trust.

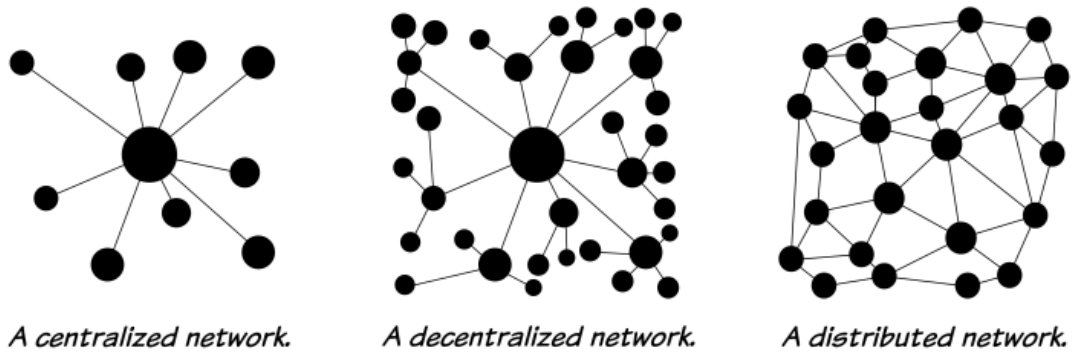


Figure 3: A comparison of the topography of centralized, decentralized and distributed networks (Source: Baran, 1964).[25]

Blockchains also use asymmetric cryptography to achieve greater levels of trust.[26] [27] Cryptography is used when a transaction record is digitally signed by an individual wishing to execute a transaction using a blockchain system (see *supra*). It is also used to chain together blocks of transaction hashes to create a block hash – a 256-bit random number computationally generated from input information – thereby creating an append-only, sequential chain. Each chain in a blockchain starts with an original, or genesis block, followed by a time ordered sequence of blocks. The blocks of entries are digitally signed in a manner that cryptographically

links them together. This forms a long continuous chain of hashes, hence the name blockchain (see Figure 4).[28]

This process of cryptographically chaining together blocks of transaction entries makes tampering difficult, because a change to the input data at any point in the chain will produce a different hash, thereby making the fact that the original input data has been altered very obvious. As a result, ledger entries can only be added, never removed, since removal of entries would change the input data and invalidate the original hash and all subsequent hashes in the chain. This protects the integrity of the ledger and also makes repudiation of transactions difficult, but as we will discuss later on, also complicates removal of information in the context of records disposition or compliance with privacy regulations. Distributed ledgers, which are also sometimes included under the general rubric of blockchain technology, do not necessarily organize transaction entries into blocks, as in the classic blockchain structure, but they often still cryptographically link together transactions to provide a basis of trust in the ledger.

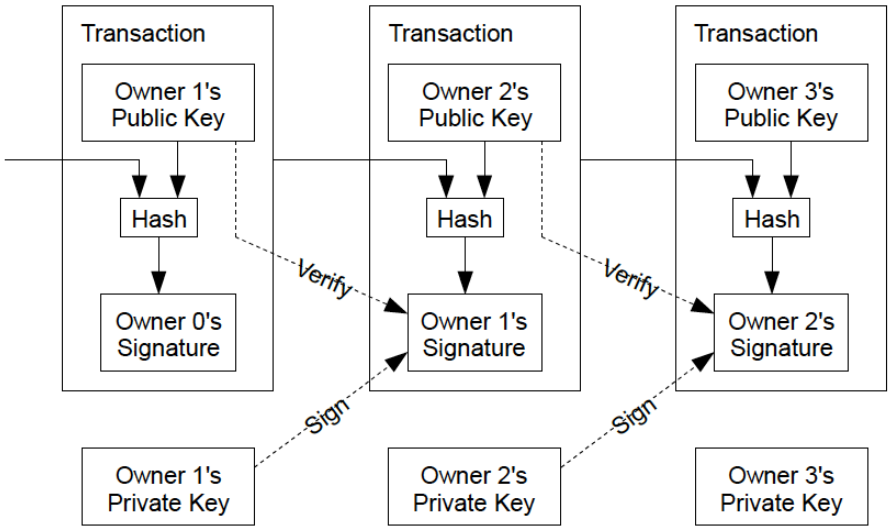


Figure 4. Blockchain structure (Source: Nakamoto, 2008)[29]

Finally, information is only entered into a blockchain ledger once it has been validated and confirmed through a process called consensus. Each blockchain has a consensus mechanism that enables agreement among computers operating the blockchain client software (the nodes) that a

transaction is valid and that there is a consistent set, and a guaranteed ordering, of the transactions to be stored in the blockchain.[30] [31] A consensus mechanism is necessary because, in a distributed system comprised of many independent participating nodes that do not necessarily trust one another, there must be some way to determine how the nodes come to an agreement about the contents, ordering and insertion of transactions in a blockchain, and the means by which any changes to what has been written to the ledger will be detectable. This challenge is generally referred to as the Byzantine General's Problem.[32]

The rules relating to which transactions are considered valid and how consensus is achieved are usually socially determined for any given blockchain (i.e., agreement of influential actors such as core developers or "miners" in a public blockchain or by means of a contract between a consortium of business partners in a private blockchain) during the creation of a blockchain system, and may be updated over the lifetime of the system.[33] These socially determined aspects of consensus have a profound effect upon the operation of the technical aspects of blockchains. In the Bitcoin Blockchain, disagreements about what transactions should be considered valid and how they should be confirmed has led to both social divisions in the Bitcoin Blockchain community and technical divisions in the Bitcoin Blockchain itself (i.e., "forking" of the blockchain into "Bitcoin Core" and "Bitcoin Cash").[34]

Forking occurs when there is some change to client software that encodes the agreed criteria for the creation of valid transactions. If a change to these criteria occurs during the lifetime of the system, individuals operating older nodes may choose to continue to use older client software instead of installing the new client software. When transactions generated by nodes using older client software are no longer recognized as valid, and cannot be confirmed by nodes operating new client software, this is referred to as a "hard fork," a situation that leads to the creation of two separate chains of transactions from a shared block: one chain that operates according to the validation rules encoded in the old client software and another that operates according to the rules encoded in the new client software.[35] In a "soft fork," on the other hand, a new version of the client software does not fundamentally alter what is considered to be a valid transaction and does not create a fork (despite the use of the word fork in the name).[36]

The actual mechanism by which consensus is achieved varies by the type of blockchain system. Delegated Proof-of-Stake, Paxos Algorithm, Practical Byzantine Fault Tolerance, Proof-of-Authority, Proof of Burn, Proof-of-Capacity, Proof of Ownership, Proof-of-Stake, Zero

Knowledge Proof, and Proof-of-Work are among the many mechanisms that can be used. Each has its own strengths and weaknesses.[37]

In the Bitcoin Blockchain, the oldest of the public blockchains, consensus is achieved by "Proof of Work" (PoW). In this consensus mechanism, the creation of new blocks of transactions requires that a difficult cryptographic or computationally hard puzzle is solved, i.e., figuring out what random number – or nonce - when combined with the block header produces a specific output hash value. The node – or miner, as such nodes are called in the Bitcoin Blockchain - that solves the puzzle first becomes the "leader node," or node to create the new block and propagate it out to the other nodes in order to update the distributed ledger. To incentivize miners, who have to make significant capital expenditures in infrastructure and electricity in order to mine, the first miner to solve the PoW puzzle receives a "block reward" as well as transaction fees connected with individual transactions included in the block. Since there is no known short-cut to solving the PoW puzzle, it requires a great deal of computing power to complete. This makes PoW consensus very secure, but it is also the focus of criticism: the amount of electricity required to compute the solution to the puzzle is said to be on the order of the electricity consumed by the country of Ireland.[38] Another criticism is that the huge investments now necessary to operate as a miner lead to a concentration of power. Small miners have formed big groups (mining pools) to reduce variation in the block reward. This has given them the ability to establish policies (e.g., filtering, postponing) on certain transactions which could lead to abuse of power and which some have said gives them an unacceptable level of control.

In private blockchains, consensus commonly is achieved by means of "Byzantine Fault Tolerance." This approach originates from the need to protect distributed systems against the threat of "Byzantine failure," wherein individual nodes in the network might be delayed in receiving new information from other nodes or might be sent maliciously-constructed information from malicious nodes. Byzantine consensus mechanisms, such as the Practical Byzantine Fault Tolerance (PBFT) mechanism, require that the number of nodes in the network be known, for the number of malicious nodes to be small (typically, less than one third of the total number of nodes), and for every node to establish evidence of the validity of the transaction from a quorum of other nodes, typically a clear majority.

Consensus mechanisms are one of the main technical means by which trust is achieved in blockchain systems. They enable blockchains to "transfer the burden of trust from institutions

and organisations, who may have a vested interest in not acting in a trustworthy manner, to a technological solution which is not controlled by the interests of one single entity."[39] In the case of PoW, trust can be placed in the fact that ledger records have not been tampered with because any change in the input value used to solve the PoW puzzle would produce a different output hash value. As all of the output hash values, or block hashes in a blockchain are cryptographically linked together to form a long sequentially ordered chain, changing any input value anywhere along the chain invalidates all the subsequent output hash values. Any alteration of a ledger entry thus would be very evident because the hash values produced from the altered input would no longer produce the correct output hash value. A malicious miner who wishes to alter ledger records undetected would have to alter the target ledger entries, wherever they are stored in the chain, and then race to re-compute or re-solve all the subsequent PoW puzzles and then propagate out the altered ledger entries before a legitimate miner is able to solve the puzzle for the next legitimate block. It is said that this requires that a miner control at least 51% of the network (and thus a successful alteration of the ledger is called a 51% attack). Given the amount of computing power it takes to solve just one PoW puzzle, an attack of this nature would require more computing power than currently exists to attack the Bitcoin network, though some sources speculate that quantum computing may make it possible to launch such an attack in the future. Smaller networks where the amount of computing power needed to overcome the network is lower are vulnerable to such attacks, however.[40]

Byzantine Fault Tolerance consensus mechanisms are not as tamper-resistant as PoW consensus, since much less effort is needed to alter ledger entries stored on nodes in the blockchain: an attacker only needs to gain control of one-third of the nodes comprising the network. Typically, therefore, Byzantine Fault Tolerance consensus is used more often in private, permissioned blockchain systems, where some of the trust that is lost in using a weaker consensus mechanism is offset by the fact that the social actors (e.g., business partners) using the blockchain system are known to each other and, at least on some level, trust one another (e.g., because they are bound by contractual agreement).

Different Types of Blockchains

There are a wide variety of blockchain systems, each exhibiting slightly different configurations across a range of features. Each of these features involves some trade-off in the

design of a blockchain system, typically in an effort to balance trust with some other desirable, use-case specific design requirement (e.g., efficiency, high throughput, etc.). Appendix A offers a high-level comparative analysis of some of these features in a selection of blockchains.

Among the most important of the features that distinguish blockchain systems is the degree to which ownership and operation is centralized. In some blockchains, all of the technical components of the blockchain are owned and operated by a single entity (e.g., Quorum[41]). These are called private blockchains. Such blockchains are generally less trusted because it is technically possible for an entity that owns and operates all the infrastructure to manipulate its operation in order to alter the ledger, though in practice there may be many socially-defined incentives (e.g. laws, investor disapproval) that would prevent this from happening.

In other blockchains, the technical infrastructure of the blockchain is owned by a consortium of business partners, each operating their own independent node(s) (e.g., Ripple)[42]. In theory, the fact that copies of the ledger are held by different consortium partners who must all collude to alter the record – a less likely scenario than alteration by a single party – makes these blockchains relatively more secure. This, of course, would not be the case if the blockchain were owned by a consortium of partners but the infrastructure was operated by a single entity on behalf of those partners (e.g., when the blockchain operates on cloud infrastructure).

Finally, in the large public blockchains, such as Bitcoin and Ethereum, there is no centralized party or group of parties that is said to own or control the network. Each node, in theory, is under the ownership and control of an independent, autonomous entity. In practice, this may not be the case: Bitcoin miners have formed mining pools in which a large number of nodes are actually controlled by a small number of miners.[43] [44] Moreover, as Walch has observed, core developers write the code and establish the rules by which blockchains operate. Consequently, core developers actually wield a great amount of control, even though individual nodes may be free to join or leave a blockchain as they please.[45]

Another important distinction between different blockchains is whether they are "permissioned" or "permissionless." Public blockchains are called permissionless because any participant (node or end user) may use and access the network; that is, participants do not require special authentication or authorization to access, read, write and participate in transactions and in the consensus process.[46] Examples of permissionless blockchains are Bitcoin and Ethereum.

Permissioned blockchains, on the other hand, are ones in which nodes must have a member identity and participants must authenticate (e.g., enter a user name and password) to gain access and must have authorization to use the system resources. These are often private blockchains, meant for the use of only members of a shared ledger - a single ledger that multiple participants may access and use. Permissioned blockchains have membership services that manage the identity, privacy, confidentiality and auditability within the system.[47]

The Blockchain Technology Stack

Blockchain systems comprise a "technology stack" that combines a number of interacting blockchain and non-blockchain components besides the core blockchain processing layer, which is often identified as "Layer 1" of the blockchain technology stack, described in the previous sections. Figure 5 provides a high-level overview of some of the distributed components of blockchain technical systems that add functionality for transaction processing and recordkeeping.[48] These include distributed applications, sometimes referred to as "Layer 3" of the blockchain technology stack, that permit participants to easily interact with blockchains. An example of a common distributed application is wallet software which is used to hold and manage cryptographic keys.[49] Smart contracts also add functionality.[50] These are computer programs stored in a blockchain that express transaction procedures that, once triggered and executed, result in an entry in a blockchain ledger indicating the execution of the transaction.

Through the use of smart contracts, many kinds of contractual clauses may be made partially or fully self-executing and self-enforcing. A smart contract might represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction; however, the legality of such contracts depends entirely upon how they are treated under the law in each legal jurisdiction.

Smart contracts sometimes rely on "oracles."[51] These services are designed to supply trusted external data to a smart contract or blockchain system. "Asset registries" link digital currencies to other assets or records on top of a distributed ledger.[52] Off-chain services provide secure means to access capabilities outside a blockchain system, such as trusted data sources, like oracles, or functions, such as data storage.[53]

Sidechains, sometimes called "Layer 2" blockchain technologies, are physically separate blockchains associated with a core blockchain and can participate in transactions with it,

typically in both directions.[54] Often sidechains are used to remove responsibility for processing all transactions from the core blockchain processing layer in order to add functionality, such as the ability to process higher volumes of transactions (e.g., Bitcoin's Lightning Network). As such, sidechains often use different protocols for how nodes reach consensus, communicate with one another and store data.[55]

In contrast, subchains are logically separate chains that form part of a blockchain.[56] Each subchain may be owned by a different entity and may be accessible to a different set of users. Nodes may be set up so that some nodes participate in certain subchains and not in others. The result of this configuration is that the ledger on some nodes contains transactions for that subchain while the ledgers on other nodes do not. The purpose of subchains is to enhance privacy.

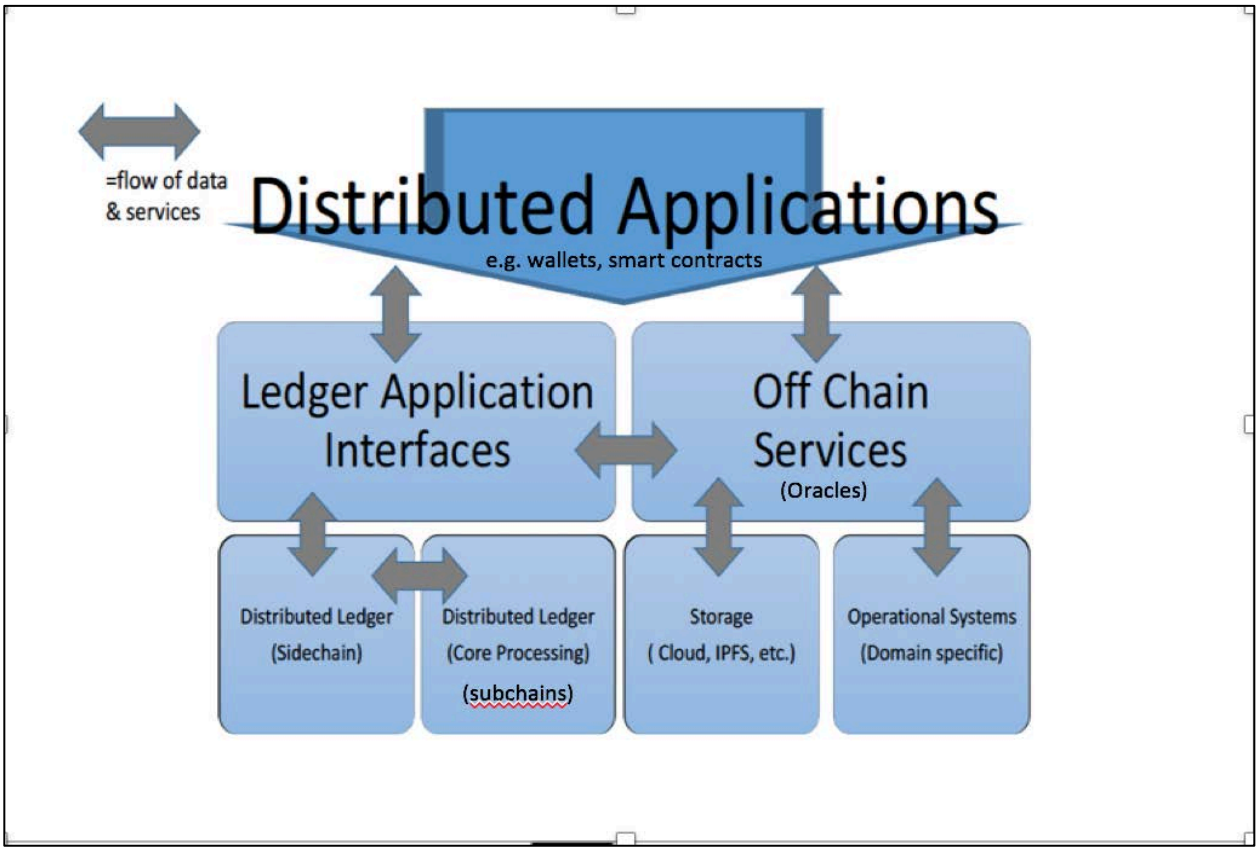


Figure 5. Generic Blockchain Recordkeeping Reference Architecture (Source: Lemieux, 2017, updated for this study).

Conclusion

This chapter has provided an overview of blockchain technology as a "technology of trust" to provide a foundation for understanding the topics covered in subsequent chapters. In this chapter, we have covered blockchains' main technical aspects and how these relate to records and data storage and protection, as well as their relationship to social and business aspects of the operation of blockchains. In the next chapter, we delve more deeply into a fundamental question of interest to records and information managers; namely, how are records created and stored on blockchains.

Chapter 2: The Creation & Storage of Blockchain Records

In order to be able to manage blockchain records effectively, records professionals need to understand what records are actually generated by and stored in blockchain systems. As it turns out, this is not easy. It is a task that is complicated by four key factors: 1) differences among various blockchain systems in terms of how they generate and store records, 2) the distributed and decentralized architecture of blockchain systems, 3) the design choices of blockchain solution developers about what and how to record and store records in blockchain systems, and 4) the way in which the nature of records and recordkeeping is being transformed by blockchain technology.

Differences Among Blockchain Records Generation and Storage

Bitcoin is the original implementation of a blockchain system. As discussed in chapter one, it was designed to serve as a ledger. A ledger is a very particular and circumscribed type of record, being a document containing entries of debits, credits, and other financial transactions, typically organized into separate accounts.[57] Like all ledgers, blockchain ledgers were designed to generate these simple records of financial debits and credits. They were *not* initially designed to store a large amount of data. Most blockchains can store these simple records of credits and debits, or transfers of value from one account to another. Typically, these are generated and stored as hashes, as described in chapter one. For purposes of clarity, we call these types of records "ledger records," to differentiate them from transactional records. Ledger records can be defined as a record comprising hashes of transaction records or references to transaction records

recorded on a blockchain or distributed ledger system. Transaction records can be defined as a record documenting any type of transaction, and records can be defined as per ISO 15489 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."[58]

What these simple ledger records represent in the real-world, of course, varies with the use case for a given blockchain solution. In some cases, the ledger records will represent the transfer of cryptocurrency (i.e., a debit from one account and a credit to another). In other cases, the ledger records may represent the transfer of some other kind of real-world asset, such as the movement of a commodity, such as diamonds, along a supply chain, or the transfer of property from a seller to a buyer. In Ethereum, it is possible to store not only transactions, but computer programs, called "smart contracts," that represent transactional procedure(s), wherein the outcome of any execution of the program is recorded on the distributed ledger as a ledger record.[59]

Even though Bitcoin, and its underlying technology, blockchain, was not designed to store anything but these simple ledger records, from the outset Bitcoin was used to embed other types of data using Bitcoin transactions and the ledger records they generated as a means of conveying messages, or to embed data that provided additional contextual information about a Bitcoin transaction and its associated ledger record. The most iconic example of this was the original message embedded by Satoshi Nakamoto into the first block of the Bitcoin Blockchain: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks," which referenced an article on the front page of the times from January 3rd, 2009 about the UK Government's bailout of British banks following the financial crisis of 2007-2008.[60] Another iconic insertion of data into the blockchain is the ASCII image of former US Central Bank Governor, Ben Bernanke, that appears at Block 3, along with an image and obituary of Len "Rabbi" Sassaman, a cryptographic researcher and cypherpunk.[61] Reviewing the data that has been embedded into the blockchain over time makes for fascinating reading.

As the number of use cases for the core technology underpinning Bitcoin has expanded, the need to generate and store different types of data has emerged. This has included everything from images to metadata about transactions, some of which comprises personally identifiable information. Each blockchain has different capabilities regarding the generation and storage of records. According to Sward, in Bitcoin Core (the original Bitcoin protocol), there are five

different scripts – or coding languages – each of which can be used to embed data into the blockchain; these are: Pay-to-Public Key (P2PK); Pay-to-Public-Key-Hash (P2PH); Multi-Signature; Pay-to-Script Hash (P2SH); and OP_RETURN. The most common method by far is the use of the OP_RETURN code, which currently allows for the storage of 80 bytes of data. As Sward explains "OP_RETURN allows a small amount of data to be included in each transaction, creating a provably un-spendable UTXO [transaction output] that miners do not need to track, and that does not require a non-dust burn value [use of Bitcoin in order to facilitate the data storage]."[62]

Public blockchain developers have been split on whether the insertion of additional data into blockchains is a good idea. As Andreas Antonopoulos states, "The use of bitcoin's blockchain to store data unrelated to bitcoin payments is a controversial subject. Many developers consider such use abusive and want to discourage it. Others view it as a demonstration of the powerful capabilities of blockchain technology and want to encourage such experimentation."[63]

The embedding of information on blockchains has given rise to concerns about the use of blockchain recordkeeping in relation to compliance with EU General Data Protection Regulations (GDPR) as well.[64] As one blockchain commentator put it, "Immutability is, of course, a virtue. It is immutability that gives the blockchain openness . . . However, there is a downside to the coin. All the data that applications write to the blockchain remain there forever. You have played words game - the blockchain remembered this. You placed information in the social network - it is permanently stored in blockchain, even if you later deleted your profile."[65] Thus, blockchain immutability may conflict with EU GDPR requirements relating to destruction of information no longer needed to meet the needs for which it was gathered in the first place, or meet rules relating to the "right to be forgotten." As will be discussed in chapter nine, blockchains are not inherently in conflict with GDPR specifically nor privacy requirements in general. In fact, blockchains, like Bitcoin, were originally designed to be privacy preserving. Rather, the devil is in the design; that is, what choices designers or developers make about what is recorded on the blockchain in the first place can determine whether or not a solution will be compliant with GDPR or other privacy requirements.

Developer Design Choices

Designers and developers of blockchain solutions have choice when it comes to how and where data is recorded in a given blockchain ledger or system. For example, as a result of the structural limitations of OP_RETURN and other methods of embedding data into the Bitcoin Blockchain, many blockchain developers simply embed hashes of data that form cryptographic links – that is, references to data constructed using a cryptographic hash function technique - to other transactions on the blockchain or to external data stores.[66] In other blockchains, designers/developers have created a database within the blockchain ledger capable of holding much larger amounts of data (e.g., Chromaway's Postchain solution).[67] It is important to bear in mind, that whatever is stored in the blockchain, be it a ledger record, a transaction record, supporting documentation, or other data, it is not simply stored in one place, but usually will be replicated on all the nodes that participate in the operation of the distributed ledger. In small, private blockchains operating according to the Practical Byzantine Fault Tolerance consensus mechanism, this may be as few as four nodes while in large, public blockchains such as Ethereum, this may be in the order of 30,000 plus nodes.

In other words, the type, amount, and place of data storage in blockchain ledgers and entire blockchain solutions, though constrained in some ways by the technical structure and capabilities of different blockchain solutions, is very much a question of choice. Each designer/developer may make a different choice about what data to store in the ledger or elsewhere, and in what form (e.g., as clear text, cyphertext, a hash link, etc.) according to the requirements of a particular use case or other design and technical considerations. For this reason, it is incorrect to say that blockchains are fundamentally incapable of being in compliance with GDPR or that they are inconsistent with the "right to be forgotten." It is perfectly possible to design a blockchain solution that is compliant with privacy regulations and the right to be forgotten. For example, designers and developers can simply avoid placing personally identifiable information on an immutable ledger, as is envisioned by solutions designed to support self-sovereign identity.[68]

The Distributed and Decentralized Blockchain Technology Stack

If blockchain solution designers and developers can simply choose not to record data in a blockchain ledger that is not related to a financial or other transaction, how can important

supporting documentation or contextual metadata be linked to a ledger record? If contextual metadata are not embedded into a blockchain ledger to provide an intellectual link to the procedural context of a transaction, where should this data be stored? Designers and developers of blockchain solutions do not necessarily give a great deal of thought to these questions in relation to their implications for the trustworthiness, preservation, and accessibility of records, being more concerned with transaction processing efficiency and other technical concerns. Here, as in choices about how to embed data into the core blockchain processing layer, designers and developers can make choices – choices which will have consequences for managing records and recordkeeping.

As discussed in chapter one, blockchain systems are comprised of a complex "technology stack" that combines a number of interacting blockchain and non-blockchain components. Figure 5 in the previous chapter provides a high level overview of some of the distributed components of blockchain technical systems that add functionality for transaction processing and recordkeeping.[69] Given the complex distributed and decentralized architecture of blockchain systems, records can be scattered across a broad array of systems and infrastructural components. Examples of where records may be stored, and comments on their advantages and disadvantages, include:

- InterPlanetary File System (IPFS): IPFS is a distributed file system technology based on Distributed Hash Tables and the BitTorrent protocol. This is a peer-to-peer protocol in which peers coordinate to distribute requested files, much as Bitcoin nodes coordinate to record transactions on a distributed ledger. And, as with Bitcoin, peers can be located anywhere in the world. It allows peers to combine file systems on different devices into one, using content addressing. Among its advantages are that each blockchain node stores only those files that it needs, plus any metadata about the location of files on other devices. Among the disadvantages of IPFS is that after the file is seeded to BitTorrent, data storage by other devices is not guaranteed, to guarantee the provision of a file to others its originator must remain active and stay online.[70] Files are also static (unchangeable), and deleting a file is not supported.
- Distributed databases: These are databases, like MongoDB, Cassandra, or REthinkDB, wherein the client works with one of the replicas, and the data is automatically synchronized with other nodes. There are several advantages to these types of databases, including that

they are fast, very scalable and resistant to inaccessibility of individual replicas. Among the disadvantages, however, is that it is impossible to create a fully distributed database that ensures consistency, availability and partition tolerance. As Kochin observes, “In all the above, this type of database may seem ideal for use in a blockchain. Nevertheless, imagine that someone in the well-established cluster of such databases added a malicious replica, which begins to inform other replicas in the cluster that all data must be deleted! All other replicas obediently delete all data, and the database will be hopelessly corrupted. That is, such a coordinated work of replicas is possible now only in a trusted environment (a cluster of such databases is not Byzantine fault tolerant). If a maliciously working replica is placed in a cluster, it can cause the destruction of the entire cluster data.”[71] The use of a Practical Byzantine Fault Tolerance consensus mechanism, like that used in some private blockchains, among nodes helps guard against this risk.

- BigChain DB: or IPDB (InterPlanetary DataBase) is a specific solution with a very high transaction speed according to its creators (1 million/sec), as well as large storage capacity (due to distributed storage with partial replication). BigChain DB gets these benefits through a simplified consensus when building blocks, and by storing all blocks and transactions in an existing noSQL database implementation - RethinkDB or MongoDB. However, since each node may have full rights to write to the common data store, which means that the system is not Byzantine fault tolerant, BigChain DB suffers from the same weakness as noted above for distributed databases.[72]
- Cloud storage: Cloud comprises, “A broad range of infrastructures and services distributed across a network (typically the internet) that are scalable on demand and that are designed to support management of high volumes of digital materials.”[73] The main advantage of cloud storage is that it is a mature technology now, the risks of which are relatively well understood.[74] The main disadvantage is that it centralizes data storage, which eliminates many of the advantages of using blockchain technology in the first place.

  Table 1 provides a framework for understanding the different types of records that can be generated from and stored in blockchain solutions.

Table 1. Types of blockchain records, examples and location

Supporting Documentation	Transaction Records	Ledger Records
Description: Information that provides background or supporting information relevant to the execution of a transaction and that has an archival bond to a transaction record)	**Description:** Representations of transactions in the form of records, which is "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 15489, 2016)	**Description:** Hashes recorded and stored in a blockchain, which may represent and be intended to provide proof of executed transactions, or of the existence of an asset or claim. These comprise the entries in a distributed ledger.
Example: images of a property offered for sale	**Example:** sale contract used to transfer ownership of property	**Example:** transaction hash on a blockchain representing the completed/executed sale contract transferring property from a seller to a buyer
Location: may be stored in an organizational database, a cloud data store, or in a distributed data store such as the Interplanetary File System (IPFS)	**Location:** may be stored in a blockchain as a smart contract, or as a document or hash link to a document embedded into a ledger transaction record in cleartext or ciphertext, or off-chain in a similar manner to supporting documentation	**Location:** on a blockchain or distributed ledger

Ubitquity's blockchain solution for real estate (see Appendix B.1) exemplifies the distributed and decentralized architectures typical of blockchain ecosystems. The solution comprises a web front end (see Figure 7) that captures information taken from the Municipality of Pelotas' real estate registry's general real estate registry. The general real estate registry is a traditional centralized database, containing the registration number for a property, the name of the owner, the address of the property, as well as an image of the property, photos of books, and the title certificate.

The client-facing web front end of the blockchain solution communicates with a web server and backend storage. Ubitquity's backend storage hosts the images of the property as well as PDFs of deeds and other supporting documents relating to the property. These components, although they contain information relating to Brazilian citizens generated by the Pelotas land registry, are stored on a server physically located in the US which is owned and operated by Ubitquity. Ubitquity's web server communicates with a Colu Application Programming Interface (API) server, translating what is entered into the web front end into a format that permits the

tokenized assets - crypto-assets (i.e., land) - and transactions involving those crypto-assets (i.e., land transfers) so that they can be recorded on a blockchain.

Colu[1] is an Israeli company that offers a "coloring scheme" that allows for association of unlimited amounts of metadata (e.g., the name, address, photo of property, location data, property value, etc.) using publicly available torrent files. In this way, data or metadata relating to a crypto-asset can be stored and associated with a transaction using BitTorrent. Data are uploaded to BitTorrent through a process called "seeding", which in theory, is handled by Colu. As previously mentioned, the continued existence of the data online depends upon at least one, preferably many, peers holding the downloaded data and continuing to participate in the public BitTorrent network. While conducting the research for the case study, one of the magnet links - a link used to associate a colored Bitcoin transaction to related data stored using BitTorrent was tested, and it was discovered that the associated data had not been seeded to BitTorrent but rather remained on Colu's servers in Israel. Ubitquity has since addressed this issue.

[1] https://www.colu.com/.

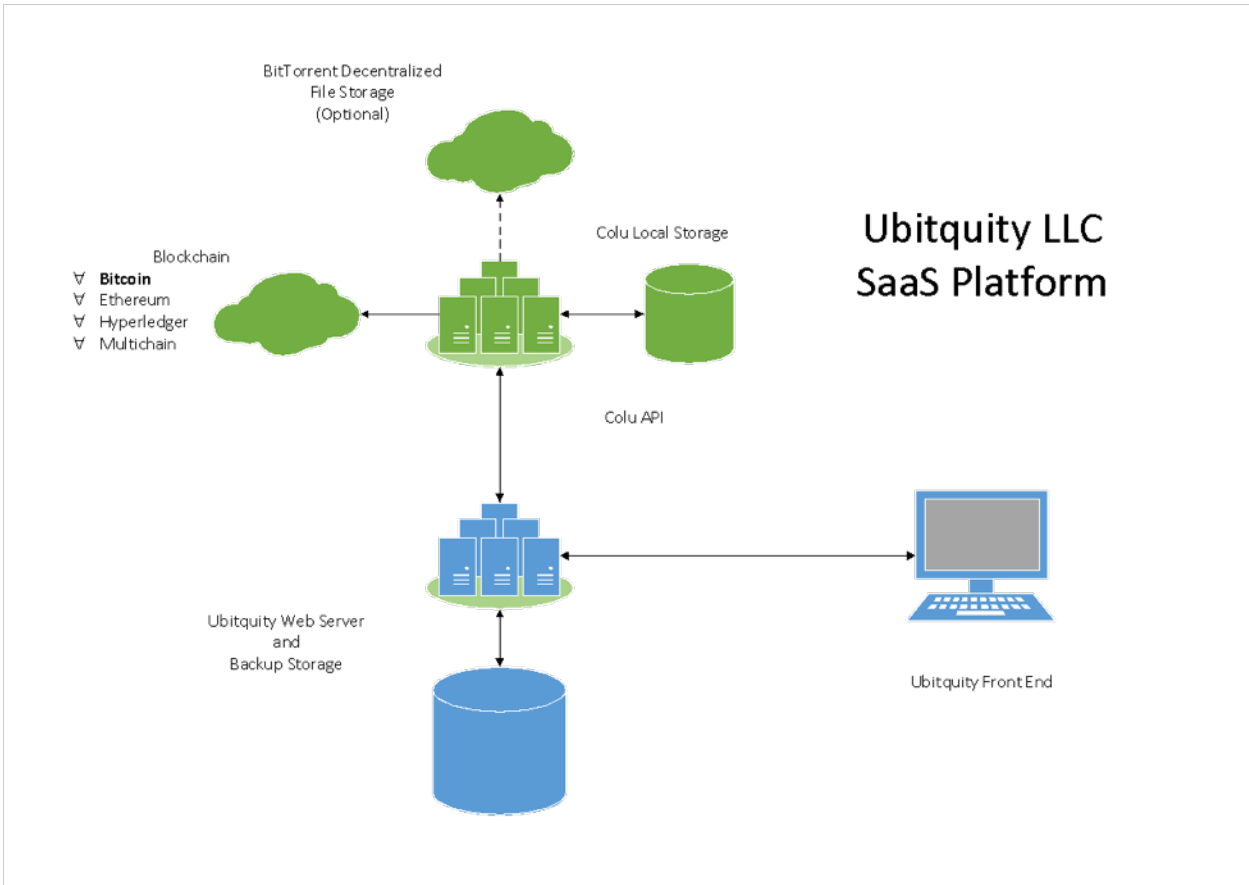


Figure 7: Overview of the Architecture of Ubitquity's Pilot Blockchain Solution for the Pelotas Land Registry in Brazil (Source: Ubitquity)

The architecture of Ubitquity's pilot solution for the land registry in Pelotas illustrates the complexity of a distributed and decentralized blockchain architecture. Records relating to Brazilian land transactions, including data that personally identifies individuals, did not reside in a single, centralized database. Rather copies, and various representations (both encrypted and unencrypted) of the records and associated metadata could be found on Ubitquity's servers in the US, Colu's servers in Israel, and on nodes throughout the Bitcoin Blockchain network (~10,000 at time of writing). If the data had been seeded to BitTorrent as planned, it would also have existed across the network of computers supporting the BitTorrent network (i.e., several thousands of nodes, potentially).

Blockchain technology thus takes distributed computing to the extreme, magnifying issues of custody, ownership, and trustworthiness and privacy that have been identified in cloud

environments. In a blockchain technical ecosystem, information processing happens on a complex technological stack in which different technical components may be in the custody of, and operated by, very different actors. Some of these may be under the control of a single organization, others under the control of business partners who are members of a blockchain consortium, and still others under control of unknown third-party actors. An organization's records literally could be in the custody of thousands of independent actors over which records creators exercise little or no control.

Further, the consensus mechanism and other protocols or standards determining how the blockchain or distributed applications, such as smart contracts operate, may not be within the decision-making purview of the creator (or the creator's designated records and information professional). Instead, these may be decided by remote (and even unknown) third party developers. In many cases, these protocols and standards are still unstable, and thus the reliability of organizational records created using blockchain technology could be very difficult to establish with any certainty. This situation has caused some observers to call for developers to have fiduciary responsibility, which would enable organizations to sue if blockchain protocols or contracts caused harm or loss.[75]

The above-noted issues seem complicated enough for records creators and records and information professionals to address, but blockchain technology may introduce even more challenging issues. In the Ubitquity case study, and in many existing blockchain solutions, records creators are still the legal owners of the records they generate, if not the custodians of them. Some proponents of blockchain, however, advocate for a world of self-sovereign identity and data, in which even if a record is generated by a specific organizational creator, the legal owner and custodian of the records will be the person who is the subject of the record. This new data architecture is a response to the extreme centralization of data and associated infringements of personal privacy that have occurred in recent times.

This new world of self-sovereign data poses many potential challenges for records and information professionals that have yet to be fully explored. For instance, if a records creator generates records, do they retain some legal ownership of those records even though the records will now be in the custody and control of data subjects? Do records creators continue to be responsible for compliance with regulatory requirements, such as GDPR in a self-sovereign data world? Blockchains require the management of cryptographic keys, in particular, and the careful

preservation of private keys. Are individuals willing and able to take on this kind of responsibility? What happens when an individual loses their private key and there is no backup? Will they lose all their records? How will individuals and society preserve records that may be stored in millions of distributed and decentralized data stores? How can access to such records be maintained for personal and business purposes or as collective memory? As a society, we do not yet have the answers to these questions, but we will need to find them quickly given the pace at which blockchain technology is being adopted.

The Distributed and Decentralized Record

Blockchain takes us from the distributed and decentralized solution stack to the distributed and decentralized record as well. Instead of all the elements of intellectual form being embodied in a single unitary entity – e.g., the record as it was known in the paper recordkeeping era - in the blockchain era the elements of intellectual form may be scattered and distributed. To explain further, using diplomatic theory,[76] we can say that records possess the following intellectual components:

- Acts: An action that the record participates in or supports
- Persons: The agents, human on non-human (i.e., juridical), who agree and give rise to the record's creation (i.e., author, writer, originator, addressee, and creator [agent who accumulates records, either by creation or receipt, in the course of carrying out business])
- Archival Bond: Network of relationships among records related to the same acts, and to the acts themselves
- Context: Juridical-administrative, provenancial (creator), procedural, documentary and technological
- Medium: The technology by which the content and other components of the records are conveyed from addresser (sender) to addressee (receiver); a necessary part of the technological context, not of the record
- Fixed form and stable content: Pertaining to the facts which the record captures and represents, and to which it refers.

In a given record, we may observe several intrinsic elements of intellectual form – entitling, title, date, superscription, salutation, subject, preamble, exposition, disposition, appreciation, clauses, attestation, qualification of signature, secretarial notes, invocation, formula perpetuitatis,

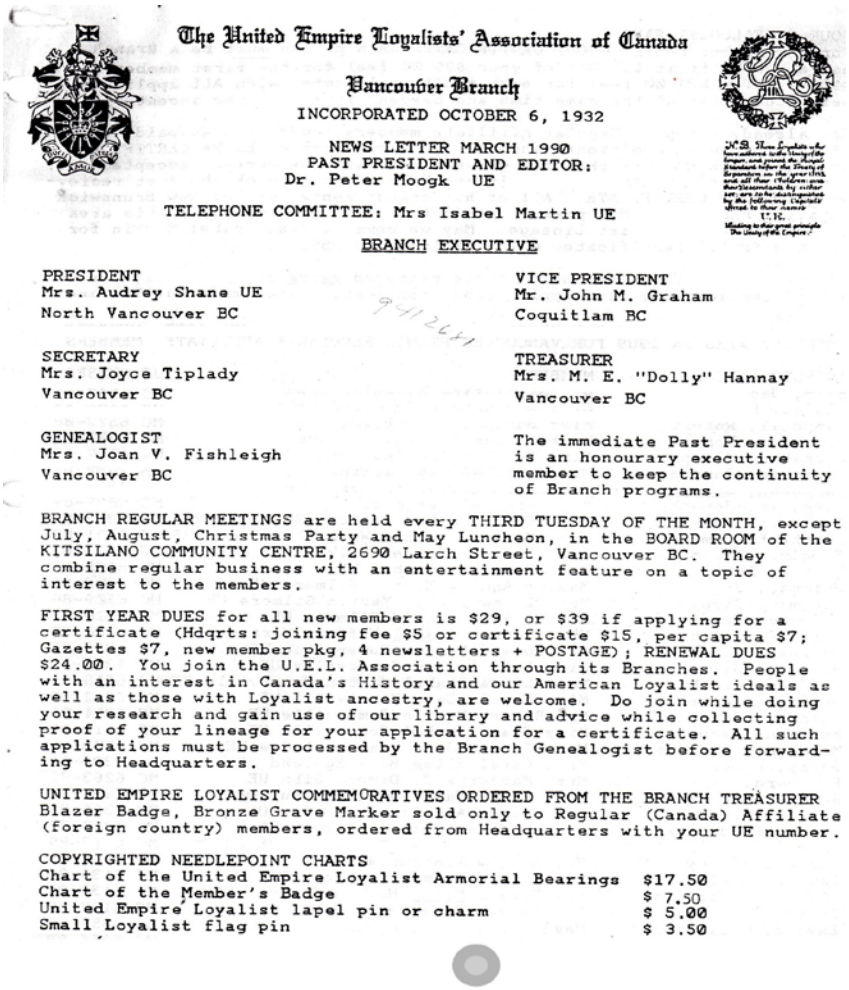
notification, corroboration - that embody all the above aspects. These are the elements of form that determine the appearance and determine its meaning (i.e., the record's semantics).

In traditional paper-based recordkeeping, the elements can be found in a single unitary entity (Figure 6). As Duranti and Thibodeau observe, in the early digital record era, the encoding of digital records no longer produced a fixed and stable documentary form and, as a result, digital records could no longer be preserved as physical objects. They had to be preserved as bit streams that could be correctly processed by computers to be rendered in the proper documentary form; in other words, their documentary form (i.e., the intellectual components of the record) had to be made persistent.[77] This is also true of blockchain records, whose form is computationally mediated.

Duranti and Thibodeau also pointed out that "there are also cases, most notably in the arts, but also in government and science, where interactive, experiential and dynamic systems contain documents whose presentation or rendering always shows some unique or spontaneous variation in content or form. In such cases, one must distinguish between what is output by the system and the document(s) that enable the system to produce its output. Such documents are 'enabling:' they enable the interactions, experiences or processes the system executes. Provided they are properly maintained and managed as intellectually interrelated parts of records aggregations, enabling documents can be considered records." This is also true of blockchain records, wherein various documents comprising the aggregated records (e.g., supporting documents, transaction records, and ledger records) individually, can be considered records and which in aggregate, produce "the record."[78] There is no categorical difference between blockchain records and dynamic, experiential records *qua* records in this regard.

Where matters of blockchain records and matters of the form of paper and digital records up until now begin to diverge is in the locus of the elements of intrinsic intellectual form. In paper records, these occurred as mentioned, in a single unitary document. In digital records up until now, these occurred if not in a single unitary object, at least in a Binary Large Object, or BLOB, the elements of which were reasonably tightly coupled together by virtue of being generated and kept as a single encapsulated "large object." For example, a digitally signed document might be stored in a zipped file, a BLOB, containing the unsigned digital document in XML form together with the digital signature.[79] Even in a distributed computing system, the

BLOB remained a unitary object, which, rather than being rendered asunder is simply replicated on different nodes constituting a distributed system.



The United Empire Loyalists' Association of Canada

Vancouver Branch

INCORPORATED OCTOBER 6, 1932

NEWS LETTER MARCH 1990
PAST PRESIDENT AND EDITOR:
Dr. Peter Moogk UE

TELEPHONE COMMITTEE: Mrs Isabel Martin UE

BRANCH EXECUTIVE

PRESIDENT
Mrs. Audrey Shane UE
North Vancouver BC

VICE PRESIDENT
Mr. John M. Graham
Coquitlam BC

SECRETARY
Mrs. Joyce Tiplady
Vancouver BC

TREASURER
Mrs. M. E. "Dolly" Hannay
Vancouver BC

GENEALOGIST
Mrs. Joan V. Fishleigh
Vancouver BC

The immediate Past President is an honourary executive member to keep the continuity of Branch programs.

BRANCH REGULAR MEETINGS are held every THIRD TUESDAY OF THE MONTH, except July, August, Christmas Party and May Luncheon, in the BOARD ROOM of the KITSILANO COMMUNITY CENTRE, 2690 Larch Street, Vancouver BC. They combine regular business with an entertainment feature on a topic of interest to the members.

FIRST YEAR DUES for all new members is $29, or $39 if applying for a certificate (Hdqrts: joining fee $5 or certificate $15, per capita $7; Gazettes $7, new member pkg, 4 newsletters + POSTAGE); RENEWAL DUES $24.00. You join the U.E.L. Association through its Branches. People with an interest in Canada's History and our American Loyalist ideals as well as those with Loyalist ancestry, are welcome. Do join while doing your research and gain use of our library and advice while collecting proof of your lineage for your application for a certificate. All such applications must be processed by the Branch Genealogist before forwarding to Headquarters.

UNITED EMPIRE LOYALIST COMMEMORATIVES ORDERED FROM THE BRANCH TREASURER
Blazer Badge, Bronze Grave Marker sold only to Regular (Canada) Affiliate (foreign country) members, ordered from Headquarters with your UE number.

COPYRIGHTED NEEDLEPOINT CHARTS

Chart of the United Empire Loyalist Armorial Bearings	$17.50
Chart of the Member's Badge	$ 7.50
United Empire Loyalist lapel pin or charm	$ 5.00
Small Loyalist flag pin	$ 3.50

Figure 6: The unitary record of the "old" paper recordkeeping world (Source: Vancouver City Archives)

Not so in the world of blockchain recordkeeping. The various intrinsic intellectual elements of records form may be scattered across the complex distributed and decentralized blockchain solution stack. For example, a diplomatic analysis of blockchain records suggests it is not atypical to note the following differences of how elements of intellectual form may be treated in blockchain recordkeeping:

- Date: Refers to both the chronological date and the topical date or place where the document was issued. **This is often achieved by the embedded timestamp in the blockheader, but**

also by means of publishing of hashes to external reference sources such as newspapers or social media.

- Superscription: In contractual documents, the superscription is the mention of the first party by name. **Parties are not identified by name in blockchain transactions and are only known by their addresses; however, this information may sometimes be embedded as clear text into transactions i.e., in OpCodes or in unused multisig fields to render it human readable.**
- Disposition: Contains the expression of the will or judgment of the author and communicates the nature of the action and the function of the document. **This is often not evident in blockchain records, which only show that an act has been carried out, and must often be inferred from metadata embedded into a transaction record or supporting documents kept elsewhere. In some cases, text may be embedded in opcode/multisig but often this is just a hash link out to supporting documents. Without this element the archival bond cannot be determined or instantiated.**
- Clauses: These are formulaic phrases which ensure the execution of the act, guarantee its validity, protect against violation of the act, preserve the rights of third parties, and indicate the means by which the document has probative value. They express the obligation of concerned parties to conform to the will of the authority which issued the document. **In blockchain recordkeeping, this is entirely handled by the consensus mechanism.**
- Attestation: This is the means used to validate a document. It usually takes the form of the signature of those who took part in issuing the document: the author, writer, and countersigner. However, for some documents such as account books, journals, and invoices, the process of creation itself validates them. **In blockchain records, this is the digital signature that the addresser of the transaction produces by digitally signing a transaction with their private key. In multisig arrangements, this is the digital signature of all parties who must sign to execute the transaction.**
- Qualification of signature: This is mention of the title and official or juridical capacity of the signer. **This is usually not provided in blockchain, since they operate pseudonymously. However, in some blockchains, such as Hyperledger Indy, where there are "Trust Anchors" and "Issuers" of credentials, this may be represented by the public key of the trusted issuer of a credential.**

- Formula perpetuitatis: Comprises a sentence declaring that the rights put into existence by the document are not circumscribed by time. **In the context of blockchain recordkeeping, this is implied by the placement or recording of the transaction on an "immutable ledger".**

Conclusion

The manner in which records are created and kept in blockchain systems raises many potentially new records and information governance challenges for records professionals and the creators of records. This technology, it can be argued, is also fundamentally altering the records that records and information professionals manage. New strategies and techniques will be needed to address these changes, but the records and information profession and society as a whole are only beginning to grapple with the issues. With increasing use of blockchain technology across a wide range of sectors for a growing number of use cases, it is critical to hold discussions about records and information challenges, and for designers, developers, and policy makers to work with records and information professionals as they develop corporate and national blockchain technology strategies for the future. In the following chapters, this report considers the implications for the changes that blockchain technology is rendering for records life cycle management, ownership and custody of records, records as evidence, retention & disposition of records, and the long-term preservation of blockchain records.

Chapter 3: Blockchain Technology & the Life Cycle of the Record

Introduction

In archival science, there are two main models for the management of records: the lifecycle and the continuum. The first one considers records as objects that, despite the "cycle" concept in its name, presents a linear process view of records' existence, with definite periods for creation, use and disposition. The continuum model suggests notions of the record in different dimensions through time and space without specific divisions or directions. Blockchain-based records can be guaranteed as trustworthy and effectively managed only with adaptation of these two models to the unique challenges presented by blockchain records, and through use of the models in the development of functional requirements for blockchain systems.

This chapter analyzes the applicability of these two models to blockchain-based records and blockchain systems. It begins with providing an overview of the two models, and then analyzes their relevance to blockchain systems, primarily in relation to the Bitcoin and Ethereum public blockchains.

The Records Life cycle

From the beginning of the last century, governments and organizations worldwide faced an explosion in the amount of paper records and had few procedures to address this challenge. The life cycle model emerged as a mechanism to manage the explosion in the volume of institutional records being created. Records professionals in North America, especially in the US, embraced this new model.[80]

The records life cycle describes the sequence of activities required for the record to fulfill two basic functions: as a by-product of the business activity (documenting the activity itself and used in support of that activity), and as a cultural and historical resource for research. From a records life cycle perspective, archives are repositories for records that no longer serve the primary needs of their creators but which, nonetheless, are of potential informational value to researchers. The term life cycle is used to describe the stages of a record's existence from creation or distribution, to use and maintenance, and finally disposition. The model carries the idea of a linear process with a determined period and a definite end that can be destruction or transfer to archives. In the life cycle approach, the creation of records is not considered as a role of the archivist, but rather is solely the responsibility of the records creator. The model sets out a framework in which records have distinct phases of existence and the actions required of the recordkeeper depend upon what phase of the life cycle the records are in.

The most significant feature in this approach is the separation of recordkeeping responsibilities into two professions. At the beginning of their existence, records are created and managed by their creators and stored elsewhere as their use and value gradually decreases. These stages are administered by records and information managers. After the primary stages, records reach a disposition phase where they can be destroyed or transferred and preserved as archives. That is when the role of the archivist begins. The records and information manager has the task of improving business efficiencies through the management of records as input needed for ongoing business purposes. On the other hand, the archivist needs to serve the interests of the research community through the selection, preservation and provision of access to records relevant to research interests.

The life cycle approach also makes a clear distinction between the primary and secondary values that records supposedly possess. Primary value is the immediate value that the records have to the creating agency related to its needs, and in particular, the legal, administrative and

financial relevance. Secondary value is comprised of cultural and historical values the records may possess apart from the initial intention of the creator. It is the value of a record as evidence and information to users other than the creator and is embodied in all those records comprising the archives as memory institutions.

Based on the needs of records creators, the primary value of records is present in the current stage of the life cycle, which is divided into two phases, the active and semi-active, based largely on the creators' need to refer to the record within the context of the original business activity and the frequency of record retrieval as well as the records creators' need to keep the record for other reasons, such as evidence of the action. The transition of records from an active to semi-active phase is usually represented by the transferring from storage in the office to storage in a records center that can be on or off-site. The records center is a space created to reduce the cost of storing large volumes of paper records no longer referred to frequently, but which must still be retained to meet audit, legal, regulatory or other business purposes.

The current stage is composed of creation, capture using classification code attribution and/or registration, use of the record in relation to the original activity, and disposition, which might be destruction or transfer to an archival repository. After being transferred to an archival repository, records are subjected to another linear sequence of processes beginning with appraisal, deemed to be the responsibility of the archivist, and selection and acquisition of archives' content. The following processes are arrangement, description and physical preservation, followed by the provision of access to users of the records such as researchers.

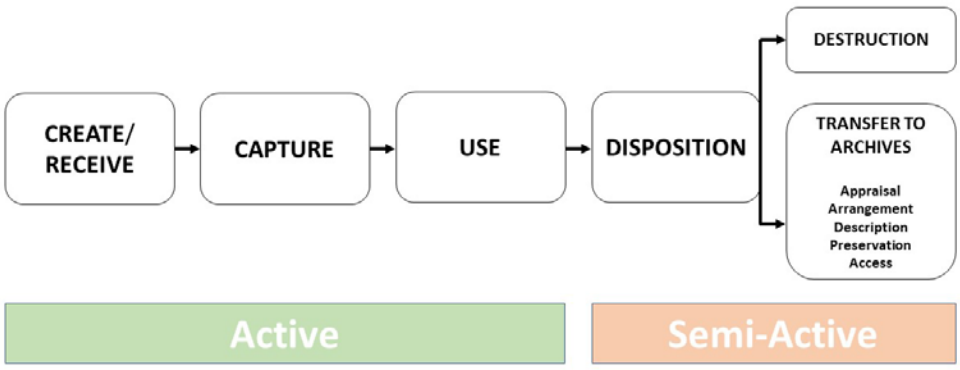


Figure 7. The life cycle model (Source: authors' own rendition)

Despite the continuing popularity of this model, it has limitations. The separation between the duties of records managers and archivists that the model encourages presents a barrier to proper preservation of digital records. The vulnerability of these records requires specialized management from the point of creation, well before they become archives.[81] In an electronic environment, records are also very dynamic and may exist in more than one stage of the life cycle at the same time. That fact implies that they may not follow a linear existence with definite stages from creation to disposition. In the electronic environment, it is easy to cut and paste and create new documents and records. Also, it is common to use data from the same database to create a series of different records. In both situations, records creators are using records to create or re-create new records, contributing to the existence of a loop completing the cycle. Thus, the idea of a circular dynamic, implied by the name "life cycle" is not a reality in most applications of the model.

Dimensions of records in the blockchain space – the Continuum model

Continuum theory is another approach to guide management of records. It presents an alternate perspective on the nature of records and archives, the societal role of recordkeeping and archiving, and the relationship between theory and practice. The central idea in the model is that records move across space and time, recognizing that archival objects are not in a fixed position in a determined period, but continually shifting and transforming, and gaining new meanings. It presents a layered and interconnected model to show the fluid movement of records between dimensions. The model is considered an upgrade over the unidirectional aspect of the life cycle model. According to the continuum, records are archives from the moment of their creation and archivists and records managers' attributions converge to both make and manage records and archives. Another feature of the model is that it highlights the evidential, transactional and contextual nature of records.

The model was proposed as a reaction to issues related to the life cycle and digital records, the disparities between the life cycle and accountability and the new government model of western countries. The increasingly pervasive deployment of information technology, especially demonstrated by the deployment of desktop information technology in workplaces, significantly impacted recordkeeping practices.[82] A lack of processes and regulation for

electronic records management contributed to significant challenges around the control and preservation of naturally accumulating information, especially by separating the records managers and archivist's roles. Accountability aspects are considered in the continuum model, different from the life cycle idea of the primary value of the record being for the creator. The relevance of accountability and its relation to records management came from the idea of the significance of the record as evidence of social and organizational activity. Evidentiary character supports democratic and corporate accountability that could only be associated with accountable recordkeeping. Archival science studies have found a correlation between corruption and the lack of (good) recordkeeping practices.[83] Finally, public-sector reforms that occurred between the 1980's and 1990's to improve efficiency and accountability brought to reality new administrative structures where it was harder to apply the life cycle model in relation to archival records.

The model was built on an attempt to unify records attributes and archives functions showing the records of continuing value. It also explored ideas about the "fixed" and "mutable" nature of records and the articulations of the role of recordkeeping and archiving in society related to "governance, accountability, identity, memory, and information provision."[84] The continuum model highlights the need to intervene in the process of records creation, which is not considered a starting point, but a continuous process that reinforces the assertion that records are "always in a process of becoming."[85] The model emphasizes the evidentiary, transactional and contextual nature of records and rejects any records definitions related to their subject content and informational value.

The continuum model takes a multidimensional view of the creation, capture, organization and pluralization of records. The archival functions such as appraisal and description are contextualized in the model also as dynamic activities. One way for describing records according to the model is checking how records conform to each dimension. Disposition, in this approach, is critical and never absolute. The four dimensions that the continuum model proposes are where records can rest occupying simultaneous spaces or not, following no mandatory or pre-established sequence. They are Create, Capture, Organize and Pluralize. There are also four continua that intersect with the four dimensions which are Identity, Transactionality, Evidentiality and Recordkeeping containers/objects.

Creation is the action that leads to a record, and it can also refer to a re-creation. Action takes place, leaves a trace that something happened and is recorded in documents.[86] This dimension refers to the creation of documents in the context of social and organizational activity, and it is so important to the continuum that every change in context reflects re-creation of the record. The creation of a record is also seen as a role of the archivist, not just the records manager, which gives rise to the idea that archivists should intervene in the process of records creation and maintenance "by adopting new roles such as monitoring and auditing."[87]

Capture happens when documents are integrated into an institution's records management system. That is when and where the record is captured into a records system in a way that guarantees its evidentiary character. It involves metadata creation that places the record in a greater context. The connection to the context must exist so records can function as evidence of the acts they support. "Usually, the systems capture records-as-evidence by linking documents-as-trace to the transactions, acts, decisions or communications they document, related records and their immediate business or social context."[88]

Organize is the process of turning a record into a part of a larger role, an archive. This is the dimension of the archive or the *fonds*, where records are organized and placed in the context of an organization or individual archive and managed in frameworks that "enable them to function as individual, group or corporate memory."[89]

Pluralize is the dimension wherein a record is communicated to others outside the organization. It is the dimension of access for the community and positions records as accessible collective memory. Pluralization happens so the records can become collective archives, representing a collective memory. That is why openness and accessibility are key features of the continuum model. In this dimension, the record is liberated beyond the boundaries of the organization, so it can "constitute the social memory of the broader community and can be (re) used in multiple ways and forms."[90]

The first element that interposes the pluralize and create dimensions is identity. It relates to the authority that creates and keeps the records, including their authorship, from the particularities of actors creating records to the broader social context beyond the organization or individual that originated them. Transactionality relates to records as products of activities, passing from the single transaction through activity, functions and finally reaching the social purpose of the document. Evidentiality relates to the record as evidence starting from the point

where the record presents traces of evidence to the point where it becomes part of the collective memory. Finally, recordkeeping containers/objects relate to the objects created in order to store records, from the archival document to the archives.

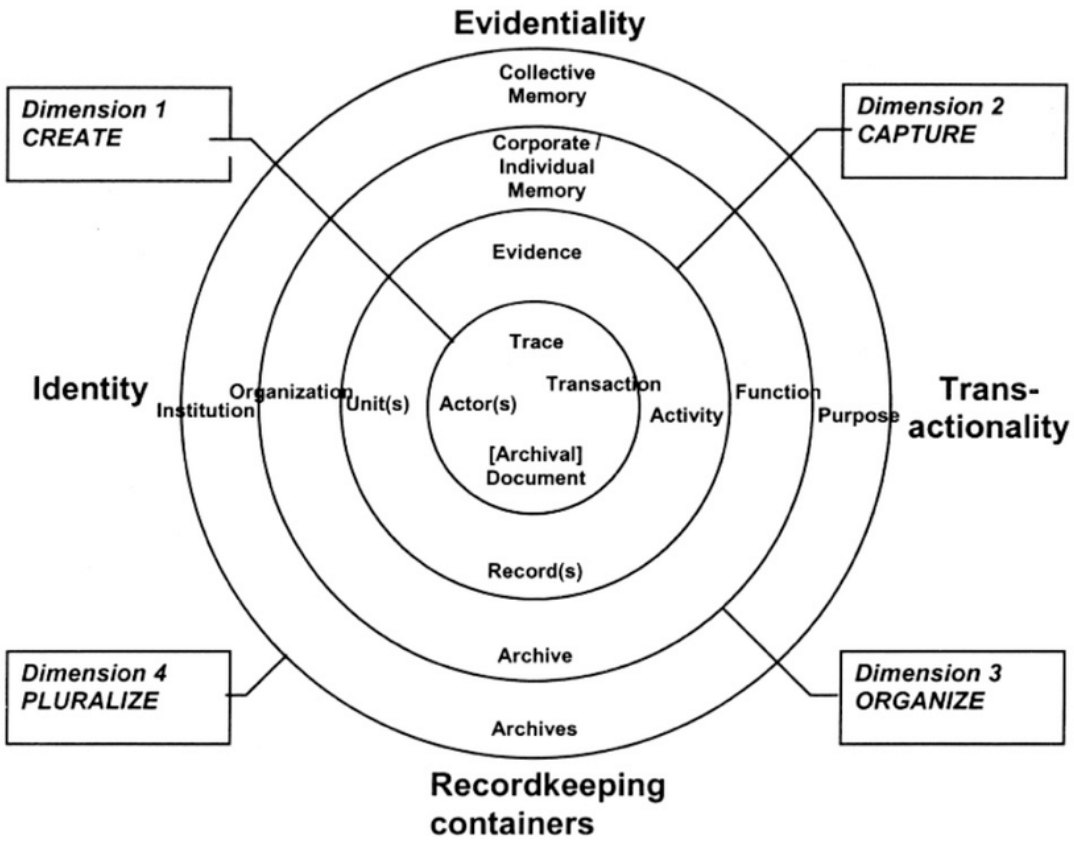


Figure 8: The continuum model (Source: Upward, 2000)[91]

Different from the perspective of the life cycle, in continuum thinking archives do not show a beginning and an end, as they are always in motion within the present moment. This dynamic characteristic aligns with the character of the electronic record. There is some confusion surrounding the model given that not everyone understands how it works. Case studies of the applications of the model are very limited such as its use to describe the role of records and recordkeeping in society. There are also some challenges related to the archival community shifting from the position of custodians of physical objects to the position of advisors working with technology experts, legal counsellors and others. When transparency is not a norm, it is also difficult to apply it to public records.

LIFE CYCLE	CONTINUUM
APPRAISAL	
. appraisal happens in a single point in time when records enter the archival custody **. it is a passive role of the archivists after a decision of creator.**	. a process of information gathering throughout the existence of the record. . it begins on record's creation.
DESCRIPTION	
. archivists must ensure the preservation of explicit metadata **. archivists should make implicit metadata explicit** **. archivists make sure that the pertinent information about the record is linked to the record.**	. descriptive metadata should be captured and linked to the records throughout the record's existence. . archivists assure that all relevant metadata is explicit and attached to the record (incorporating routine for the capture of metadata into the procedures of creation, maintenance, and use of the records throughout the record's existence)
BOUNDARIES	
. boundaries between recordkeeping processes (linearly arranged). **. the boundary between the roles of recordkeepers and different accountabilities (who to be accountable for and what to be accountable for)**	. questions the need for and the existence of boundaries within and between recordkeeping processes and roles.

Table 1: Comparing archival functions and boundaries in the models.

The records models and blockchain systems

There are differences in how the life cycle model and the continuum perceive the archival function, but in both models appraisal is considered one of the most important of the core archival functions. Both models bestow upon archivists the power to frame society's collective memory. In the life cycle model, appraisal is placed in a single point of the life of the record – the "archival threshold" – as records pass into archival custody. The archivist receives those records that the creator considers to be relevant for future use. After receiving the records, the archivist decides which ones should be preserved based on appraisal criteria. In the continuum model, on the other hand, appraisal is a more dynamic process that occurs throughout the entire existence of the record, starting from its creation. In both cases, the appraisal process requires knowledge of the context of the creation of records, functions and activities related to records, and the application of a classification schema.

In the case of blockchain systems, it is difficult to see how appraisal, at least as it is conceived of in the life cycle and the continuum models, could be carried out. In some blockchain systems, knowledge of the context, and consequently, knowledge of the functions

and activities of records creators, is very hard to obtain. In the case of the major public blockchains, Bitcoin and Ethereum, for example, transactions of diverse provenance enter the blockchain in sequential order to become part of the same block regardless of their origin or the procedural context of their creation.

Another limitation is the application of a classification schema. Classification links a record to its procedural context (the archival bond), establishing a unique identity for the record and enabling its interpretation and retrieval, an activity which has largely been unsuccessful in electronic information processing environments. In digital systems, human classification of records has been notoriously difficult, and machine classification is still in its infancy and suffers from inaccuracy. But at least in a centralized system, there exists an authority to design and oversee the implementation of a classification scheme. In a decentralized system, the question arises as to who is responsible for the classification of records? There is also the potential for difference in contexts among the records in a given blockchain system, and also in where the record is actually stored, which might demand the application of different classification schemes in different situations.

Both models agree that description facilitates access to records and establishes authenticity of records to act as evidence. The hardest task of this function in the electronic environment is documenting the relationships. Description is a practice that happens in different moments in each one of the models. The life cycle model envisions description taking place after the acquisition of records in the archives. It is a task the archivist undertakes to ensure the preservation of explicit metadata, to make explicit any implicit relationship, such as the archival bond, and to make sure that important information about the record will remain linked to it. In the continuum model, metadata should be associated with the record from the moment of its capture and important information about the record must be made explicit throughout its entire existence.

In the case of blockchain records, some metadata may be linked to the records since their capture, but it will all depend on the type of blockchain and how it is designed to operate. In any case, our research suggests that, at present, blockchain systems do not present an adequate metadata schema according to recognized standards, such as ISO 23081/2011 - indeed, far from it. Description, as conceived in the life cycle model, is impracticable in the blockchain environment, since there is no way to select the records kept in the chain for transfer into the

custody of an archives. The continuum model description is a better approach for blockchain systems, given that the records kept in the chain are electronic records. Even the continuum model falls short, however, given that it begins with records creation. In a blockchain recordkeeping world, much greater emphasis must be placed on upstream systems design, a "phase" of the record life cycle or a moment of it in the space/time records continuum that predates a record's existence.

In terms of professional boundaries, both models have very different perspectives, which is one of the main differences between them. The life cycle model establishes fixed boundaries between recordkeeping processes and between the records manager's and archivist's professional roles. The continuum model questions the need for such boundaries in both recordkeeping processes and professional roles. In the digital environment, division between the roles of the two professionals is not the best strategy to deal with the volatile and vulnerable electronic records. This is also true of blockchain records.

Blockchain and the life cycle model

On the blockchain, it is difficult to match elements of the record's life cycle to the records existent in the system. The first reason for this is that blockchain technology is a very recent phenomenon: the first block of the Bitcoin Blockchain is from January 2009, and Ethereum blockchain was launched in 2015. The life cycle is a model from the middle of last century, idealized for paper records that were constantly increasing in volume. Second, there are no regulations related to the records produced and kept in blockchain systems. Table 2 compares the elements of the life cycle and points to their presence or absence in blockchain systems. For the time being, it is legitimate to assume that most of the transactions registered in the chain are still in their active phase. The records in the blockchain system show primary value since they were created to support transactions involving cryptocurrencies and other assets. Their creation and capture processes are not distinct. For the system, a transaction only exists in the moment of its capture. The use of record might also not be a process apart from the creation, because the previous transactions are always used to validate the new blocks – composed of new transactions - entering the chain.

In the case of blockchain disposition, there exists another problem. Initially, it is not possible to separate records that should be destroyed from those that present informational and

cultural value. Records are meant to be permanent once they are uploaded in the chain. Taking out any information from a block implies changing all the remaining blocks, thereby invalidating them, which in turn results in problems with integrity of the records. Transferring historical blockchain records to an archives has yet to be done and it is difficult to conceive of how this might even be achieved, as discussed in chapter 4.

For purposes of collective memory, blockchain records receive the same treatment as other electronic records. Secondary value is already evident in the first transaction of the Bitcoin Blockchain, for example. As previously mentioned, however, appraisal is challenging in the blockchain environment, especially because of the impossibility of maintaining relationships among records and their component parts. Arrangement is challenging in blockchain environments since it is not possible to change the initial order of blockchain records without invalidating their integrity. Transactions are captured in the chain according to their timestamps, no matter their provenance or function. This is certainly an issue for respecting the principle of provenance and preserving the archival *fonds*. Descriptive metadata in blockchain systems is insufficient according to records management best practice.

LIFE CYCLE		
	Elements of the model	**Detected on blockchain systems?**
CURRENT RECORDS Active + semi-active phase	Primary value	Present in blockchain records.
	Creation	A process that cannot be separated from capture.
	Capture	A process that cannot be separated from creation.
	Use	A process that cannot be separated from creation and implies re-creation.
DISPOSITION	Destruction	Cannot be done in blockchain systems.
	Transfer to archives	Cannot be done in blockchain systems.
ARCHIVES	Secondary value	Present in blockchain records that pose cultural and informational value.
	Appraisal	Cannot be done in blockchain systems.
	Arrangement	Cannot be done in blockchain systems.
	Description	Cannot be done in blockchain systems.
	Preservation	Not present in blockchain systems.

Table 2: Life cycle and blockchain systems

The preservation of records in the system is another problem. Research shows that preservation of electronic records depends upon records metadata and trustworthy storage of records. In terms of metadata in blockchain systems, it is insufficient to guarantee the long-term preservation of the records created and kept within them. In terms of records storage, its decentralized character may be considered an advance when compared with centralized systems because several copies of the ledger are stored in different nodes around the world. As we discuss further in chapter 10, however, this is insufficient to guarantee the maintenance of records for long periods.

Blockchain systems and the Continuum Model

The continuum dimensions can be partially matched with the reality of blockchain systems as they exist today.

Records creation is a vital element to the continuum, and any changes in the context reflect re-creation of records. Provenance of the record in a blockchain system is hard to define. If the whole system may be considered a context of the record, it is valid to assume that forks are a phenomenon that change a record's context, thereby altering the record itself.

In the case of blockchain systems, they were not designed for capturing records according to international standards and best practices on records and information management. Yet, they are recordkeeping systems, which implies that they should capture records according to international best practice. Capture involves metadata creation that places the record in context. In blockchain systems, efforts to generate metadata to link the records to each other and to their organizational context, i.e., to instantiate the archival bond, are idiosyncratic if they are made at all.

In terms of the organize dimension of the continuum model, pluralization depends upon a culture of openness and accessibility. This is a dimension directly related to transparency. That means that the model works well on transparent environments such as public blockchain systems. Even on the private ones, transparency is still an important operating principle among

network participants, except for those for whom some confidentiality is required according to the business model of the ecosystem.

Identity can be detected at least at the level of actors in most of the blockchain systems, even the ones that claim to be anonymous. The unit(s), organization and institution levels depend on the type of blockchain system. On a private blockchain, it is usually clear who are the participants in the network, as they will be assigned different levels of access with different profiles and attributions, so the units, organizations and institutions are defined. On public systems, like Bitcoin Blockchain, it is hard to identify those elements for each of the actors.

Transactionality is clear in all the types of blockchain systems, especially those using smart contracts because the activities and functions might be clearer given that smart contracts embed business logic. As recordkeeping containers, blockchains could be considered themselves records, archive or archives, depending on the type and the context as discussed in the previous chapter. The transaction in some blockchain systems might be the only trace or evidence of the act they represent: a transfer of cryptocurrency in the Bitcoin blockchain leaves a record of the transfer but may leave no record of the act (or purpose) of the transfer. As elements for the composition of corporate, individual or collective memory, it might be too soon to tell if what is recorded on a blockchain will suffice. Given the acceptance and adoption of the systems by organizations and governments and the increasing size of the community involved in blockchain development, the assertion that blockchain is already part of the collective memory is not untenable. It is valuable to emphasize that the evidence value of blockchain records may be questionable given that the regulations around the system are poor or non-existent in some jurisdictions, which we discuss further in Chapter 7. Nonetheless, blockchain systems themselves in their entirety may provide historical evidence of shifting societal power relations and institutional changes.

Table 3 illustrates the elements of the continuum model present in blockchain systems.

CONTINUUM		
	Element	**Detected on blockchain systems?**
DIMENSIONS	Create	Present in blockchain systems.
	Capture	Present in blockchain systems not as standards requirements.
	Organize	Cannot be detected on blockchain systems.
	Pluralize	Present in blockchain systems.
CONTINUA	Identity	Present in some blockchain systems.
	Transactionality	Present in blockchain systems.

	Evidentiality	Partially present in blockchain systems.
	Recordkeeping containers	Present in blockchain systems.

Table 3: Continuum elements and blockchain systems

It is not always possible to see the boundaries, or record stages, articulated in the life cycle model reflected in blockchain systems. The continuous transformation of the chain with its growth or through fork events aligns better with the continuum model. The continuum model's assertion of the constant re-creation of records and that disposition is not absolute aligns well to the blockchain recordkeeping world wherein dependencies exist between previous transactions and blocks that, if broken, re-create and even destroy the record. These features of blockchain systems point to the continuing relevance of the continuum model in a blockchain recordkeeping environment.

Conclusion

It is clear that neither the life cycle nor the continuum model is completely applicable to the management of records in blockchain systems. The elements of the continuum model, however, appear to match most of the characteristics of blockchain records and systems.

Adoption of digital technology in private and public administration brought about some deep questioning of paper-based recordkeeping practices once established by the life cycle model. Given that neither model is a perfect fit to the world of blockchain recordkeeping, it may be that the decentralized and distributed characteristics of blockchain systems will ultimately need to lead to a reframing of recordkeeping practices into a new paradigm.

Chapter 4: Retention & Disposition of Blockchain Records

Introduction

Retention and disposition are central to the effective management of records. ARMA's Generally Accepted Recordkeeping Principles include the Principle of Retention, which states: "An organization shall maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements."[92] Indeed, at the center of EDRM's Information Governance Reference Model[93] below, is retention:

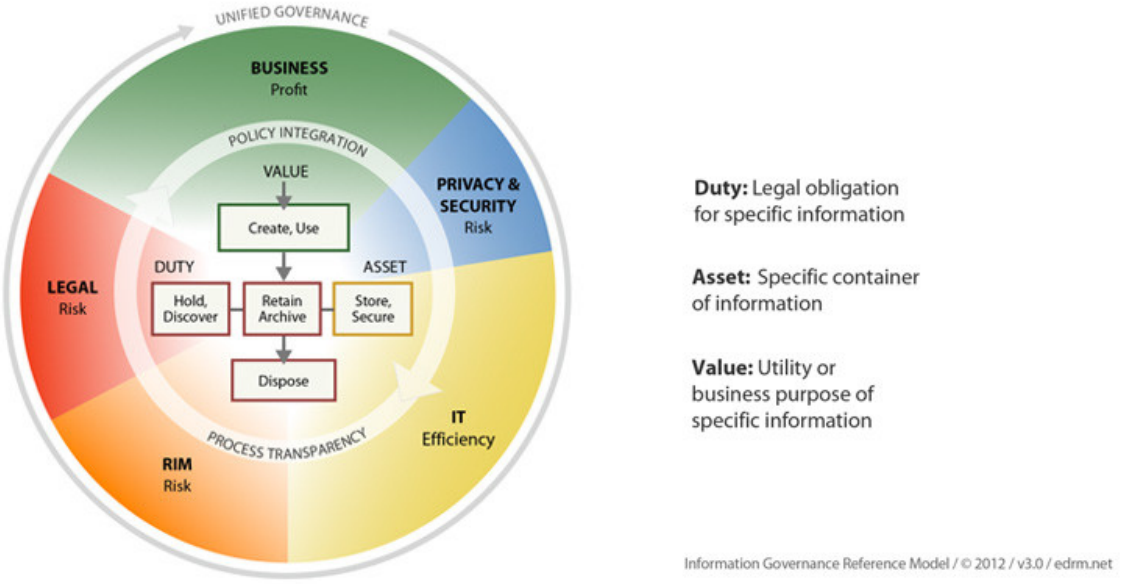


Figure 9: Information Governance Reference Model

Appropriate retention of records is crucial. Having the right records available can enable organizations to enforce their rights or exculpate themselves from liability, improve organizational decision making, provide deeper insight into organization risks, and reduce inefficiencies and transactional friction. Despite these benefits, however, organizations still struggle to retain records appropriately. Contoural, Inc., in its report on defensible disposition, identifies "uncertainty about record retention requirements," "lack of agreement on the business value of records and documents," and "not knowing where information resides" as primary problems organizations face with regard to records retention, and particularly, in connection with retaining records beyond their useful life.[94]

These problems can be alleviated through good records retention and disposition. Records retention schedules should clarify uncertainty around record retention requirements; a mature records retention schedule will also make clear when a case truly is exceptional due to its non-inclusion. Retention policies dictating records' storage and access during their active, semi-active, and inactive periods should reduce the amount of records whose whereabouts are unknown. However, implementing and maintaining appropriate records retention throughout an organization remains a challenging proposition; it requires time, expertise (including RIM, technological, and subject matter expertise), and organizational buy-in. Can blockchain reduce any of the investment required for records retention? Does it impose new challenges or risks? What could blockchain records retention look like? These are important questions for records and information managers to come to grips with as new blockchain projects for recordkeeping grow.

The Principle of Disposition, in turn, holds that "an organization shall provide secure and appropriate disposition for records and information that are no longer required to be maintained by applicable laws and the organization's policies."[95] Disposition, then, must be carried out in a defensible way that supports the organization's needs. Despite the benefits of appropriate disposition, however, many organizations are drowning in information. In 2014, "the average information worker [spent] an estimated 28 percent of the workweek managing e-mail and nearly 20 percent looking for internal information or tracking down colleagues who can help with

specific tasks."[96] Reducing the information glut requires defensible disposition.[2] As noted above, organizations face a number of barriers to disposition, including employee resistance.[97] At first glance, it seems natural to think that a technology inherently designed so that records may only be appended, and never deleted, would only add to the problem.

Blockchain and Records Retention

As discussed previously in this report, there exist a diversity of blockchain technologies; the retention affordances of a particular blockchain implementation would depend on the design of that implementation. However, all blockchains differ from paper and existing digital records management systems in a number of ways, both good and bad. Firstly, blockchain's tamper resistance could challenge the traditional records life cycle and the retention approaches that have arisen concurrently with that life cycle. Secondly, blockchains' distributed architecture could help integrate diverse records systems, bringing about more unified retention and classification amongst those systems. That distributed architecture, however, also lends itself to transjurisdictional arrangements, which could pose a challenge for determining legal retention requirements. Thirdly, blockchain technologies are nascent as a records management technology; the capacity to integrate a blockchain solution with records retention schedules and classification systems remains undeveloped.

Although the records life cycle is addressed in depth in Chapter 3, it is worth addressing here those aspects of records retention that are tied to the life cycle, and their potential disruption by blockchain technologies. This disruption comes from the tamper resistance of blockchain transactions. As Fazzio puts it, "permanent data retention collides with ordinary records life cycle and disposition policies."[98] This is because blockchains default to permanent retention. For organizations, however, permanent retention is deeply problematic. Permanent retention requires extensive data storage; this could be mitigated, for example, by storing parts of records off-chain, but organizations are then left to implement both a blockchain and off-chain storage in a manner that supports their needs. Furthermore, permanent retention of records means that organizations might well be retaining records which could be used to hold them liable in litigation; had those records been disposed of in accordance with the organization's retention schedule in the ordinary

[2] See Chapter 5: Blockchain & Defensible Disposition, *infra*.

course of business, the records would no longer be available. Finally, permanent retention increases the inaccessibility of records due to information glut. Blockchains could also disrupt the transition of active records to semi-active states. For example, organizations may choose to move semi-active and/or inactive digital records to less expensive storage media or to off-site storage. In a system with a blockchain, even one where the records themselves were stored off-chain, such an eventuality would have to be planned and designed into the system, and currently there exists no technical capacity to do so.

While it is a myth that all records have a legally mandated retention period,[99] it is unquestionable that legal compliance requires organizations to understand those retention requirements that the law does impose upon their records. Indeed, Howell and Cogar, both attorneys, go so far as to state that:

> It is impossible for an organization to achieve acceptable legal compliance without an appropriate and functioning records retention program. This is so for two distinct but important reasons. First, record retention is an important substantive component of many of the laws with which most corporations must comply. Second, retained records are often the vehicle by which compliance is established.[100]

However, the legal retention period applying to any particular record or record set is dependent upon jurisdiction. As a very simple example, the Canadian province of British Columbia requires employment records be retained for two years; the Canadian province of Manitoba requires employment records be retained for three years.[101] If an organization has nodes across Canada (and therefore its records stored across Canada), great care will be need to be taken to classify records according to the proper provincial authority to ensure appropriate retention. If Manitoba employment records are destroyed after two years, there could be serious consequences to the organization should subsequent litigation arise, such as fines, adverse inferences, or even a dismissal of claim or negation of a defense.[102] As it is possible to imagine, this issue becomes manifold in a global blockchain implementation.

Without thoughtful metadata design, it's very easy for records in blockchain systems to lose contextual markers (such as indicators of jurisdiction) that enable organizations to manage, retain, and dispose of those records appropriately. For example, blockchains do not natively instantiate the archival bond, the relationship between records that participate in the same

action.[103] Without the archival bond, appropriate records management in accordance with retention polices and schedules and classification systems is extremely difficult. Actions to be taken at the file level will require re-examining all the individual records hashed in the system in order to determine which records belong to which files. Similarly, blockchain records management systems do not yet have the sophisticated classification schemes built into them that systems such as EDRMS have. This, of course, does not mean that such capacity cannot be built with blockchain technologies, but rather, that serious design deficiencies exist currently and must be remediated if blockchain-based solutions are to provide adequate records retention.

Blockchain technologies, however, also bring unique potential to records retention. For example, one of the problems in managing electronically stored information is the prevalence of duplicate and near duplicate records, such as drafts of the same final records ("dupes" and "near dupes").[104] Finding, identifying, and appropriate disposal of dupes and near dupes can be time-consuming and costly, but is necessary for effective records management. Blockchain's hashing function can be used to identify dupes and near dupes efficiently;[105] if an organization's records are all being hashed as a matter of course, it becomes a comparatively simple matter to apply a tool such as a search algorithm to those hashes to identify duplicates and near duplicates, saving substantial effort and improving the organization's records retention. This approach would not necessarily require the deployment of blockchain systems; it is possible, for instance to achieve the same outcome by simply hashing the records without recording those hashes in a blockchain. However, where a blockchain system has been implemented for other business reasons, its hashing functionality could be leveraged to support deduplication efforts prior to recording records' hashes on-chain.

Blockchain Disposition: The Difficulty of Destruction

The issue of destruction of blockchain records is a pernicious challenge, yet one that must be dealt with if blockchains are to be effective records management tools. Retaining records beyond their useful life, e.g., beyond that period in which they are serving a legal, regulatory, business, or historical purpose imposes costs and risks on the organization. As the Dupont Records Management Guide helpfully points out, "'Just in case' is *not* a valid records retention period" (emphasis in original). Smallwood explains the bleak reality of not destroying unneeded records:

> [E]stablished organizations, especially larger ones, are being crushed by this onslaught of Big Data: It is just too expensive to keep all the information that is being generated, and unneeded information is a sort of irrelevant sludge for decision makers to wade through. They have difficulty knowing which information is an accurate and meaningful "wheat" and which is simply irrelevant "chaff." This means they do not have the precise information they need to base good business decisions upon. And all that Big Data piling up has real costs: The burden of massive stores of information has increased storage management costs dramatically, caused overloaded systems to fail, and increased legal discovery costs.[106]

Records destruction, then, is imperative. But, as discussed above, the blockchain defaults to permanence. Deleting one transaction in one block destroys the integrity of the chain. The challenge of destroying blockchain records has been brought to the forefront by the European Union's General Data Protection Regulation (GDPR).[107] GDPR guarantees a "right to erasure" – data subjects whose data is within the scope of the law have the right to have their personal data destroyed by the data processors and/or controllers in whose custody the data lies.[108] Blockchain solutions implemented in or processing personal information of Europeans, then, must either have no personal data or permit the destruction of records if they are to be compliant with GDPR. As Lima notes, "the immutability of data transactions that are imprinted in the fabric of [blockchains] implies that one of the key principles of GDPR, Art. 17 right to erasure […] is not met by Blockchain."[109]

Furthermore, Maxwell and Salmon note, the right to erasure will prove a particularly interesting question because, as it stands, "[what] constitutes 'erasure' is still open to debate."[110] So, too, is it for records: when is destruction not destruction? As it stands currently, electronic records that have been "destroyed" can often be reconstructed. "Deletion" is not actually destruction. There are four primary means of destroying electronic records: physical destruction, degaussing, overwriting, and crypto-shredding.[111] Given the distributed nature of the blockchain, destruction and degaussing are likely to be impractical, if not impossible. As noted above, tampering with transactions on the blockchain is technically extremely challenging, even impossible, and, if successful, destroys the integrity of all previous transactions in the chain, negating the whole point of utilizing blockchain technology in the first place.

If the "editable" blockchain is out as a solution, this leaves crypto-shredding for destroying blockchain records. Crypto-shredding is a process whereby records are encrypted, and the encryption key is then destroyed. So long as the underlying cryptography isn't broken, crypto-shredding is effective as a form of destruction, because the plain text of the message (i.e., the interpretable, meaningful version of the message) is irretrievable. All that is left is cyphertext (or, not to put too fine a point on it, "gobbledygook"). Blockchain solutions can fairly easily be designed to support crypto-shredding as a means of records destruction. Whether crypto-shredding is sufficient for destruction, on the other hand, is a fact-dependent question. For example, it remains to be answered whether crypto-shredding is "erasure" within the meaning of the GDPR for organizations within the scope of that law. Or, for organizations where records security is an especially high priority, such as military or national security organizations, the risk of the cryptography being broken might be too high or the adversaries too motivated. In such a case, crypto-shredding might prove insufficient for destruction, even though it would be more than sufficient in a lower risk recordkeeping context.

In those cases where crypto-shredding will not do, it is possible to store the records themselves off-chain, with a URI or hash pointer on-chain to point to the record. The record could be destroyed off-chain without disrupting the blockchain or its integrity-preserving function. However, such a system limits the ability to leverage the disruptive potential of having records generate natively on-chain (such as the ability to utilize a fully-tokenized system). The best means of approaching records destruction on the blockchain is less a technical, and more an information governance question; the best means will depend upon the goals, needs, and available resources of the organization implementing the solution and careful design of an optimal data/records architecture.

Conclusion

Blockchain technologies could prove useful in records retention and disposition, but only if they are carefully designed and implemented to instantiate traditional records retention requirements while still taking advantage of blockchain's affordances. Careful fact-based analysis must support an organization's implementation of a blockchain solution for records retention and disposition. A number of decisions – such as how records will be destroyed, what records might be stored off-chain, how retention schedules and classification will be integrated

into the system, and how the blockchain should be supplemented to support digital preservation – should be made at the design stage, taking into account organizational context, needs, and constraints. Although Lima, in the following passage, is considering blockchain vis-a-vis the GDPR, his fundamental point stands in the case of retention, preservation, and destruction as well.

> Blockchain can be considered as technology that can not only improve the fundamental aspect of data privacy and security, as specified in GDPR […and] can also be carefully studied, architected and implemented with GDPR-compliance intent for data privacy, using some unique techniques. These alternatives are not simple to implement, and they require deep understanding of how Blockchain works and how the technology ecosystem is interrelated.[112]

Our current systems, including EDRMS and digital archives, are the result of careful study, architecture, and implementation, born of many years of gaining an understanding of these technologies. However, blockchain solutions cannot help organizations with their records retention and disposition needs unless they are integrated into a comprehensive approach which leverages blockchain's strengths – tamper-resistance, security, auditability – as a complement to, and not a panacea for, a full RIM program that addresses the human, fiscal, operational, legal, regulatory, and technical requirements of the organization.

Chapter 5: Blockchain and Defensible Disposition

Defensible Disposition and Records Over-retention

The Sedona Conference, in its *Commentary on Information Governance,* advises that "the effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program."[113] After all, "[i]n litigation, it's not the records that have been discarded that create the most legal problems, *it's those that remain*. Attorneys can more easily defend the *absence* of documents that have been systematically destroyed under an established retention policy than they can defend existing records' *content.*"[114] Even when information and records do not pose a direct legal risk to an organization, their over-retention is nonetheless problematic. "Assuming information is an asset, at some point when there is so much data, its value starts to decline [… due] to the inability to expeditiously find or have access to needed business information."[115] Yet over-retention remains the norm in many organizations. Indeed, "71 percent of organizations surveyed have no idea of the content in their stored data [and] 79 percent of organizations say too much time and effort is spent manually searching and disposing information."[116] The modern situation is akin to "drinking from a firehose through a straw."[117]

The Sedona Conference observes that the record and information overload "struggle is often caused by many factors, including the incorrect belief that organizations will be forced to 'defend' their disposition actions if they later become involved in litigation."[118] Due to the fear that a particular record might be required in litigation at some point, organizations (and individuals) default to a "keep everything" disposition strategy. However, this strategy is largely in error. "While it is true that organizations must make 'reasonable and good faith efforts to

retain information that is relevant to claims or defenses,' that duty to preserve information is not triggered until there is a 'reasonably anticipated or pending litigation' or other legal demands for records."[119] In other words, absent some other obligation to keep information (such as a statutorily imposed retention period), organizations do not have a generic duty to retain information simply because someone, somewhere, might someday file a lawsuit against them. The duty to retain information relevant to defenses and/or claims in a lawsuit only arises when litigation is reasonably anticipated or has actually arisen. As the first of the defensible disposition principles put forth by the Sedona Conference states, "Absent a legal retention or preservation obligation, organizations may dispose of their information."[120] "*Disposition*," then, is as critical as "defensible." "It is good business practice to destroy unneeded content, provided that the rules on which those decisions are made consider legal requirements and business needs."[121]

Organizations must consider the legal and business requirements obligating the retention of information against the technical challenges and costs of continuing retention. In the case of blockchain records – either records generated and/or stored on-chain or those stored off-chain and hashed to a blockchain – the legal and technological elements of defensible disposition require special attention.

The Legal Elements of Defensible Disposition on the Blockchain

Blockchain is still sufficiently new that legal and regulatory systems are still grappling with it. Although over-retention does not achieve defensible disposition, organizations cannot be blasé about the very real, non-litigation related legal retention requirements on their records. The default retention period on the blockchain is "permanent." Although, as noted above, over-retention of any records, including paper records, imposes risks on organizations, this can be heightened with blockchain records. By defaulting to permanent retention, blockchain solutions could obligate organizations to actively destroy records when their retention conflicts with law. As an example, one area of such potential conflict is between the blockchain's permanent retention period and data privacy laws, such as the General Data Protection Regulation (GDPR) as previously discussed in chapter 4.

Under GDPR, if a data subject successfully requests that data processor or controller destroy his/her/their data in that processor's custody, then the processor must find some way to do so that meets the requirements of the law. It remains an open question as to how blockchain records can be "destroyed" in a way that meets the requirements of GDPR. The two main solutions proposed thus far are to store the records off-chain, in which case, the record can be destroyed, leaving only its hash on the blockchain, from which the record cannot be reconstituted. For on-chain records, one potential solution is to encrypt the record and to destroy the encryption key. Although this would not "destroy" the record in the traditional sense, it would render it unintelligible, thereby arguably meeting the data protection purposes of the statute. Whether or not such solutions to destroying blockchain records will meet the requirements of the law, however, remains to be seen.

Custody and control of records is another potential legal complication for blockchain records. Defensible disposition operates from the perspective of an organization: the organization's legal obligations, the organization's business requirements, and the organization's technological capabilities. However, blockchains are frequently (though not always) designed in a way that makes them an interorganizational information infrastructure. This is an area with many questions, and very few answers. How is an organization to protect itself from liability when it has responsibility for records whose custody and control is shared? When does an organization have responsibility – for example, as a data processor or controller – over records in a blockchain in which the organization is just one participant? Given the geographically distributed nature of many (but not all) blockchains, how is a defensible disposition plan to account for differing retention requirements? Can an organization assert privilege over records that are, arguably, public by being shared through a blockchain? These questions will likely be answered, over a period of years, by courts and legislatures. Unfortunately, organizations are using blockchains and creating blockchain records now. Defensible disposition becomes much more important – and much more complex – when there is so much legal uncertainty attached to the information infrastructures through which records are created and stored.

The Technical Elements of Defensible Disposition on the Blockchain

The Sedona Conference characterizes information technology infrastructure as "the 'how' of the [defensible disposition] process."[122] Indeed, Kahn, in a chapter on defensible disposition, traces current struggles with information governance to, in no small part, the technological realities of records and information management in modern organizations:

> The nature of electronic information is such that its governance today requires the participation of IT, which frequently has custody, control, or access to such data, along with guidance from the legal department. As a result, IT personnel with no real connection or ownership of the data may be responsible for the accuracy and completeness of the business-critical information being managed. See the problem?[123]

Even if an organization has a solid defensible disposition plan in place, taking into account the legal and regulatory obligations the organization has towards its records, the business needs for those records, and a clear risk profile, it will fail if it doesn't take into account the particular technology infrastructure and capabilities of the organization. As The Sedona Conference explains, "[w]here the available technology limits the achievability of information objectives, the organization should decide whether to revise the objectives, update the technology or both. Technological capabilities affect key decisions when designing a disposition program."[124] Blockchain systems require particular consideration because of the challenges of achieving certain information objectives in a blockchain system. Most notably, blockchains, because of their immutability, make it challenging to destroy records, particularly those stored on-chain. Additionally, several technical capabilities that are commonly relied upon in defensible disposition plans, such as automated records management and classification, suspension of automated deletion, technology assisted review (TAR) and content search of records for diligence purposes are not necessarily available yet as part of blockchain systems. Technology assisted review,[3] for example, is a judicially recognized processing "involv[ing] the interplay of humans and computers to identify the documents in a collection that are responsive to a production request, or to identify those documents that should be withheld on the basis of privilege."[125] TAR requires human subject matter experts to train machine learning algorithms to

[3] Also known as "computer-assisted review"

identify those records which are most likely to meet certain parameters, for example, those requiring permanent retention when doing diligence before disposing of records. Increasingly, TAR is recognized not just as a cost and time-saving measure, but as a process which "can yield higher recall and/or precision than an exhaustive manual review process, in which humans code and examine the entire document collection."[126] The intersection of blockchain and machine learning is still fairly novel and developing; how TAR for blockchain systems will develop and the particular affordances and limitations of TAR for blockchain is yet to be seen. Organizations adopting blockchain systems will have to consider the specific risks and balances of being early adopters in understanding the role of their blockchain systems in their defensible disposition plans.

Furthermore, the design of a particular blockchain solution will have a substantial impact on its affordances and limitations. As noted in Chapter 1, blockchains can be public or private, permissioned or permissionless. They can rely on any of a number of consensus mechanisms. They can be intra- or interorganizational. Assessing the risks, benefits, and limitations of blockchain records for purposes of defensible disposition is not merely a question of looking at a blockchain. It is a matter of examining the particular blockchain(s) that a particular organization uses to create, manage, access, or otherwise use its records and considering that blockchain in the context of the broader goals and needs of the organization in order to create a workable defensible disposition plan.

Conclusion

Over-retention of records is a serious problem, costing significant amounts of time and money, impairing the ability of organizations to make fast, data-driven decisions, and imposing unnecessary legal risk from records that could have been destroyed. The "keep everything" approach has arisen from a number of factors and is in fact the default state of the tamper-resistant records on the blockchain. A successful defensible disposition plan must deal with any existing backlogs of records as well as laying the groundwork for actively managing records disposition moving forward. To do so requires an organization to consider its legal obligations, business goals and needs, technological capabilities, and the risks and benefits to the organization. Doing so when blockchain solutions are implemented requires an extra degree of care, because blockchains are a novel technology that defaults to permanent retention. This

default means that organizations must actively design record destruction into their blockchain systems; doing so, however, requires understanding the legal and technical nuances of the particular blockchain infrastructure(s) employed by that organization.

Chapter 6: Preservation of Blockchain Records & Systems

Introduction

This chapter explores how blockchain technology can be used to support long-term preservation of archival documents as well as some of the issues around the long-term preservation of blockchain records and systems.

The use case for blockchain in long-term preservation

Blockchain technology is a technology that has the potential for application in many areas, including in the long-term preservation of archival documents. Research has begun to explore this use case. While this research is still in its infancy, this chapter highlights two interesting projects that appear to hold potential for understanding how this technology could aid archival work.

Project ARCHANGEL

ARCHANGEL explores a shift from an institutional underscoring of trust, to a technological underscoring of trust through the use of Distributed Ledger Technology (DLT) to guarantee the integrity and provenance of digital records entrusted to archives. The project is a two-year collaboration between the UK's National Archives, the University of Surrey, and Tim Berners-Lee's Open Data Institute (ODI). ARCHANGEL combines Computer Vision and Artificial Intelligence techniques to fingerprint visual records (e.g. digital videos of court

proceedings) entrusted to The National Archives with blockchain technology for use as a curation tool and as a means of securing content against tampering during the custody of the record. The project team notes the value of this capability: "Blockchain offers a shield which archives can use to defend the records as authentic. By enabling researchers to compare the content of evidence (including the checksum of the record) to that recorded on the blockchain, they can see proof that no changes (deliberate or accidental) have been made to the record since it was preserved in the archive. Further to this, the decentralized nature of blockchains removes the need for citizens to trust individual institutions as each is the guardian for the other guardians."[127]

ARCHANGEL uses blockchain technology to record digital signatures derived from either scanned digital or born-digital archival images using the Ethereum blockchain platform as a prototype implementation to assure the integrity of those images. As shown in Figure 10, the process works by creating a hash of the original digital document, recording that on the blockchain, preserving that document in the archives, and then subsequently checking that the document has not been altered by comparing the hash of the preserved document with the hash originally recorded on the blockchain. Project ARCHANGEL shows significant promise as a tool for transforming the future work of archival preservation, particularly as the research team is exploring new business models for archives that could promote sustainable funding through users paying for a blockchain-based service for verification of the integrity and authenticity of archival documents.

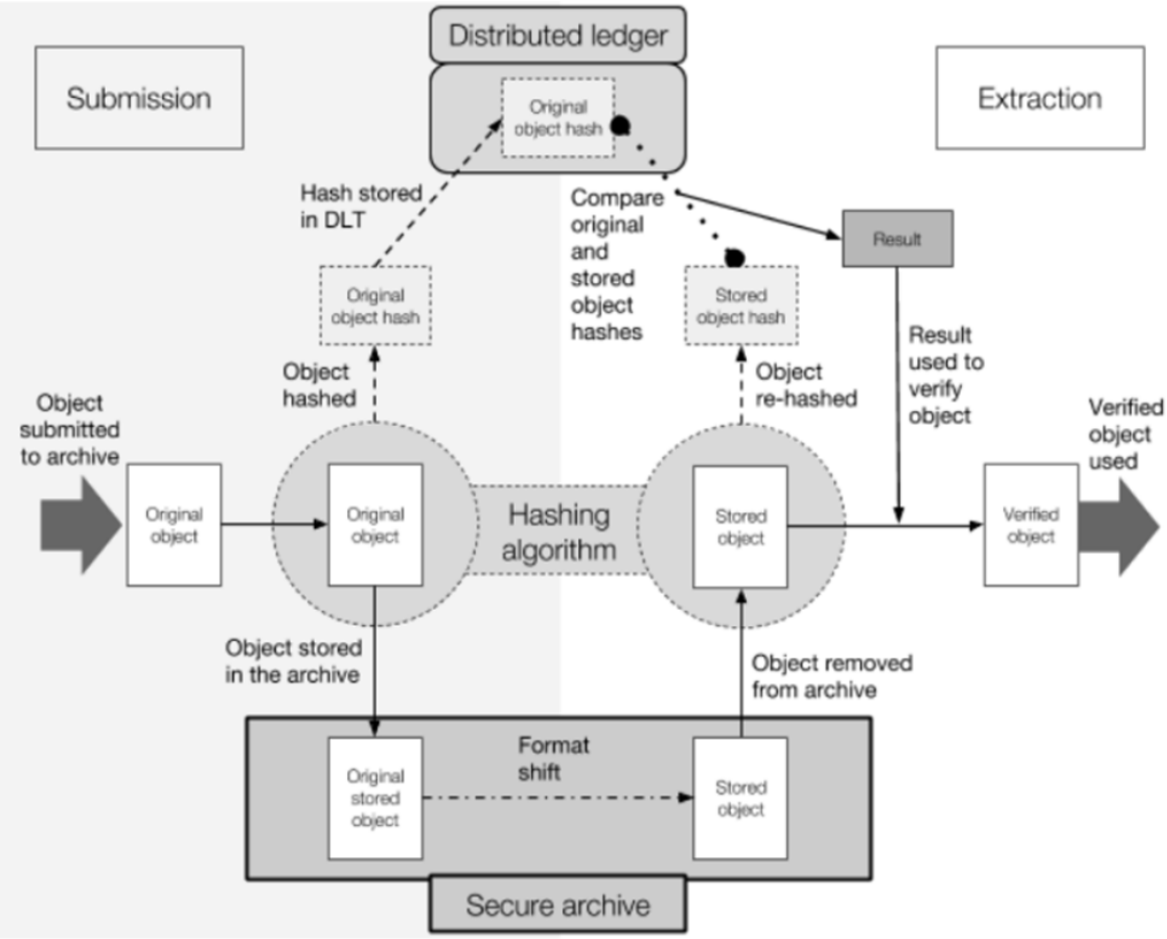


Figure 10: Overview of the ARCHANGEL System which leverages blockchain technology to assure the integrity of archival documents (Source: Collomosse et al.)

InterPARES TRUSTER Project

The InterPARES Trust TRUSTER project led by a team of researchers at the University of Zagreb in Croatia, tackles a slightly different issue related to the long-term preservation of the integrity and authenticity of archival documents.[128] Many records, especially in a European context, are digitally signed as they come up for final disposition and selection for preservation. In traditional digital signature systems, an entity will have a public key (known as a certificate) issued by a certificate authority that links that key to its identity and a private key, known only to it, which is used to "sign" a digital document. The problem with this traditional approach to digital signatures is that, over time, the certificate used in the signature will expire or possibly the certificate authority will cease to exist. Once this happens, the signature can no longer be confirmed and tampering with the document is possible.

To solve this problem as a means of assuring that continuity in attestations about the integrity and authenticity of digitally signed documents, the TRUSTER research team proposed TrustChain, a model for long-term preservation of digitally signed documents using blockchain technology. As explained in Bralic, Kulic and Stancic, "The core of the system is a blockchain containing hashes of digital signatures. Any interested individual or institution can request a record to be added to the blockchain but only the authorized nodes are allowed to write the new record into the blockchain (after confirming validity of digital signature(s)). TrustChain nodes are servers maintained by institutions participating in the TrustChain project. These servers accept new record requests, process them, write them into the chain and keep the blockchain stored and available to be read by interested parties. Communication between a party requesting a new record to be added and nodes can be achieved via a specialized TrustChain client software or a web interface provided by the nodes themselves. Similarly, a party interested in confirming the validity of a document with an expired signature would contact a node, read the blockchain, find the relevant entry and compare it to the document that needs signature conformation. Finding the relevant block in the blockchain would be achieved by an indexing system that relies on the document metadata stored in the blockchain. This indexing system might be part of the TrustChain nodes, or it might be outside of the system (since the blockchain is freely readable). The basic architecture of the TrustChain system is shown in Figure 11. While TrustChain cannot extend the life span of a digital certificate, it would provide a guarantee that the document and its signature have remained unchanged since the TrustChain entry was created. Since the digital signature contains the name of its owner, this can be used to confirm the creator of the document at a later date."[129]

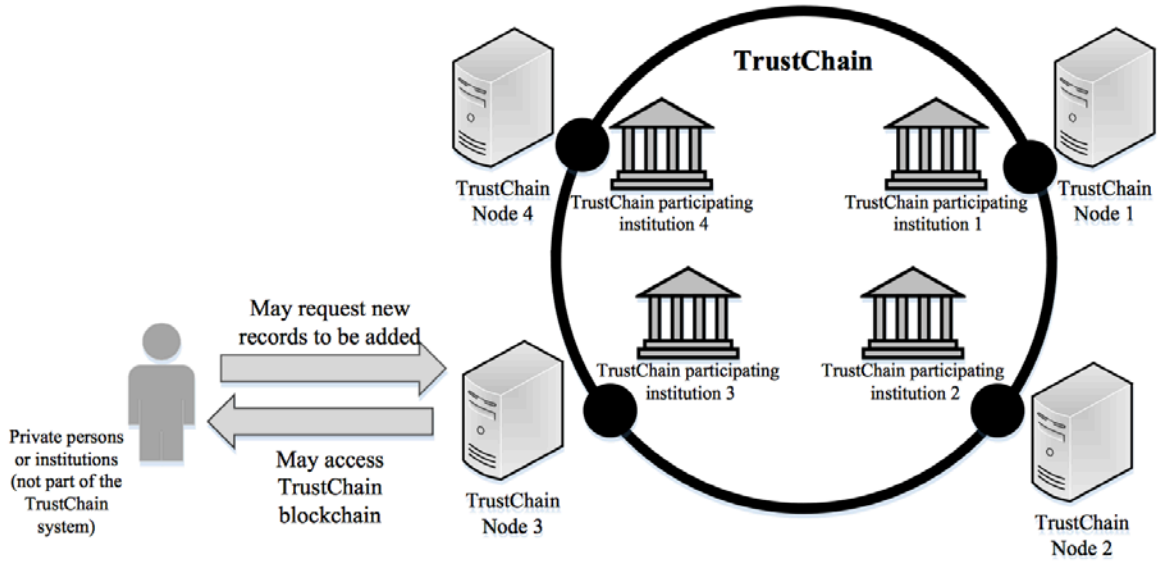


Figure 11. Overview of TrustChain System, which leverages blockchain technology to extend guarantees of integrity and authenticity of digitally signed records.

Issues relating to long-term preservation of blockchain records

The solutions discussed in the previous section both point to how records professionals can use blockchains to address problems in a recordkeeping world that is not fundamentally different from the current state. Answering questions about how to ensure the long-term preservation of blockchain records in a future state in which records creation and keeping are fundamentally transformed by distribution and decentralization is still uncharted territory, however. Current models of long-term digital preservation are premised on ingesting records selected for long-term preservation into archival institutions. Blockchain technology raises the question of how to bring records that exist on possibly thousands of independent and globally distributed nodes into a single archival repository. The answer is likely to be: you don't. Blockchain technologies are very good at ensuring the integrity of records; as Lemieux notes, "blockchain technology […] is transforming the creation and keeping of authentic records and long-term preservation of archives."[130] However, blockchains are not, in and of themselves, archives or digital preservation systems. So, if traditional custodial approaches to long-term archival preservation are unlikely to work in blockchain recordkeeping contexts, then what?

Some argue that we can rely on the LOCKSS principle; that is, the idea that "Lots of Copies Keeps Stuff Safe." That is certainly a viable option as long as a particular blockchain system continues to operate. Blockchains, however, are susceptible to human-based governance challenges that, at least at present, produce plenty of acrimonious disputes over technological changes to the operation of the system. Whenever one of these disputes occurs, i.e., when a certain group of core developers has a "fit," a "fork," or split in the blockchain soon follows. This pattern of fits and forks threatens the viability of the LOCKSS principle, since a fork in the chain that does not continue to be supported by a sufficient number of nodes operating the system may wither and die off, taking all copies of the records stored with it, or at the very least, it may consist of so few nodes that the integrity of the records on the system could be called into question or attacked (e.g., by executing a 51% attack).

In the near future, then, blockchain records preservation will have to be accomplished either through integration with existing digital preservation technology, or by leaving the records chosen for preservation in the blockchain (while destroying the rest at the end of their retention period). Neither solution is ideal. Existing digital archive software does not provide the same affordances as blockchain technology, and those might well be lost in trying to integrate a blockchain system with an existing digital archives technology. Leaving the records in the blockchain system, without further design for the particular demands of long-term preservation, is also far from ideal.

As Lemieux finds in her examination of blockchain through the lens of digital preservation standards, including the Open Archival Information System (OAIS) model and its associated ISO Standards, long-term digital preservation imposes a number of specific demands on a system which are not a given with how current blockchain systems are designed. One possible answer to the problem of abandoned forks or entire blockchain systems may be to transfer the records in them into a virtualized version of the system, such as a cloud operating simulated nodes representing the version of the blockchain protocol used to generate the particular blockchain records. While this would enable preservation, it relies on the continued existence of a centralized archival authority for the persistence and preservation of the integrity and authenticity of the records.

A slightly modified version of the above approach would be to have several archival institutions or other concerned social actors operate "preservation nodes" that keep a blockchain

platform (and the records recorded using it) alive. The challenge with this approach is finding an incentive and the resources to implement this model. Archival institutions have a mission to preserve society's collective memory and are publicly funded by nation states (mostly not very well) to do so. Private social actors concerned with long-term preservation would have to find alternate sources of funding, such as private donations. In all cases, measures would be needed to ensure sufficient independence and numbers of nodes to guarantee the long-term integrity and persistence of the records.

Given that operating a multitude of deprecated blockchain protocols is likely to place a strain on any system, whether distributed or centralized, there is a need to consider how to transform a record created and recorded in one blockchain system into a record on another system without losing the guarantee of its integrity and authenticity – in other words, a blockchain digital migration strategy.

A recent report by the US National Archives begins to grapple with the issue of long-term preservation of archival documents in blockchain form, suggesting a number of challenges and possible approaches to transfer and preservation of government blockchain records, including the possibility that the National Archives could operate as a blockchain node, noting that, in this scenario, the transfer of archival documents becomes moot (since the national archives operates as part of the blockchain system), but raising a question about whether legal transfer happens when the national archives become part of the blockchain system or later.[131] Archival preservation raises many process and technical challenges yet to be solved.

Another issue that surfaces is the eventual obsolescence of the cryptographic algorithms used in the creation of blockchain records. The most obvious source of such obsolescence, at present, is thought to be coming in the form of quantum computing. As Rodenburg and Pappas explain, "The inversion of hashes is assumed to be computationally difficult. If this can be dramatically simplified by a quantum computer, the authenticity of the upstream blockchain can no longer be guaranteed and the authenticity of entries in the blockchain is compromised."[132] The sheer computing power of this novel method of computing makes the breaking of existing cryptographic algorithms child's play. The tamper resistance of blockchain technologies relies on the security of the hashing algorithm. As quantum technology develops further, blockchains may well require redesign, and archives relying on blockchains may require migration. Obsolescence and insecurity, of course, are not unique threats to the blockchain, but common to all digital

systems. Indeed, the Information Assurance Directorate of the United States' National Security Agency states that "algorithms used in national security systems require twenty years for full deployment and should be designed to protect information for at least thirty years,"[133] a time scale that pales in comparison to the requirements of digital archives. In a sense, the breaking of the hash function would not be entirely dissimilar to the problem digital archives currently face with the expiration of digital signatures to ensure records' authenticity. The expiration of the signature, or the breakability of the hash, does not mean that the records have been tampered with or are in any way less authentic. Rather, it reduces the value of the signature/hash as evidence of records' authenticity. Given the central role that cryptographic tamper resistance plays in the ability of blockchain technologies to ensure records' integrity, blockchain records management systems must be designed with an eye to ensuring authenticity even if the hashing function is weakened by quantum computing or other disruptive technologies. Naturally, researchers are working on quantum cryptography as a solution. This suggests that there will be a need to introduce mechanisms for upgrading from outdated cryptographic primitives to more advanced ones, which presents yet another digital preservation challenge.

Yet another challenge associated with the long-term digital preservation of blockchain system-based records is, as discussed in a previous chapter, the very distributed and decentralized nature of existing blockchain ecosystems. Such systems rely upon a complex network of links between records (e.g., to instantiate the archival bond by linking records to information that establishes the procedural context of their creation and to other records associated with the same procedure) and between different intellectual components of records (e.g., between the content in the record that expresses the will of its author – the disposition – and the signature, or means used to validate the document). Currently, these links are very fragile, being dependent upon technical components that may reside in remote locations under the control of different legal entities. This fragility means that they may also not be very persistent. As a consequence, important elements needed to understand the intellectual content of records while relying upon them as evidence may not be available over time. Addressing this issue requires complex technical and procedural preservation strategies that have yet to be explored.

Aside from preservation challenges related to the distributed and decentralized nature of records and recordkeeping, there is the question of how to handle the preservation of self-

sovereign blockchain records. In a world of data self-sovereignty, as discussed at greater length in Chapter 8, records, especially those containing personally identifiable information used for identity or attestation purposes (e.g., civil registrations, driver's licenses, educational certificates), may no longer be kept in central databases nor even be recorded in blockchain systems. Such records will be held only in individuals' personal crypto wallets, or in their personal data store of choice. Given that a future world of data self-sovereignty is premised upon a fundamental distrust (increasingly well-deserved) of centralized information processing and storage, a solution wherein individuals may deposit their records into a centralized archival institution is unlikely to present an attractive option. What then? Archival researchers have only just begun to reflect upon this challenge.

Conclusion

The future world of blockchain-based records creation and keeping is still emerging. While archival researchers have begun to think about how to leverage this novel technology to address existing problems, they have yet to grapple with the challenges that growing use of blockchain technology for a wide variety of use cases pose, and the attendant alterations in the nature of records and recordkeeping, will present. It is still difficult for records and archival professionals to even understand blockchain technology, let alone envision the transformations that will take place in a world of blockchain-based data and records self-sovereignty. More difficult still is the task of envisioning what long-term digital preservation challenges may need to be identified and solved in such a world. However, if the world is set upon increasing use of blockchain technology for the creation and keeping of records, records and archival professionals, as the professionals most likely to understand what is at stake if society fails to devise ways of preserving blockchain records, must begin to explore these challenges and research possible solutions.

Chapter 7: Blockchain Records as Evidence

Introduction

Given the importance of records creation and keeping in the operation of blockchains as a technology of trust, the creation and preservation of trustworthy blockchain records cannot be overemphasized: when the design or operation of blockchain systems interferes with the trustworthiness of records, one of the key bases of trust offered by blockchains is eroded. Bad actors may repudiate their transactions, undermining the foundation of confidence of all participants in a blockchain network to act. They may, for example, double-spend their cryptocurrencies, sell their land twice, or dispute that they have given consent. Moreover, they may alter the record to remove "inconvenient" facts about actions they have taken to avoid accountability or may insert false claims into the ledger in order to gain some undeserved benefit. Thus, blockchain systems, in order to fulfill their purpose, should be designed to – indeed, must - provide final, definitive and immutable records of transactions.

Many developers of blockchain systems have made, and continue to make, strong claims of being able to provide trustworthy records. Brian Deery, Chief Scientist at Factom has claimed that "*Blockchains are archival record keepers. Permanent and transparent, they are the perfect solution for an industry-wide problem of transmitting and archiving critical accurate records.*"[134] Similarly, BlockTech has claimed that their blockchain-based distributed application, Alexandria, ". . . *preserves the integrity of the historical record. It taps into collective, on-the-ground reporting by scraping Twitter as events unfold and prevents after the fact censorship by archiving the information on a blockchain.*"[135] In earlier work on blockchain technology for recordkeeping, we found that claims by many blockchain systems developers seemed to amount to no more than hype and therefore launched a program of research, "Records

in the Chain," to investigate the issue of trustworthiness of records in blockchain recordkeeping environments with a view to assisting blockchain system developers to identify gaps and strengthen the design of their systems vis a vis trustworthy recordkeeping.[136]

The theory of trust in records

Much has been written over centuries about the basis of trust in documentary evidence, particularly from a legal and historical perspective.[137] Our approach to the study of the trustworthiness of blockchain-based records draws upon archival and diplomatic theory, especially that developed and systematized over the past 30 years at the University of British Columbia, which has sought to create a modern diplomatics applicable to new digital forms of records.[138] [139] Diplomatics may be defined as "the discipline which studies the genesis, forms, and transmission of archival documents and their relationship with the facts represented in them and with their creator, in order to identify, evaluate, and communicate their true nature" (e.g., their authenticity).[140] In contrast, archival science is the study of archival documents as aggregates – e.g., archival *fonds* – and focuses on analyzing the interrelationships among the archival document and other documents of the same provenance, the relationship of the archival document and the transaction of which it forms a part, and the contexts in which the aggregated archival documents are situated, e.g., the organization, and the juridical system. Together, diplomatics and archival science form complementary perspectives that enable understanding of the nature and basis of trust in records as sources of evidence of the facts and acts to which they refer. In general, this perspective is characterized by the requirement that records possess three fundamental qualities to be considered trustworthy: accuracy, reliability and authenticity.[141] [142] These decompose into various characteristics and requirements as represented in Figure 12, our "Taxonomy of Trust."

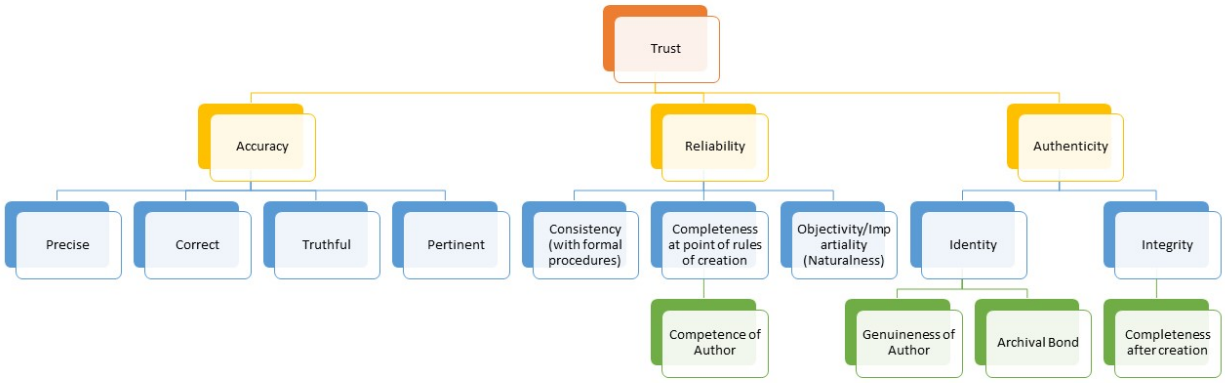


Figure 12: Taxonomy of Trust (Source: Lemieux, 2017, rendered by Alysha Joo).[143]

To be considered accurate factual representations, records must be precise, correct, truthful and persistent. Reliability concerns the "trustworthiness of a record as a statement of fact. It exists when a record can stand for the fact it is about. . . [and is] established by examining the completeness of the record's form and the amount of control exercised on the process of its creation."[144] In the digital environment, an assessment of the reliability of the record entails examination of the system used in the creation of the record (i.e., whether it was a reliable writer of the statement of fact the record represents). An assessment of reliability also includes examination of whether the record was created by an author who is competent to give effect to the transaction. Finally, it includes examination of whether the record was created in the usual and ordinary course of conducting activities, which imparts the record with impartiality (a certain detachment from the future use of the record that is said to imbue it with "documentary objectivity" in relation to the facts represented even if the author of the record is not an objective observer of those facts) and results in a natural accumulation of records over time. Authenticity refers to "[t]he trustworthiness of a record as a record; i.e., the quality of a record that is what it purports to be and that is free from tampering or corruption."[145] Over the centuries, authenticity

has been established by an examination of the characteristics of records or by virtue of the principle of *ius archivi*, a presumption of authenticity conferred upon records by virtue of their being preserved by special custodians and in special places (e.g., public archives) accorded special legitimacy under a juridical system.[146] When established by an examination of the record, on the other hand, authenticity relies upon establishing the unique identity of the record, which is accomplished through an examination of the archival bond (the interrelationship of the record to other records formed as part of the same transaction and its relationship to that transaction), the identity of the author (i.e., a determination that the purported author of the record is genuine), and the record's integrity, the "quality of being whole and unaltered from loss, tampering, or corruption."[147]

Questions of trustworthiness in blockchain records

Through an examination of several different types of blockchain systems used for recordkeeping, as summarized in Appendix B of this study, we have formed some high-level initial impressions of the impact of blockchain technology on the trustworthiness of records.

With respect to accuracy of records, we have found that blockchain ledgers will only be accurate to the extent that creators of records are motivated to, and processes of records creation, produce accurate records. In other words, there is nothing inherent in blockchain systems that makes records *ipso facto* any more or less accurate. It is a case of the well-known adage "garbage in, garbage out." The concern about the accuracy of records in blockchain systems comes as a result of claims about the accuracy of blockchain recordkeeping systems, such as in the quote from Brian Deery of Factom *supra*, when such a presumption cannot be made alone on the basis of making an entry into a blockchain ledger. Additional checks to ensure, at the point of creation, or subsequently determine through examination of the accuracy of records, would need to be made.

With respect to reliability, which concerns processes of creation, we also note a number of problematic aspects of blockchain recordkeeping, any of which may impact upon the trustworthiness of ledger records:

1. Consistency: While in some of the use cases we have studied there exist well-defined and documented procedures for the creation of records whether these processes are manual or

automated, blockchain technology introduces a new dimension that is not yet fully incorporated procedurally. To illustrate, in the pilot of a blockchain system for land transaction recording in Brazil, the blockchain recordkeeping system was running in parallel to the existing registry system. In addition, the pilot involved transcribing existing records into the new blockchain ledger. This could result in inconsistency between the versions of land titles found in the parallel systems (i.e., the original registry and the blockchain ledger), presenting the opportunity to dispute the legitimacy of one or the other. This points to the need to carefully consider how blockchain systems will be introduced into the process flow of transactions and to establish procedural controls that control potential sources of inconsistency.

2. Completeness: Our case studies to date reveal that the absence of well-defined procedural controls over records creation processes using blockchains means that completeness is difficult to determine and not well-defined. For example, questions arise in a blockchain recordkeeping environment as to whether transactions should be considered complete when a transaction record is digitally signed or when that record is validated, confirmed, and entered into a blockchain ledger, or when the ledger entry has been confirmed and updated by the number of nodes determined to be sufficient to avoid repudiation. This is an important distinction, especially when blockchain records represent contractual agreements that may be considered legally binding, as in the case of consent and access to use of health records, or in conferring rights and entitlements, such as in the case of land transfers. Determination of whether, and at which point, a transaction can be considered complete and having entered into effect is often very significant in settling legal disputes. Much more clarity is needed therefore, around the status of transmission of a record and of its processing and transformation as it moves through recording processes that involve blockchain recordkeeping.

Moreover, significant questions remain as to the status of blockchain records under law. It is not clear, for example, whether a digitally signed blockchain transaction record such as a smart contract and ledger entry, would be recognized as legally binding in law. Some jurisdictions, such as the U.S. state of Arizona, have declared signatures secured through blockchain systems to be considered digital signatures, and contracts created using blockchain systems to be on par with contracts created using other technologies of record creation. In other jurisdictions, however, the status of blockchain-based digital signatures and records as

instruments capable of giving effect to intended transactional outcomes (i.e., contractually binding legal agreements) has not yet been clarified in law.[148]

3. Competence: Our case studies reveal that it is not always clear who is the authority with competence to enact a transaction and, moreover, if that authority was actually competent to enact the transaction (e.g., fully aware of what was being consented to in the case of a digital signature used to authorize consent to the use of healthcare data). Uncertainty surrounding the question of competence exists in blockchain recordkeeping environments because addresses might not be explicitly linked to the legal identity of a competent authority. Indeed, in public blockchains, the legal identity of the transacting party is not linked to the transacting address and legal entities (persons, corporations, etc.) and real-world entities (e.g., services, machines) operate pseudonymously. In some permissionless, public blockchains (e.g., Monero), pains are taken to deliberately mask the source of the originating address, and thus, the real-world or legal identity of the transacting party, in order to protect privacy. As a result, in such systems, determinations of competence can remain murky. It is possible to clarify the question of competence in the design of blockchain systems, however. For example, we have observed three design alternatives thus far: the blockchain could require identification and authentication (as is the case in permissioned blockchains) to make it easier to link a real world and/or legal identity of an entity to a blockchain address. Another approach would be to capture real-world and/or legal identity as metadata within a blockchain transaction or as a link within a transaction out to an external data store with this information, preferably in encrypted form, to protect personally identifiable information and privacy. A third approach involves using verifiable claims that establish the identity of transacting parties.[149] Each design choice has its pros and cons in relation to the operation of the system and compliance with regulations such as GDPR (which is outside of the scope of the discussion here, but dealt with in chapter eight), but which would have to be taken into account.

A second issue concerning competence is how to prove that a transacting party, once identified as such, was, in fact, competent to engage in the transaction. To the best of our knowledge, this is not a determination that can be made simply by examining the records or the recordkeeping system itself, whether it is a blockchain recordkeeping system. It must be determined by examining facts surrounding the context of records creation. Typically, however, in a traditional recordkeeping environment, attestations about the competence of the transacting

party are made by means of witnessing the signature. Thus, we surmise that a similar approach could be used in blockchain systems by employing "multisig," the use of multiple signatures on records created using blockchain systems, whenever it is especially important to demonstrate competence (e.g., the production of legally binding smart contracts).

4. Objectivity/Impartiality: At this stage, most of the blockchain-based recordkeeping systems we have observed have been operating as pilots outside of the "usual and ordinary course of business" and thus lack the objectivity, impartiality and naturalness typically accorded to records as reliable evidence. There is no reason, however, that, once blockchain systems are incorporated fully into the usual operations of an organization, consortium of organizations, or group of interacting participants, they should not be considered as objective, impartial or natural in the same manner as other types of records.

5. System reliability: Where once it was the records themselves that primarily determined reliability, now an examination of the system of recording records weighs much more heavily in the determination of reliability.[150] It has already been noted that it is still rare to be able to prove that a blockchain system was operating in the usual and ordinary course of business, which is one of the standards by which the reliability of record producing systems is typically judged. More importantly, however, is the question of how to determine whether the system was operating properly in a technology that is still emerging. Proper operation of the system is difficult to determine because technical standards of operation are constantly changing and may not always be well-documented and transparent. In addition, security of the system is a major consideration in determinations of proper operation and the ability of systems to produce reliable records. Blockchain systems are not immune to security vulnerabilities; in fact, there are a number of known vulnerabilities (see Appendix C). There also have been some spectacular exploits relating to interacting services, such as cryptocurrency exchanges, in the operation of smart contracts, and in blockchain wallets. We observe that many blockchain system developers do not have well-developed and documented security models relating to the core blockchain processing layer. Security models are also lacking related to the broader blockchain solution stack, nor is there evidence of systematic testing of the system's security posture and vulnerability to lines of attack. This is likely due to the immature state of development of blockchain and associated technologies on the whole. Finally, a major issue with *post hoc* determination of the reliability of all digital record creation and keeping systems, including those

based on blockchain technology, is that security patches and measures taken to mitigate vulnerabilities can make it very difficult to determine whether a system was operating reliably at any given point in time.[151] This problem is amplified in the context of blockchain technology, however, given its dynamic, emerging nature.

With respect to authenticity – the trustworthiness of a record as a record, most blockchain solution developers understand authenticity in terms of integrity. As Cohen observes, however, "[t]he notion that using cryptographic checksums to verify the lack of alteration of a bit sequence does not even begin to address the issues of authenticity of a record in presentation and in reliability in the sense of relationship to original writing or any sort of ground truth. Causality works differently."[152] Indeed, it is usual for recordkeepers to have to transform the bit structure and make modifications to records from time to time in order to preserve them or render them as accessible using updated technical systems. Such changes would completely invalidate the hashes of the originating records stored in a blockchain system and would thus make it impossible to use them to check the integrity of the record.

Blockchain systems typically miss instantiating the archival bond as well. As Lemieux and Sporny write: "**Implicit in the definition of authenticity is the notion that records have a unique identity, for without such it would be impossible to establish that the record is what it purports to be** (emphasis in original text)**.** In other words, it would be impossible to prove that a record was an inauthentic copy of another record (i.e., a forgery), unless both records (the record to be proven and the record that serves as proof) have unique identities. . .If records are inauthentic they cannot serve as evidence (except as evidence in relation to their own inauthenticity), and therefore important rights and entitlements cannot be upheld."[153] The unique identity of a record is created by the archival bond, the "originary, necessary and determined" relationship between and among records that participate in the same activity.[154] In traditional, centralized digital recordkeeping systems, the archival bond is instantiated by associating descriptive metadata, such as a classification code that connects it with its transactional context. Typically, the archival bond is not instantiated in blockchain systems, likely because developers are unaware of its importance in relation to establishing the authenticity of records. Moreover, it is mistaken to think that because every block of transactions (and thereby every transaction) in a blockchain is chained together in a time-ordered sequence that the archival bond is instantiated and preserved. The formation of blocks is agnostic to the context of the records, with blocks

forming not on the basis of shared procedural origins but rather on the basis of time of entry into the ledger. This means that information needed to establish the unique identity of ledger records may not exist or be very hard to find.

There are ways to instantiate the archival bond in blockchain systems to overcome this weakness: Lemieux and Sporny propose embedding hash links within blockchain transaction records in order to create a bond between a ledger entry and an ontology that can later be used to interpret the semantics of the entry and identify its transactional context.[155] Another solution is to use a special tagging mechanism, such as the Colored Coins protocol, which tags the transaction record in a way that allows it to be identified with the transactional context of its creation.[156] Still another option is to use the blockchain only for the creation and keeping of records concerning a specific procedure, such as land transaction recording. This approach would likely require using a private, permissioned blockchain wherein the use of the system is pre-determined and controlled, in contrast to any of the large public blockchains which would, by their nature, always accept a variety of procedurally diverse transactions.

Similarly, determining the genuineness of the author of a record may prove challenging since in public, permissionless blockchains do not provide an explicit and stable link between a transacting address and a legal or real-world entity. There are ways to trace transactions back to their likely author, such as those used by law enforcement agencies investigating crimes, but they require a good deal of sleuthing and are not guaranteed to produce results, especially since developers of public, permissionless blockchains are very concerned about protecting the privacy of transacting parties and are constantly developing new ways to protect identity.[157] In private, permissioned blockchains, it would be no more difficult to identify the author of a record than would be the case in any other digital recordkeeping system. Such systems routinely employ identification and authentication as part of their design.

We note that some jurisdictions have enacted legislative provisions which confer upon the records produced by means of blockchain technology a *publica fides* – a confidence conferred by legitimate public authority in the authenticity of the record. This follows the tradition of *ius archivi*, which, as noted *supra*, is a presumption of authenticity of records by virtue of their being preserved by special custodians and in special places (e.g., public archives) accorded special legitimacy under a juridical system.[158] As examples, a law passed in 2016 in the

State of Vermont (H.868) (Act 157, Sec. I.1. 12 V.S.A. § 1913), an act relating to miscellaneous economic development provisions, provides that:[159]

> (1) A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and:
>
> > (A) the date and time the record entered the blockchain;
> >
> > (B) the date and time the record was received from the blockchain;
> >
> > (C) that the record was maintained in the blockchain as a regular conducted activity; and
> >
> > (D) that the record was made by the regularly conducted activity as a regular practice.
>
> (2) A digital record electronically registered in a blockchain, if accompanied by a declaration that meets the requirements of subdivision (1) of this subsection, shall be considered a record of regularly conducted business activity pursuant to Vermont Rule of Evidence 803(6) unless the source of information or the method or circumstance of preparation indicate lack of trustworthiness. For purposes of this subdivision (2), a record includes information or data.
>
> (3) The following presumptions apply:
>
> > (A) A fact or record verified through a valid application of blockchain technology is authentic.
> >
> > (B) The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain.
> >
> > (C) The person established through such a blockchain as the person who made such recordation is the person who made the recordation.
> >
> > (D) If the parties before a court or other tribunal have agreed to a particular format or means of verification of a blockchain record, a certified presentation of a blockchain record consistent with this section to the court or other tribunal in the particular format or means agreed to by the parties demonstrates the contents of the record.

Although these legislative provisions are intented to grant legitacy to blockchain records, thereby providing greater certainty to agencies who may wish to use this technology for recordkeeping, questions remain about how such provisions would be implemented in practice. These include who would be considered a "qualified person" pursuant to sub-section (1) or "the person who made such recordation" pursuant to sub-section (3)(C) in a system that may be operating pseudonymously and autonomously, as well as how to achieve the requirement for there to be a date and time of recordation (e.g., reliance on system time or use of an external source of date and time verification).[160] [161]

A law passed by the State of Arizona in 2017 gives recognition to smart contracts, conferring upon a smart contract the status of an electronic record, and specifying that: "Smart Contracts may exist in commerce. A Contract relating to a transaction may not be denied legal effect, validity, or enforceability solely because that contract contains a Smart Contract term."[162] The issue here is that the definition of smart contract is "An event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger," but the program, if following the norms and laws applicable to other types of contracts, technically might not be considered complete as a record (i.e., in effect) until digitally signed (and witnessed), validated, confirmed and entered into a blockchain ledger by a predetermined number of nodes; that is, until it could not be repudiated. It is the difference between stating "that runs," possibly encompassing what might still be considered a draft contract, and "has run" and produced an outcome, which is closer to what traditionally would be considered a final, definitive contract. Immutability would be conferred by propagation out to the requisite number of nodes on the blockchain network to assure confirmation as part of the ledger.

The emerging nature of blockchain technology taken together with variations and instability in its mode of operation, and the difficulty of applying existing legal concepts, suggests that legislating a presumption of authenticity is premature. Indeed, our view was confirmed in a report prepared by the State of Vermont's public archives at the time that the state's blockchain legislation was under discussion.[163] We observe that jurisdictions that are passing such laws appear to be doing so for economic reasons rather than overriding consideration of whether blockchain records can be established to be reliable and authentic.[164]

We also note that public blockchain system developers and proponents sometimes see themselves as presenting an alternative to existing juridical regimes, even calling for the disintermediation of governments.[165] [166]

Public recordkeeping has for centuries, provided the foundation for society's institutional systems (i.e., government, education, and so on).[167] Thus, blockchain, in staking a claim to disintermediate and replace the traditional public notary, such as signaled in the quotes from Factom and BlockTech *supra*, presents the strongest challenge yet to "the monopoly of the state over the promulgation, formation, keeping and verification of institutions and the public record."[168] Certainly, on the face of a diplomatic and archival theoretic examination of blockchain recordkeeping systems, this claim would seem to be highly problematic. However, with growing support for self-sovereign blockchain recordkeeping, there may arise a de facto legitimacy to this claim, especially in the context of failed states. The degree to which blockchains will be successful in asserting a *ius archivi* power to confer authenticity, as with so much in this emerging technical space, opens an intriguing future line of research and remains to be seen. We argue that any such claims should be supported by paying careful attention to incorporating principles of good recordkeeping into the design of blockchain systems so that claims can be backed up with substance. Not to do so would introduce unintended dystopian consequences.

Conclusion

Trusted records creation and keeping is central to the operation of blockchains as a technology of trust. Yet, careful case study analysis of the design of several different blockchain systems and a review of published literature on blockchain systems and their designs indicates that little attention has been paid to this aspect of blockchains, and current system designs may fall short of archival standards for the trustworthiness of records. Our program of research is still ongoing and thus what we present here are our preliminary results. As with all preliminary results, especially ones that relate to a technology that is still emerging and dynamic, there is still much to discover and future results are likely to considerably extend, and possibly revise, these findings. Nevertheless, early results suggest that before any strong claims to produce trustworthy records can be made about blockchain technology, additional thought needs to be put into the design of many of these systems as systems for the keeping of trustworthy records.

Chapter 8: Who Owns the Record? Ownership & Custody of Blockchain Records

Introduction

In the past decade, data breaches (such as the Sony PSN hack,[169] the Equifax hack,[170] or even more recently, the Facebook-Cambridge Analytica scandal,[171] in which the personal information and the records of individuals were compromised either due to poor information security controls, or through the abuse of control over consumer information by an organization), have exposed the risks of centralizing the custody and control of information and records. Increasingly, data breaches have brought much discussion and debate surrounding the ownership of an individual's information and records. There is a visible desire expressed from the general public to own and control their personal information and records. For instance, in the healthcare industry, the trend in recent years has been gravitating towards patients managing their own record of health information, through electronic applications called personal health records (PHR).[172] PHRs enable patients to 'own' their personal health information, through the ability to authorize or revoke access to their PHR anytime, and to whomever the patient chooses to share it with, such as with a medical practitioner, spouse, or family members.[173] Depending on the jurisdiction and legislation, as well as the terms of use, the claim that patients can 'own' their personal health information needs to be closely examined. For instance, in an American context,

generally a person retains ownership of a PHR when they create it. However, if information from the PHR is shared with a medical professional or other third party provider, it becomes part of the medical record owned by that medical professional or third party.[174] This only goes to show, that any technological solution promising or claiming 'ownership' over an individual's own data or records, should first be examined and considered with extreme caution given that existing legal frameworks are unlikely to be jettisoned entirely any time soon.

Emerging from the growing desire for self-ownership and control over one's information and records, often referred to as "self-sovereignty," are solutions leveraging blockchain technologies. The distributed and cryptographically secure nature of a blockchain are appealing for use cases in which users are put in control of their own information and records, such as for digital identity or in healthcare, for patient records and personalized medicine. In order to address the risks of centralized storage and control of information and records, and to ensure compliance with data protection legislation such as the European Union's GDPR (General Data Protection Regulation), organizations are turning to solutions which are incorporating decentralized models of information governance leveraging blockchain technologies.[175]

However, in a blockchain recordkeeping system who owns the record? As Lemieux (2017) has demonstrated, "blockchain systems offer a new form of records generation use, storage and/or control."[176] A blockchain record is potentially distributed and shared with many custodians containing a full copy or a partial shard of the record. The issue of ownership is dependant on how a blockchain is being used in managing information and records in an organization, what type of blockchain system is implemented (e.g., public, private, permissioned, etc.), how it is designed, and ultimately, where the records are stored.

This chapter intends to explore the issues surrounding blockchain records and ownership at a high level, drawing from research on the issues of record ownership in the cloud, by first discussing definitions of ownership in terms of custody and control, as well as exploring several theoretical blockchain recordkeeping systems scenarios and how ownership would theoretically apply. This chapter by no means aims to provide legal interpretation or guidance to the issue of legal ownership of records entrusted to blockchain recordkeeping systems.

Custody and Control

When discussing the ownership of a record in this chapter, it is important to contextualize how custody and control is being used to distinguish or determine ownership. The following definitions are defined from a Canadian privacy legislative perspective, and are the terms used in the province of British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA),[177] which are not explicitly defined within the Act itself. The purpose of FOIPPA is to hold public bodies accountable to the public and to protect personal privacy.

"Custody: 'custody' (of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the records. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security. Where more than one copy of a record exists, more than one public body may have custody of a record.

Control: 'control' (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating, and administering its use or disclosure. Where the information in a record directly relates to more than one public body, more than one public body may have control of the record. The public body with the greater interest processes the request for information. The following are some factors indicating that a public body has control of a record:

- the record was created by a staff member, an officer, or a member of the public body in the course of his or her duties;
- the record was created by an outside consultant for the public body;
- the record is specified in a contract as being under the control of a public body;
- the content of the record relates to the public body's mandate and functions;
- the public body has the authority to regulate the record's use and disposition;
- the public body has relied upon the record to a substantial extent;
- the record is closely integrated with other records held by the public body; or,
- the contract permits the public body to inspect, review, possess or copy records produced, received or acquired by the contractor as a result of the contract."[178]

Other jurisdictions have legislation that are similar in defining 'ownership.' For instance, Rule 34(a) and Rule 45(a) of the United States of America's Federal Rules of Civil Procedure obligates a party to produce records or electronically stored information (ESI) in that party's

"possession, custody, or control." However, this phrase is not explicitly defined in the Rules, nor is it being consistently interpreted and applied in case law. It is acknowledged that new technologies are further complicating who 'controls' the record or ESI.[179]

Essentially, the main takeaways for contextualizing how ownership is discussed in this chapter are that custody is the physical possession of a record, and control is the power or legal authority to manage a record throughout its life cycle. Custody does not necessarily mean the legal control or authority over a record.

Blockchain Recordkeeping Systems and Record Ownership Scenarios

In considering issues of information or record ownership in a blockchain system, it is important to identify whether the blockchain is being utilized as a recordkeeping system itself, or as a part of a larger recordkeeping system as a whole. Depending on the context, the term 'recordkeeping system' can invoke different interpretations in different contexts, and as a component of information governance, recordkeeping systems may be defined as "organized sets of people, policies, processes, tools, technologies, ongoing education, and maintenance required to establish and support the infrastructure for recordkeeping within an organization."[180] In the latter described scenario, the blockchain is only a component of a recordkeeping system in the context of information governance. Through an analysis of case studies, Lemieux (2017) has identified three emerging typologies of blockchain solutions for recordkeeping, and refers to them as the mirror type, the digital record type, and the tokenized type.[181]

Mirror Type Blockchain Recordkeeping Solutions

In mirror type blockchain recordkeeping solutions, records are neither created nor stored on-chain. Essentially, the blockchain in these solutions types, functions "as a repository of 'digital fingerprints', or hashes… The original records, which may be born paper or digital, but not exist in digital form, are hashed… These hashes are anchored into the blockchain, with the blockchain being used as a means of validating the integrity of the records."[182] In the recordkeeping scenario in which a blockchain is part of the recordkeeping system, it can be said that the recordkeeping system 'mirrors' current practices of recordkeeping in organizations and the blockchain is being used to enhance the preservation and/or security of the authenticity of the records. It does not matter whether the blockchain in question is a public (e.g., Bitcoin) or private

and/or a permissioned blockchain, because the issues of record ownership are then the same as current issues of record ownership in relation to determining who has custody and control of an organization's records. These records are not generated on-chain. The straightforwardness or difficulties of determining record ownership are then dependant on where the original records or non-hashed records reside in terms of storage and custody, as well as who has control over them. Factors which complicate record ownership in this scenario include storage location – are the original records stored on the premises of the originating organization (e.g., physically in storage or electronically on localized storage options, such as on disk or on local servers), or are they stored with a third party (e.g., a records storage centre) or in the cloud? The cloud is a records storage environment that further complicates the ownership of electronic or born-digital records, depending on whether the cloud is located on premises (e.g., local server) or offered as a service through a third party organization, such as Microsoft or Amazon, and in which case, the cloud functions as a disembodied metaphor for hosting an organization's records in remote data centres within a jurisdiction or cross-jurisdictionally.

Mirror type blockchain recordkeeping solutions may also implement peer-to-peer distributed file systems, such as InterPlanetary File System (IPFS), which shares similarities and characteristics with BitTorrent and Git, in which "IPFS nodes store IPFS objects in local storage. Nodes connect to each other and transfer objects. These objects represent files and other data structures."[183] The distribution of files in a distributed network presents even further complications in determining the ownership of a record. Essentially, the record is "chunked" by IPFS and cached locally with the creator and is also cached with all nodes who request the record. This caching is only temporary until memory needs to be freed for a new file.[184] Unlike other peer-to-peer hosting services, IPFS nodes are designed to be able to "only store and/or distribute the content they explicitly want to store and/or distribute."[185] This means that custody of a record is distributed to all who request access to the record, and that other peers in the IPFS network do not have to 'host' or store everyone's content in the network in order to be a participant. As a result, there is some degree of control concerning who gains custody over the record. There is no control to guarantee the long-term availability of a record, because once a peer in the network stops hosting a record, either deliberately or through the freeing of their memory cache to make room for another record, the availability of the record is at risk.

Digital Type Blockchain Recordkeeping Solutions

The other two emerging blockchain recordkeeping typologies, the digital record type and the tokenized type, are even more challenging in considering the issues of record ownership. The main difference which separates digital records and tokenized blockchain solution types from mirror blockchain solution types is that records are generated or stored on-chain. In a technological context, the term recordkeeping systems "is often used to refer to business systems that manage records – that is, systems that capture, maintain, and provide access to records over time."[186] In digital recordkeeping blockchain solutions, records are said to be "actively created on-chain in the form of 'smart contracts.'"[187] In this scenario, the blockchain is the recordkeeping system from a technological context. Lemieux addresses one of the most fundamental challenges of determining record ownership in digital blockchain recordkeeping solutions by questioning what is the actual record in this system? Lemieux poses: "It may be considered to be the instructions or procedures drafted in narrative or diagrammatic form to be implemented in a smart contract. It may be the raw code written in the smart contract scripting language… It may be the completed code produced after a complier converts the instructions into a machine-code or lower level form so that they can be read and executed by a computer."[188] Given these implications, the issues surrounding record ownership is further complicated by the fact that "smart contracts encode procedures that execute among a multi-stakeholder network as part of work process flow."[189]

Whether a blockchain is a public, private, or permissioned ledger further contributes to this complication. On a public permissionless blockchain network, such as the Bitcoin network, anyone can join the network and the identity of participants are pseudonymous at best. As a result, no one knows where the record is stored or who specifically has custody of the record since in distributed networks, every participant theoretically has a copy of the record. In a private network, within one or more organizations, ownership could be potentially more determinable, since all participants in the network are known – or in the case of a single organization, all participants are the same. However, jurisdiction and transnational data flows would have to be considered in a multi-national organization. In considering the nature of digital blockchain records, ownership is more readily determinable within an organization, or between organizations in a private blockchain network since contracts, policies, or other regulations would be in place detailing ownership. Permissioned blockchain networks face similar hurdles

but generally, permissioned blockchain networks are public and therefore, all participants are known or identifiable. As a result, the custody of records is held by all participants in the network, and the participants in a smart contract transaction control the record with their private key.

Tokenized Type Blockchain Recordkeeping Solutions

The last blockchain recordkeeping system solution, the tokenized type, is considered the most 'innovative' of current blockchain recordkeeping solutions because, "not only are records captured on-chain, but assets are represented and captured on-chain via linking them to an underlying cryptocurrency."[190] This blockchain system, presented as a recordkeeping solution, consists of both the technical and information governance contexts of recordkeeping systems. In this blockchain recordkeeping solution there are two distinct types of records that can be identified in this recordkeeping system: digital record type (i.e., smart contracts) and the tokenized asset. Ownership of the record in this system is complicated by the link between the physical ownership of an asset, such as land, a car, a diamond or anything really, to a token or cryptocurrency on the blockchain, as well as the digital record type on-chain, which transfers ownership of the asset between participants.

A Comparison of Records Ownership in Similar Digital Environments: Cloud Computing Storage

New technologies impact the way ownership is defined and interpreted in law. It is also generally acknowledged that the lawmaking process is too slow to keep up with new, and fast-moving technologies.[191] In the debate over information ownership, it can be argued that "information in digital form is generally not any kind of personal property, but instead is protected by a combination of the laws of intellectual property, confidence, and contract, among others. The composite effect of these laws gives customers a set of rights with respect to their information which is very similar in effect to owning physical property."[192] The relationships between the pace of new technologies, information ownership, and lawmaking are shifting, and as such, in order to understand the implications of blockchain record ownership, it would be beneficial to analyze the legal implications of other technologies or digital environments which

have impacted upon the issues of information ownership in the digital environment, such as cloud computing storage.

Cloud Computing Storage

The Sedona Conference identifies two major issues for ownership in the cloud: "(1) the location of the data, and (2) who is managing the data (be it one's own company or a third party.")[193] Similar to the distributed nature of blockchain recordkeeping systems, cloud storage environments face multi-tenancy issues in which the data of more than one client may be stored in the same physical or logical computing environment.[194] Depending on the type of blockchain recordkeeping system and its consensus mechanism (e.g., proof-of-work in the Bitcoin Blockchain), a record (be it the hash pointer to the storage off-chain, the smart contract, or the combination of token and smart contract) may be transacted with other types of records as well as the records of other parties in a block. Therefore, each record or transaction in a block in a blockchain recordkeeping system, may not be procedurally related to one another nor owned by the same party (i.e., when the blockchain recordkeeping system is governed by more than one organization). In this regard, cloud computing storage multi-tenancy is similar to the transactional level of a block, in which "multi-tenancy computing environments may require an understanding of how a computing environment uses metadata to track, manage, and maintain logical distinctions among comingled data to comply with legal obligations to access, preserve, collect, and understand commingled data."[195] Lemieux and Sporny have proposed a data model and syntax for instantiating the archival bond in blockchain recordkeeping systems,[196] which could be used to distinguish comingled records in the blocks of a blockchain recordkeeping system. Additionally, cloud computing storage faces similar issues and challenges as blockchain recordkeeping systems regarding storage location and jurisdictional issues. Records stored 'in the cloud,' "may also reside in more than one physical location… data sets may either be split into multiple locations or redundant storage locations."[197]

Another perspective recognizes that information which originates outside the cloud, already has an established ownership status before being placed into the cloud through intellectual property rights, copyright law, and service level agreements explicitly expressing that ownership remains with the customer.[198] This would be similar to blockchain recordkeeping

scenarios, in which the records are stored off-chain but the hash or hash pointer of the record is stored on-chain.

But what if the boundaries of blockchain record ownership could be logically delineated? NIST 800-146 is a standard which provides cloud computing recommendations and, "uses the concept of access boundaries to organize and characterize the different cloud deployment models"[199] in order to understand who controls resources in a cloud. Control is defined by NIST 800-146 as:

> "the ability to decide, with high confidence, who and what is allowed to access consumer data and programs, and the ability to perform actions (such as erasing data or disconnecting a network) with high confidence both that the actions have been taken and that no additional actions were taken that would subvert the consumer's intent (e.g., a consumer request to erase a data object should not be subverted by the silent generation of a copy)."[200]

Control and visibility, which is "the ability to monitor with high confidence, the status of a consumer's data and programs and how consumer data and programs are being accessed by others," are the two important capabilities identified by NIST 800-146, which consumers must give up to cloud storage providers.[201] Additionally, NIST 800-146 acknowledges that the extent to which control or visibility is relinquished depends on a number of factors, which includes the: "physical possession and the ability to configure (with high confidence) protective access boundary mechanisms[202] around a consumer's computing resources… by implementing a security perimeter around its important resources, an organization can achieve both a measure of control over the use of those resources and as a means for monitoring access to them… The various cloud deployment models in the NIST cloud definition[203] have implications for the locations of consumer-controlled security perimeters and hence for the level of control that consumers can exercise over resources that they entrust to a cloud."[204]

Additionally, Reed argues that accountability, in the form of transparency and verification, can enable cloud customers to achieve greater control over their information by enabling them to know how their information will be used in the cloud.[205] Accountability as described by Reed, as well as visibility from NIST 800-146, draws parallels to blockchain recordkeeping systems, in which participants of a blockchain network must entrust their records or data to the blockchain and the degree of control and custody over a record depends on the type

of blockchain recordkeeping system. Blockchain systems, whether they be public or private, are inherently designed to ensure 'visibility,' in which all transactions are transparent to participants of the network, thus providing accountability.[206]

Furthermore, Reed has argued "that national laws are incapable of producing appropriate regulation for cyberspace activities… And because cloud technologies operate with little or no reference to physical geography, they can only be properly regulated by a globally uniform set of rules. National law does not produce uniformity."[207] Reed proposes the need for external rules and guidelines which would then build a global representative structure to regulate the uses of derived information by cloud service providers.[208] This proposal for community development of guidelines or regulations for the cloud is similar to blockchain governance. Blockchain governance can be defined as:

> "the rules, practices and processes by which the blockchain network is directed and controlled…Permissioned blockchain networks are generally setup and run by an owner or consortium, which governs the blockchain network. Permissionless blockchain networks are often governed by blockchain network users, publishing nodes, and software developers. Each group has a level of control that affects the direction of the blockchain network's advancement."[209]

In permissioned blockchain recordkeeping system networks, control and ownership are easily determined by who governs the blockchain network. Control is defined by the network consortium through policies and regulations, while custody of the records is shared. However, in a permissionless network, a record owner/creator must expect to lose some degree of control and custody of a record.

Conclusion

This first foray into questions of ownership and custody is very preliminary. We admit that there remain many questions of ownership and custody to be explored in a blockchain recordkeeping future-world, including what happens when organizations generate personally identifiable information databases with an expectation that data subjects should ultimately become the owners and custodians of those records (i.e., obtain full data self-sovereignty). The ownership of information in a blockchain recordkeeping system, just like in cloud computing environments, must carefully be defined by policy, regulations and service level agreements

between organizations and interacting or participating parties. Depending on the type of blockchain recordkeeping system, some degree of control and custody of the record needs to be relinquished. Custody is distributed in all blockchain recordkeeping scenarios, unless the blockchain is only being used to maintain the integrity of the records, in which case, the blockchain functions as a digital signature database. Ultimately, ownership is controlled by the participant with the private key. Blockchain recordkeeping systems are redefining ownership and information governance into distributed ownership. This distributed model of information ownership gives all participants in the network transparency with respect to how their information is being accessed and the ability to track the provenance and custody of records, which in turn empowers participants to feel in control of their information.

Chapter 9: Blockchain Technology & Privacy

Introduction

In an ancient Jewish story, a man asked the famous rabbi Hillel to recite the entire Torah while standing on one foot. Hillel replied, "That which is hateful to you, do not to your neighbor: that is the whole Torah, the rest is commentary; now go study." So, too, is it with privacy: while it can be explained as a simple principle, it must be examined deeply to be understood and implemented. Warren and Brandeis offered one of the most succinct and still widely cited definitions of privacy when they described it in 1890 as "the right to be let alone,"[210] to control when and to what extent one will engage with others and share oneself. However, just as the Golden Rule was not enough for Hillel's questioner to live by the Torah – he was told to "go study" – Warren and Brandeis' simple formulation is not enough to make "privacy" meaningful.

Many subsequent definitions of privacy, particularly within law, have accepted Warren and Brandeis' fundamental concept, while grappling with its limits and implementation. The United States' Department of Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems, in its 1973 report on *Records, Computers, and the Rights of Citizens*,[211] cites Westin's seminal *Privacy and Freedom* in defining privacy: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[212] It is "the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public."[213] This definition touches on a number of different facets of privacy through the overarching value of informational privacy. "[E]ach ideal type of privacy contains an element of informational privacy – that is, a privacy interest exists in restricting access or controlling the use of information about that aspect of

human life." "Informational privacy" of course, is the realm of records; managing privacy in records, however, is no simple matter. As Pekka Hentonnen so adroitly states:

> People feel that their privacy is violated when information about them is passed inappropriately from one context or social sphere to another. This makes records and archives management a focal point of privacy issues, because its goal is to transfer information from one context, place, and point in time to other contexts, places, and points in time.[214] [215]

In other words, we feel that our privacy is violated when information about us flows into inappropriate contexts and/or to parties or situations where we do not trust how our information will be used. Legally, we rely primarily on what the American legal scholar Daniel Solove has termed "privacy self-management" to allow a person to signal that he/she/they trusts a particular party or system enough to permit them to control, process, and/or use their personal information. As Solove explains:

> the law provides people with a set of rights to enable them to make decisions about how to manage their data. These rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data. The goal of this bundle of rights is to provide people with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the disclosure of their information.[216]

However, making those rights meaningful in the digital era remains a thorny challenge. Privacy self-management hinges on consent; people exercise their right to make decisions about how to manage their data by granting or withholding consent. This regime is known as "notice-and-choice"; the party wishing to use the data provides notice regarding how the data will be used, and the data subject chooses whether or not to allow them access to make such use. However, the ultimate ways in which information systems use personal information are so complex that notice-and-choice is largely undermined by what privacy scholar Helen Nissenbaum terms "the *transparency paradox* […] If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. […] An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance."[217] In other words, it's one thing to click "I accept" to sharing my data with Facebook. It's another thing entirely to try to understand Facebook's

backend and myriad interrelationships with advertisers and other third parties to whom Facebook is now allowed to sell one's data.[4] For organizations which control and process personal information, meaningful consent from data subjects is central and must be documented.

Furthermore, our notions of records privacy arose when records were paper. When analogue records required effort to copy and accessing them required a trip to a clerk's office, most records remained private because it simply wasn't worth the work to access them - a concept known as "privacy through obscurity."[218] In the world of digital records, including blockchain records, obscurity is no longer a given. Instead, it requires conscious effort. Traditionally, tools such as access restrictions, redaction, and privacy through obscurity were enough to protect private information in records while allowing those records to be accessed and used appropriately and to remain in their context. However, the proliferation of digital records has necessitated new tools for managing privacy.

Blockchain and Privacy

Blockchain technology is sometimes posited as the privacy-protecting alternative for digital records. After all, blockchain technology leverages public key infrastructure and cryptography which can be powerful tools for protecting data privacy. Indeed, many blockchain use cases seek to capitalize on the potential of the blockchain to empower granular control of privacy on the part of data subjects. Blockchain technology, after all, produces an automatic, immutable audit chain. Theoretically, a blockchain system could allow users to see exactly who wants to see/use their data, when, and for what purpose, and then trace the use of that data. In other words, blockchain could help solve Nissenbaum's transparency paradox by allowing users to see every use of their data. Furthermore, although it is not automatically so, it is possible to build a blockchain that encrypts data in transactions, so that only parties who have permission can view the data, even though the transaction itself is stored in a verifiable, transparent way.

Indeed, the seeming privacy of pseudonymous transactions helped what is perhaps the most famous blockchain-based system, Bitcoin cryptocurrency, become a popular payment method for illegal goods and services.[219] However, researchers have shown that "using Bitcoin leaks public information that can be exploited to deanonymize Tor hidden service users"[220] – in

[4] Indeed, given the myriad of scandals, one wonders if anyone, even with the major data processing and controlling organizations, could truly map all of the third-party relationships and uses of users' personal information.

other words, Bitcoin leaked information could be used to reveal the real life identities of people who used an additional service for the specific purpose of providing anonymity. Indeed, as Henry at al. point out, "[m]ost blockchains are, at their core, massively distributed and publicly accessible databases."[221]

For this reason, some blockchain platforms and solutions are specifically designed to avoid recording any personal information – indeed, any transactional information – on the blockchain. Blockchains like Sovrin,[222] (Hyperledger Indy),[223] and British Columbia's OrgBook Project,[224] an implementation of Hyperledger Indy for a business registration use case, are purposefully designed to record only data schemas, or ontologies, on the blockchain. The public key of the issuer of the data can then be used to check "verifiable claims" about individuals, such as whether they are old enough to drive, have a job, or have a degree, without revealing specifics of their exact age, their employer or the grades they achieved in their studies. This is achieved by means of using "Decentralized Identifiers" (DIDs),[225] verified credentials and "Verifiable Claims."[226] These systems aim to follow a set of principles for the design of blockchains that support full data self-sovereignty and respect for privacy.[227]

Protecting the privacy of records, then, is not as simple as "use a blockchain." Instead, blockchain systems – like any other records system – require thoughtful design and a holistic understanding of the requirements of the system in order to adequately preserve privacy while providing needed access to records. For example, "privacy" encompasses a number of legal rights and obligations concerning personal information; those rights will vary depending upon jurisdiction, sector, and context.

Using blockchain technology does not obviate the need to understand the legal rights and obligations attached to the specific records within a particular system and to provide for appropriate controls on those records. Indeed, ensuring compliance can be even more difficult with a blockchain system in certain circumstances. From a jurisdictional perspective, when records fall within the scope of the European Union's General Data Protection Regulation (GDPR),[228] data subjects (people whose personal information is contained within the records) have a right to have that data erased. Technically, this is challenging if such data is stored on a blockchain, given that immutability is one of the greatest strengths of the blockchain. Although solutions – such as encrypting data subject to erasure and destroying the encryption key – have been proposed to "erase" data from the blockchain, the legal acceptability of such solutions

remains unknown.[229] As an example of how blockchain intersects with sectoral privacy laws, the Health Insurance Portability and Accountability Act,[230] a federal law concerning health data in the United States, "prohibits use of mathematically-derived pseudonyms because of potential re-identification of de-identified protected health information (PHI) […] effectively [making] blockchain non-HIPAA compliant."[231] Now then, this doesn't meant that blockchain systems cannot be designed for HIPAA-protected records; MIT Media Lab is developing a blockchain-based system for electronic health records called "MedRec."[232] Rather, it points to the importance of understanding the specific types of records within ones' systems and the need to design with the legal and ethical constraints, including privacy constraints, that apply to those records. Finally, the context of the records will determine the privacy and access requirements that must be taken into account in designing a blockchain records management system. For example, a law firm will likely have a number of extremely sensitive records which must, nonetheless, be accessed frequently by authorized personnel, but often only within the organization. The privacy demands on such a system would be quite different from those facing a hospital, which must be capable of interfacing with the records systems of a number of other health care organizations in order to provide care. Therefore, any organization which deals with sensitive or private information must consider jurisdiction, sector, and context in designing and implementing blockchain solutions.

Additionally, any party seeking to use blockchain solutions for records must account for the fact that blockchains are particularly immature as a records management technology. Fundamental records concepts, such as the archival bond and the preservation of context, are not natively instantiated in blockchain systems.[233] "Absent the archival bond, it is nearly impossible to understand the acts and facts of which the records are evidence; instantiating the archival bond is necessary to preserve records in their context."[234] Without such context, records can lose their value as assets to an organization and, moreover, as trustworthy evidence of agreements. For example, contracts secure important rights. However, whether a particular record embodies a contract, as opposed to simply negotiations, is a context-dependent question. Legally, a contract is only formed if an offer is accepted while the offer still stands; the offering party can withdraw his/her/their offer, and an acceptance will be meaningless. "Without the archival bond, it is impossible to know if a contract has formed, because it is impossible to reconstruct the relations of the records in such a way as to prove that an 'acceptance' was actually an acceptance, as

opposed to an attempt to accept a lapsed or revoked offer."[235] Without further design, such as instantiating the archival bond through metadata,[236] reconstructing the relationship between transactions and records on the blockchain is, at best, a time-consuming, manual activity. This is particularly problematic when one considers that the personal-information dossiers being built are used to support decision making concerning such serious matters as who gets a mortgage or whether an individual has consented to use of their data for medical research. Unless the archival bond and other indicators of records trustworthiness are somehow built in to our systems, blockchain recordkeeping could perpetuate the digital era's tendency to rely on data without evaluation or indicia of that data's reliability as evidence.

Similarly, longstanding records management tools, such as classification and access restrictions, will require thoughtful design to be integrated into blockchain systems. If encryption is the primary means of restricting access to blockchain records, then decryption is the primary means of providing access. However, decryption is a one-way street. There is not, currently, a decryption equivalent of "reading room only" access. Instead, once a record is decrypted for a party, that party has access to that record in plain text and can send it to all corners of the Earth, if so desired. The ability to redact blockchain records is still being developed; the technological tools to deal with data at a sub-record (sub-transaction) level are still nascent. Finally, the management of private keys themselves will prove a critical issue for both privacy and access moving forward. If encryption of transaction data is the norm, then accessioning and providing access to records will require not just the records, but individuals' private keys.

Conclusion

Blockchain technology has powerful affordances that could make it a privacy dream – or nightmare – for records management. End-to-end encryption and an automatic, immutable audit trail could be powerfully leveraged to ensure that personal information is only accessed and used when data subjects have consented. However, blockchains were not designed by records and information managers, and a number of the tools we traditionally rely upon to manage privacy – access restrictions, privacy through obscurity, classification – and to manage records' trustworthiness are not native to the blockchain. Blockchains can, theoretically, be designed in such a way as to enhance records' privacy, security, and accessibility – a privacy dream. Without significant thought and effort into privacy up front, however, a blockchain remains a distributed

database which anyone can read and to which anyone can write – the nightmare scenario that records professionals must help their organizations avoid.

Chapter 10: Blockchain Standards & Best Practices

Introduction

As an emerging technology, the process of standardization of blockchain technology is only just beginning. In fact, when standardization efforts first began to gather steam in late 2016 many cried foul, believing that it was too early for standardization efforts to take place. Now, however, we have the first *de facto* blockchain standard in the form of the NISTIR 8202[237] and many others are underway as well. This chapter does not propose to present a comprehensive list of standards initiatives – in a dynamic emerging technical ecosystem, it is almost impossible to capture all of these – but does outline some of the major standard-making initiatives likely to have impact.

International Standards Organization

The International Standards Organization (ISO), is an independent, non-governmental international organization that develops voluntary, consensus-based, market relevant international standards. The ISO Technical Committee 307 on Blockchains and Distributed Ledger Technology is the main technical committee setting the future course of standardization for this technology. TC 307 was established in 2016 and has its secretariat in Australia. The TC currently has 41 participating members, 11 observing members, 7 working groups, and 11 standards under development.[238] These are:

- ISO/NP TS 23635. Blockchain and distributed ledger technologies -- Guidelines for governance

- ISO/NP TR 23578. Blockchain and distributed ledger technologies -- Discovery issues related to interoperability
- ISO/NP TR 23576. Blockchain and distributed ledger technologies -- Security management of digital asset custodians
- ISO/DTR 23455. Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
- ISO/AWI TS 23259. Blockchain and distributed ledger technologies -- Legally binding smart contracts
- ISO/AWI TS 23258. Blockchain and distributed ledger technologies -- Taxonomy and Ontology
- ISO/CD 23257. Blockchain and distributed ledger technologies -- Reference architecture
- ISO/NP TR 23246. Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies
- ISO/NP TR 23245. Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities
- ISO/NP TR 23244. Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations
- ISO/CD 22739. Blockchain and distributed ledger technologies – Terminology

None of these standards have been finalized yet, but three of them – ISO/CD 22739 (Terminology), ISO/CD 23257 (Reference Architecture), and ISO/DTR 23455 (Interactions between Smart Contracts and Blockchains) have reached committee stage. The first of these standards expected to be finalized is ISO//CD 22739 on terminology, anticipated in 2020.

Of note to records and information professionals is that ISO TC46/SC 11, Archives and Records Management has recently proposed the formation of a new work item relating to the application of blockchain technology to records: issues and considerations. At time of writing, the proposal was still out for ballot and it has not yet been approved.[239]

CEN-CENELEC

CEN and CENELEC are business catalysts in Europe with a mission to remove trade barriers for European industry and consumers in order to foster the European economy in global trading, the welfare of European citizens, and the environment. Through their services they provide platforms for the development of European Standards and other technical specifications.

CEN-CENELAC have created a new Focus Group on Blockchains and Distributed Ledger Technologies.

The objective of the Focus Group is to identify potential specific European Standard-making needs, in particular those needed to support the ISO TC307 Standardization efforts in order to support Europe's digital transformation. The Focus Group aims to support the needs of European businesses, especially small-to-medium sized enterprises and to encourage greater European participation in TC307. The Focus Group has initiated and is active in participating in the work of ISO TC307, particularly in reference architecture, security and privacy, identity, smart contracts, and governance.[240]

The identification of specific requirements has been formalized in the CEN-CENELEC White Paper 'Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies,' released in October 2018.[241] The White Paper provides 26 recommendations, addresses topics as sustainable development, digital identity, privacy and data protection, and highlights specific European use cases.

International Telecommunications Union (ITU)

The ITU is the United Nations specialized agency for information and communication technologies. Its focus group on the application of distributed ledger technologies was established in May 2017 and is chaired by Switzerland. The aim of the focus group is threefold:

- to identify and analyze DLT-based applications and services
- to draw up best practices and guidance which support the implementation of DLT applications and services on a global scale
- to propose a way forward for DLT-related standardization work in ITU study groups.[242]

The Focus Group is expected to complete its work by September 2019. One of the group's priorities is to deliver an assessment framework to support efforts to understand the strengths and weaknesses of DLT platforms in different use cases. The group is also developing a high-level DLT reference architecture.[243]

World Wide Web Consortium (W3C) and the Decentralized Identity Foundation

There are also emerging standards in the area of decentralized identity, or Self-Sovereign Identity (SSI). Decentralized identity management is a growing area with a variety of use cases, which rely on any exchange of credentials, attestations (e.g. bank account, university degree) or attributes or "verifiable claims" (e.g. name, over 18) between untrusted entities following privacy and security-by-design principles.[244] Platform vendors, such as Microsoft, uPort, and Sovrin, have recognized the need for interoperability and now work together in dedicated working groups in the W3C and in the Decentralized Identity Foundation (DIF) on the general architecture of decentralized identities and to develop standards that enable interoperability between different implementations.[245]

The following represent the standards of greatest interest:

- W3C Community Group - Decentralized Identifier (DID): "Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs that are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority."[246]
- W3C Working Group - Verifiable Claims: "machine-readable statement made by an entity that is cryptographically authentic (non-repudiable)."[247]
- DIF - DID Auth: "The term DID Auth has been used in different ways and is currently not well-defined. We define DID Auth as a ceremony where an *identity owner*, with the help of various components such as web browsers, mobile devices, and other agents, proves to a *relying party* that they are in control of a DID. This means demonstrating control of the DID using the mechanism specified in the DID Document's 'authentication' object. This could take place using a number of different data formats, protocols, and flows. DID Auth includes the ability to establish mutually authenticated communication channels and to authenticate to web sites and applications."[248]

National Standards

As is typical, most national standards bodies will introduce national standards that conform to or influence the ISO standards mentioned above. Some countries are working to set their own national standards. China is reputedly one of these countries. It is aiming to introduce

basic standards, business and application standards, process and method standards, credible and interoperable standards, and information security standards.[249]

In the US, the National Institute of Standards and Technology (NIST), which was founded in 1901 and is now part of the U.S. Department of Commerce, has released NIST Interagency/Internal Report (NISTIR) – 8202 – which "provides a high-level technical overview of blockchain technology" that discusses its application to cryptocurrency in depth, but also shows its broader applications. "The purpose is to help readers understand how blockchain technology works," so that they can be applied to technology problems. Though not a standard *per se*, in the absence of other standards, this report is to some degree setting the pace for other standards, such as those being developed by the ISO.[250]

Consortium/Foundations/Society Standardization Efforts

In 2017, the capabilities of the Ethereum blockchain unleashed a virtual tsunami of Initial Coin Offerings (ICOs). Initially non-standardized, the Ethereum community quickly realized the value of interoperability and several token standards were introduced. The first of these was Ethereum Request for Comment (ERC)-20. "ERCs (Ethereum Request for Comments) are technical documents used by smart contract developers at Ethereum. They define a set of rules required to implement tokens for the Ethereum ecosystem. These documents are usually created by developers, and they include information about protocol specifications and contract descriptions. Before becoming a standard, an ERC must be revised, commented and accepted by the community through an EIP (Ethereum Improvement Proposal."[251]

The ERC20 Token Standard allows the implementation of a standard API to ensure the interoperability between tokens. It offers basic functionalities to transfer tokens, obtain account balances, get the total supply of tokens, and allow token approvals.[252] This is the standard that has been used in the vast majority of ICOs that were issued in 2018. Another very popular token standard is ERC-721, the Non-Fungible Token Standard. This token came into being and is most associated with the now infamous CryptoKitties.[253]

More recently, the Ethereum community is differentiating between utility tokens and security tokens and proposing a new Security Token Standard.[254] As explained by the Security Token Council:

> Utility tokens represent access to a network, and your token purchase represents the ability to buy goods or services from that network—kind of like purchasing a game token being used to play an arcade machine. Utility tokens give you that same type of access but just to a product or service. On the other hand, security tokens represent complete or fractional ownership in an asset (such as shares in a company, a real-estate asset, artwork, etc.). Having a stake in a company, real estate, or intellectual property can all be represented by security tokens. Security tokens offer the benefit of bringing significant transparency over traditional paper shares through the use of the blockchain and its associated public ledger. Security token structure, distribution, or changes that could affect investors are now accessible to all via the blockchain. Security tokens and the digitalised assets they represent ownership will form the backbone of finance 3.0 driving innovation, adoption and accessibility across the financial sector.[255]

The Ethereum Enterprise Alliance (EEA) is a member-driven organization that aims to develop a set of open-source, standards-based blockchain specifications that can be trusted and utilized globally. The two most relevant standards are: 1) The Enterprise Ethereum Architecture Stack (EEAS) and Enterprise Ethereum Client Specification.

EEAS is a conceptual framework that characterizes and standardizes components from the Ethereum ecosystem.[256] The EEAS details functions of an Enterprise Ethereum blockchain client without regard to its underlying software code, application programming interfaces (APIs), and communications protocols. The purpose of the EEAS is to guide the development of the EEA's coming Enterprise Ethereum standards-based specification. Both the concepts and technologies from the public Ethereum community and the EEA Technical Steering Committee (TSC) will be integrated into the EEA's Enterprise Ethereum specification. This document specifies Enterprise Ethereum, a set of extensions to the public Ethereum blockchain to support the scalability, security, and privacy demands of private, permissioned, i.e., enterprise deployments of the Ethereum blockchain.[257]

Other foundations and consortia are developing specifications and standards for their platforms, including R3 (Corda)[258]and Linux (Hyperledger).[259]

In terms of Societies, IEEE, billed as "The world's largest technical professional organization for the advancement of technology," has a number of initiatives underway related to

development of standards for the application of blockchain technology in healthcare.[260] These include:

- IEEE Initiative to Build Consensus on Optimizing Clinical Trials and Enhancing Patient Safety with Blockchain
- IEEE Releases Findings from First Detailed Study of Blockchain Adoption in the Pharmaceutical Enterprise
- IEEE Driving Collaboration on Advancing Blockchain Adoption Within the Pharmaceutical Industry
- IEEE Launches World's First Virtual Blockchain Workshop Dedicated to Advancing HealthTech for Humanity™

Sector-Specific Best Practice Standards

In many sectors, organizations that focus on information and technology and which develop best practices and guidance for professionals in their industries are exploring the application of blockchain technology. These efforts may lead to standards and best practices in a similar manner to the way that ARMA's standardization efforts have often led to ANSI standards and fed into the international standard making process. As an example, in the healthcare sector in which there is a growing focus on the application of blockchain, and thus, increasing interest in blockchain standards for healthcare, one of the organizations that is involved in considering blockchain's application in the health sector, and standardized approaches, is HIMMS. HIMMS is a global not-for-profit organization focused on health information and technology headquartered in Chicago.[261] The HIMMS Blockchain Workgroup has developed resources aimed at communicating best practices for healthcare blockchain, which may provide helpful guidance particularly to those working with Ethereum-based solutions.[262] The Research Data Alliance also has recently established a "Working Group on Blockchains Application in Healthcare" which will explore blockchain "as a technological advanced solution for securing data sharing among clinical institutions and individuals."[263] As indicated in its charter, the aim of the working group is:

- "to analyse and compare usages of the blockchain in healthcare, implementations of blockchain architectures, associated legal and socio-economic impacts and perspectives
- to assess the potential of blockchain-based self-enacting smart contracts in handling consent and data permission systems minimising transaction costs
- to assess whether and how the blockchain can ensure compliance with advanced data protection requirements (such as those defined by the EU General Data Protection Regulation – GDPR), yet making it happen seamlessly and efficiently, at scale."[264]

  Noting that, "[w]ithin 18 months of activity, starting from concrete examples, the group will draw a set of use-cases, thus feeding a working draft and concluding on good practices, technical recommendations, and guidance to healthcare professionals interested in having recourse to blockchain solutions." Development such as those in healthcare, indicate that there are likely to be a range of emerging sector-specific best practice standards.[265]

Conclusion

Many standards initiatives are still in the early stages, and new initiatives from a range of national and global standard making bodies as well as blockchain-specific foundations and consortia are emerging. Globally, the blockchain world has come to recognize the value of standards to promote interoperability and growth of the technology and its application, but the road ahead is still very much under construction.

End Notes

[1] "Building Trust in Government: Exploring the Potential of Blockchains," Executive Report (Somers, NY: IBM Institute for Business Value, 2017), https://www.ibm.com/downloads/cas/WJNPLNGZ.
[2] Lester Coleman, "Georgia Expands Project to Secure Land Titles on the Bitcoin Blockchain," *CCN* (blog), July 2, 2017, https://www.ccn.com/republic-of-georgia-expands-project-to-secure-land-titles-on-the-bitcoin-blockchain.
[3] "The Land Registry in the Blockchain - Testbed" (Kayros Future, March 2017), https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf.
[4] "Blockchain Land Registry Tech Gets Test in Brazil - CoinDesk," *Coindesk* (blog), April 5, 2017, https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil.
[5] Records in the Chain Project, "Report on use of blockchain technology in medical recordkeeping in Estonia," 2017, unpublished report.
[6] John Collomosse et al., "ARCHANGEL: Trusted Archives of Digital Public Documents," *ArXiv:1804.08342 [Cs]*, April 23, 2018, http://arxiv.org/abs/1804.08342.
[7] See National Archives and Records Administration. "Blockchain White Paper," February, 2019, https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf and Alan Pelz-Sharpe, Rob Begley, and Jon Bushell, "Records Management & Blockchain," Deep Analysis, August, 2018, https://www.linkedin.com/pulse/free-report-records-management-blockchain-rob-begley.
[8] Not everyone agrees with this proposition. For a range of different definitions of blockchain, see InterPARES Trust Terminology Project, "Key Blockchain Terms and Definitions," 2017. http://arstweb.clayton.edu/interlex/blockchain/. And, for a discussion surrounding some of the controversies associated with defining blockchain terminology, see Walch, Angela. "The path of the blockchain lexicon (and the law)." *Rev. Banking & Fin. L.* 36 (2016): 713.
[9] John Locke, "Essays on the Law of Nature, edited and translated by W. von Leyden." (1954), cited in Geoffrey Yeo, "Trust and Context in Cyberspace," *Archives and Records* 34, no. 2 (October 1, 2013): 214–34, https://doi.org/10.1080/23257962.2013.825207.
[10] Luciana Duranti and Corinne Rogers, "Trust in Records and Data Online," in *Integrity in Government through Records Management : Essays in Honour of Anne Thurston*, 2nd ed. (New York, NY: Routledge, 2016), 203–14.
[11]Barometer, Edelman Trust, "Annual global survey." (2017). Retrieved from ttps://www.edelman.com/trust-barometer/; Paul Vigna and Michael J. Casey, *The Truth Machine: The Blockchain and the Future of Everything* (New York: St. Martin's Press, 2018).
[12] With respect to the professional role of the archivist, see Heather Macneil, "Trust and professional identity: narratives, counter-narratives and lingering ambiguities," *Archival Science* 11 (2011): 175–92, http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/s10502-011-9150-5.
[13] Chenney et al.
[14] Collomosse et al., "ARCHANGEL."
[15] This is not a new problem: Jean Mabillon wrote De Re Diplomatica, which gave birth to the modern discipline of Diplomatics, to defend the authenticity of contested charters of the

Merovingian and Carolingian periods [See, Randolph C. Head, "Documents, Archives, and Proof around 1700," The Historical Journal 56, no. 4 (2013): 909-930]. However, the lack of fixity of documents created in digital form renders the problem more severe [See, Fred Cohen, "A TALE OF TWO TRACES – DIPLOMATICS AND FORENSICS," vol. AICT-462, 2015, 3–27, https://doi.org/10.1007/978-3-319-24123-4_1.

[16] See, for example, Preedy Kasireddy, "EL15: 'What do we mean by blockchains are trustless'?", *Medium* (Feb. 3, 2018) and Alessandro Mario Lagana Toschi, "Decentralized Data: 'Why Blockchain is meaningless and Trustless is everything'." *Hackernoon,* July 10, 2018.

[17] Ibid.

[18] It should be noted that blockchain systems and the larger super-class of distributed ledger systems can vary significantly in their design. Moreover, as this is an emerging class of technologies, design features are far from stable even in the larger public blockchains, such as Bitcoin and Ethereum, which have now been in existence since 2008 and 2015 respectively. This makes generalization and stable assertion challenging. We have tried to address important differences whenever necessary, and to avoid confusing the reader with variations in the design and configuration of these systems that are not immediately relevant to the points under discussion.

[19] Arvind Narayanan et al., "Bitcoin and Cryptocurrency Technologies," *Princeton University Press*, 2016, 308.

[20] Victoria L. Lemieux, "Blockchain Recordkeeping: A Swot Analysis," *Information Management; Overland Park* 51, no. 6 (December 2017): 20-22,24,26-27.

[21] Narayanan et al., "Bitcoin and Cryptocurrency Technologies."

[22] The Bitcoin network is estimated to have approximately 10,000 nodes [See, https://bitnodes.earn.com], while the Ethereum network is estimated to have approximately 13,000 nodes [See, https://www.ethernodes.org/network/1]. On a public blockchain network the number of nodes cannot be identified with precision, since nodes may join and exit the network freely at any time. In general, the higher the number of nodes, the more secure the network since more copies of the ledger exist.

[23] See, Serguei Popov, "The tangle." *cit. on* (2016): 131 and https://iota.stackexchange.com/questions/782/full-node-vs-permanode

[24] On the question of governance of blockchains see, Angela Walch, "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk," *New York University Journal of Legislation and Public Policy* 18 (2015): 837–94.

[25] P. Baran, "On Distributed Communications Networks," *IEEE Transactions on Communications Systems* 12, no. 1 (March 1964): 1–9, https://doi.org/10.1109/TCOM.1964.1088883.

[26] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (www.bitcoin.org, 2008), https://bitcoin.org/bitcoin.pdf.

[27] For a definition of asymmetric cryptography, see "InterPARES Trust Terminology: Blockchain Terminology," 2017, http://arstweb.clayton.edu/interlex/blockchain/.

[28] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

[29] Nakamoto.

[30] Arati Baliga, "Understanding Blockchain Consensus Models" (Persistent, 2017), https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf.

[31] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of Consensus Protocols on Blockchain Applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017, 1–5, https://doi.org/10.1109/ICACCS.2017.8014672.
[32] Alex Moscov, "The Byzantine General's Problem," *CoinCentral* April 11, 2018, https://coincentral.com/byzantine-generals-problem/.
[33] Kasireddy, 2018. *Supra.*
[34] See, for example, Amy Castor, "A Short Guide to Bitcoin Forks," *CoinDesk*, Mar. 27, 2018.
[35] "InterPARES Trust Terminology: Blockchain Terminology."
[36] Ibid.
[37] Baliga, "Understanding Blockchain Consensus Models."
[38] K. J. O'Dwyer and D. Malone, "Bitcoin Mining and Its Energy Footprint," in *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 2014, 280–85, https://doi.org/10.1049/cp.2014.0699.
[39] Pelz-Sharpe, Begley, and Bushell, "Records Management & Blockchain," *Supra.*
[40] For example, in January 2019, Ethereum Core suffered a 51% attack; see, Gareth Jenkinson, "Ethereum Classic 51% Attack — The Reality of Proof-of-Work," *Coindesk* January 10, 2019, https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.
[41] See, https://www.jpmorgan.com/global/Quorum.
[42] See, https://ripple.com/
[43] Narayanan et al., "Bitcoin and Cryptocurrency Technologies."
[44] Ittay Eyal and Emin Gün Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," *Communications of the ACM* 61, no. 7 (June 2018): 95–102, htts://doi.org/10.1145/3212998.
[45] Walch, "The Bitcoin Blockchain as Financial Market Infrastructure."
[46] InterPARES Trust, "Terminology Project: Key Blockchain Terms and Definitions" (2017). *Supra*.
[47] Ibid and Iuon-Chang Lin and Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges," *International Journal of Network Security* 19, no. 5 (September 2017): 653–59, https://doi.org/10.6633/IJNS.201709.19(5).01.
[48] Lemieux, 2017. *Supra.*
[49] "InterPARES Trust Terminology: Blockchain Terminology."
[50] Nick Szabo, "The Idea of Smart Contracts," Nick Szabo's Papers and Concise Tutorials, 1997, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.
[51] "InterPARES Trust Terminology: Blockchain Terminology."
[52] "InterPARES Trust Terminology: Blockchain Terminology."
[53] Victoria L. Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework," *IEEE Future Technologies Conference*, 2017, https://www.researchgate.net/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework.
[54] "InterPARES Trust Terminology: Blockchain Terminology."
[55] "InterPARES Trust Terminology: Blockchain Terminology."
[56] "InterPARES Trust Terminology: Blockchain Terminology."
[57] Richard Pearce-Moses, *A Glossary of Archival and Records Terminology*, Archival Fundamentals Series. II (Chicago: Society of American Archivists, 2005).

[58] "ISO 15489-1:2016 - Information and Documentation -- Records Management -- Part 1: Concepts and Principles" (International Organization for Standardization (ISO), 2016), 15, http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/25/62542.html.
[59] Vitalik Buterin, "Ethereum White Paper - A Next-Generation Smart Contract and Decentralized Application Platform," GitHub, March 19, 2019, https://github.com/ethereum/wiki.
[60] See, Anduck. "Blockchain in Words," www.BitcoinStrings.com (2019) and Andrew Sward, Ivy Vecna, and Forrest Stonedahl. "Data Insertion in Bitcoin's Blockchain." *Ledger* 3 (April 3, 2018). https://doi.org/10.5195/LEDGER.2018.101.
[61] Anduck, "Blockchain in Words" op cit.
[62] Sward, 2018, op cit.
[63] Antonopoulos, cited in Sward et al., op cit.
[64] Darra Hofman et al., "'The Margin between the Edge of the World and Infinite Possibility': Blockchain, GDPR and Information Governance," *Records Management Journal* 29, no. 1/2 (February 13, 2019): 240–57, https://doi.org/10.1108/RMJ-12-2018-0045.
[65] Dmitry Kochin, "Where Do Decentralized Applications Store Their Data?," GitHub, March 16, 2019, https://github.com/TiesNetwork/ties-docs.
[66] Sward, 21018 op cit; See also, Victoria Lemieux, Daniel Flores, and Claudia Lacombe, "Real Estate Transaction Recording in the Blockchain in Brazil," *Records in the "Chain" Project Publications* (blog), 2018, https://blogs.ubc.ca/recordsinthechain/2018/01/26/real-estate-transaction-recording-in-the-blockchain-in-brazil/.
[67] Victoria L Lemieux, "Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective," *European Property Law Journal* 6, no. 3 (2017): 392–440.
[68] Andreas Abraham, "Whitepaper about the Concept of Self-Sovereign Identity Including Its Potential," n.d., 39.
[69] Lemieux, 2017. *Supra.*
[70] Kochin, "Where Do Decentralized Applications Store Their Data?"
[71] Kochin.
[72] Kochin. It is not known if the design of BigChain DB has addressed this issue since Kochin wrote his technical analysis in 2017. Thus, readers should be warned that this risk may be mitigated and should make their own investigations as to the level of trust and fault tolerance among nodes.
[73] "InterPARES Trust - Terminology," accessed March 19, 2019, https://interparestrust.org/terminology.
[74] See, for example, Luciana Duranti, "Preservation in the Cloud: Towards an International Framework for a Balance of Trust and Trustworthiness," in *APA/C-DAC International Conference on Digital Preservation & Development of Trusted Digital Repositories* (New Delhi, India: Centre for Development of Advanced Computing, 2014), 23–38.
[75] Angela Walch, "In Code (Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains," 2018.
[76] Luciana Duranti, *Diplomatics: New Uses for an Old Science* (Lanham, Md: Scarecrow Press, 1998).
[77] Luciana Duranti and Kenneth Thibodeau, "The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES*," *Archival Science; Dordrecht*, 2006, http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/s10502-006-9021-7.

[78] For a discussion of how the concept of record may apply to both individual objects and aggregations of objects, see Geoffrey Yeo, "Concepts of Record (1): Evidence, Information, and Persistent Representations," *The American Archivist* 70, no. 2 (2007): 315–43.
[79] For a detailed overview of digital signature forms, see Hrvoje Brzica, Boris Herceg, and Hrvoje Stan, "Long-Term Preservation of Validity of Electronically Signed Records," *INFuture 2013: Information Governance*, 2013, 147–58.
[80] Glenn Dingwall, "Life Cycle and Continuum: A View of Recordkeeping Models from the Postwar Era," in *Currents in Archival Thinking*, 1st ed. (Santa Barbara, Calif: ABC-CLIO, LLC, 2010).
[81] Adam Stapleton, "Continuum in Context: Post-Eighteenth Century Archival Theory and the Records Continuum Model," *ARCHIFACTS* 1 (2005): 21–46.
[82] Stapleton.
[83] Sue McKemmish, "Placing Records Continuum Theory and Practice," *Archives & Museum Informatics* 1 (2001): 333–59, http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/BF02438901.
[84] McKemmish.
[85] McKemmish.
[86] Viviane Frings-Hessami, "Looking at the Khmer Rouge Archives through the Lens of the Records Continuum Model: Towards an Appropriated Archive Continuum Model," *Information Research* 22, no. 4 (December 15, 2017): 1–14.
[87] Stapleton, "Continuum in Context: Post-Eighteenth Century Archival Theory and the Records Continuum Model."
[88] McKemmish, "Placing Records Continuum Theory and Practice."
[89] McKemmish.
[90] Frings-Hessami, "Looking at the Khmer Rouge Archives through the Lens of the Records Continuum Model: Towards an Appropriated Archive Continuum Model."
[91] Frank Upward, "Modelling the Continuum as Paradigm Shift in Recordkeeping and Archiving Processes, and beyond - a Personal Reflection," *Records Management Journal* 10, no. 3 (December 2000): 115–39, https://doi.org/10.1108/EUM0000000007259.
[92] "Generally Accepted Recordkeeping Principles" (ARMA International, 2009), https://www.armavi.org/docs/garp.pdf.
[93] LLC. EDRM, *How the Information Governance Reference Model (IGRM) Complements ARMA International's Generally Accepted Recordkeeping Principles (GARP®)* (EDRM, 2011), https://books.google.ca/books?id=h6wWrgEACAAJ.
[94] "Defensible Disposition: Real-World Strategies for Actually Pushing the Delete Button" (Los Altos, CA: Contoural, Inc., 2014), http://www.armaboston.org/images.html?file_id=t2tv5Y%2Fy%2BeI%3D.
[95] "Generally Accepted Recordkeeping Principles."
[96] "Defensible Disposition: Real-World Strategies for Actually Pushing the Delete Button."
[97] "Defensible Disposition: Real-World Strategies for Actually Pushing the Delete Button."
[98] Frank Fazzio, "Blockchain for Information Governance: Vetting a Solution," *Zasio* (blog), April 4, 2018, https://www.zasio.com/blockchain-for-information-governance-vetting-a-solution/.
[99] Stuart Rennie, "Dispelling Myths About Records Retention in Canada," *Canadian RIM, an ARMA Canada Publication* 1, no. 1 (Spring 2016), https://www.armacanada.org/index.php/resources-knowledge/documents2/canadian-rim/276-dispelling-myths-about-records-retention-in-canada/file.

[100] R Thomas Howell Jr and Rae N. Cogar, "Developing And Implementing A Record Retention Program," *Practical Lawyer* 50, no. 6 (2004): 21.
[101] Rennie, "Dispelling Myths About Records Retention in Canada."
[102] Rennie.
[103] Victoria L. Lemieux and Manu Sporny, "Preserving the Archival Bond in Distributed Ledgers: A Data Model and Syntax," in *Proceedings of the 26th International Conference on World Wide Web Companion - WWW '17 Companion* (the 26th International Conference, Perth, Australia: ACM Press, 2017), 1437–43, https://doi.org/10.1145/3041021.3053896.
[104] Anne Glover, Crystal O'Donnell, and David N Sharpe, "The Sedona Canada Principles Addressing Electronic Discovery, Second Edition" (The Sedona Conference, 2015), https://www.canlii.org/en/info/sedonacanada/2015principles_en.pdf.
[105] Gurmeet Singh Manku, Arvind Jain, and Anish Das Sarma, "Detecting Near-Duplicates for Web Crawling," in *Proceedings of the 16th International Conference on World Wide Web*, WWW '07 (New York, NY, USA: ACM, 2007), 141–150, https://doi.org/10.1145/1242572.1242592.
[106] Robert F. Smallwood, ed., *Information Governance: Concepts, Strategies and Best Practices* (Hoboken, NJ, USA: John Wiley & Sons, Inc., 2015), https://doi.org/10.1002/9781118433829.
[107] Publications Office of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)," Website, April 27, 2016, https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en.
[108] Union.
[109] Claudio Lima, "Blockchain-GDPR Privacy by Design: How Decentralized Blockchain Internet Will Comply with GDPR Data Privacy" (IEEE Blockchain Standards, 2018), https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf.
[110] Winston Maxwell and John Salmon, "A Guide to Blockchain and Data Protection" (Hogan Lovells, 2017), https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf.
[111] Steven Hernandez, and Adam Gordon, *The Official (ISC)2 Guide to the SSCP CBK*, 4th Edition (2016: Sybex), accessed March 20, 2019, https://learning.oreilly.com/library/view/the-official-isc2/9781119278634/.
[112] Lima, "Blockchain-GDPR Privacy by Design: How Decentralized Blockchain Internet Will Comply with GDPR Data Privacy."
[113] The Sedona Conference, "THE SEDONA CONFERENCE COMMENTARY ON INFORMATION GOVERNANCE," *The Sedona Conference Journal* 15 (2014): 125–66.
[114] David O. Stephens, "What Is Past Is Prologue: What History Reveals About the Future of RIM," *Information Management* 51, no. 5 (October 2017): 34–38.
[115] Smallwood, *Information Governance*.
[116] Smallwood.
[117] Randolph A. Kahn, "Why Destruction of Information Is So Difficult and So Essential: The Case for Defensible Disposal," *American Bar Association - Business Law Today*, 2018, http://go.galegroup.com.ezproxy.library.ubc.ca/ps/i.do?p=LT&u=ubcolumbia&id=GALE%7CA576220627&v=2.1&it=r&sid=summon.

[118] The Sedona Conference, "The Sedona Conference Principles and Commentary on Defensible Disposition - Public Comment Version" (The Sedona Conference, 2018), https://thesedonaconference.org/sites/default/files/publications/Principles%20and%20Commentary%20on%20Defensible%20Disposition_0.pdf.
[119] "The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production," *Sedona Conference Journal* 19 (2018).
[120] The Sedona Conference, "The Sedona Conference Principles and Commentary on Defensible Disposition - Public Comment Version."
[121] Smallwood, *Information Governance*.
[122] The Sedona Conference, "The Sedona Conference Principles and Commentary on Defensible Disposition - Public Comment Version."
[123] Smallwood, *Information Governance*.
[124] The Sedona Conference, "The Sedona Conference Principles and Commentary on Defensible Disposition - Public Comment Version."
[125] Maura R. Grossman and Gordon V. Cormack, "Technology-Assisted Review in e-Discovery Can Be More Effective and More Efficient than Exhaustive Manual Review," *Richmond Journal of Law & Technology (Online)* 17, no. 3 (2011): 1.
[126] Grossman and Cormack.
[127] Collomosse et al., "ARCHANGEL."
[128] Vladimir Bralić, Magdalena Kuleš, and Hrvoje Stančić, "A Model for Long-Term Preservation of Digital Signature Validity: TrustChain," *INFuture2017: Integrating ICT in Society*, 2017, https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain.
[129] Bralić, Kuleš, and Stančić.
[130] V. L. Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on Their Implications for the Future of Archival Preservation," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017, 2271–78, https://doi.org/10.1109/BigData.2017.8258180.
[131] National Archives and Records Administration, "Blockchain White Paper," supra.
[132] Brandon Rodenburg and Stephen P. Pappas, "Blockchain and Quantum Computing" (Princeton, NJ: The MITRE Corporation., 2017), https://pdfs.semanticscholar.org/2284/08bf3c13f0d579f21a5d999e7d4967104c09.pdf.
[133] Rodenburg and Pappas.
[134] Brian Deery, "The Blockchain & Future Of Business Records," *Blockchain News* (blog), May 7, 2016, https://www.the-blockchain.com/2016/05/07/blockchain-future-business-records-brian-deery-chief-scientist-factom-inc/.
[135] Cassie Findlay, "Decentralised and Inviolate: The Blockchain and Its Uses for Digital Archives," *Recordkeeping Roundtable* (blog), January 23, 2015, https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.
[136] Victoria Louise Lemieux, "Trusting Records: Is Blockchain Technology the Answer?," *Records Management Journal* 26, no. 2 (July 18, 2016): 110–39, https://doi.org/10.1108/RMJ-12-2015-0042.
[137] Heather MacNeil, *Trusting Records: Legal, Historical and Diplomatic Perspectives* (Springer Science & Business Media, 2000).
[138] Duranti, *Diplomatics*.

[139] Caroline Williams Director, "Diplomatic Attitudes: From Mabillon to Metadata," *Journal of the Society of Archivists* 26, no. 1 (April 1, 2005): 1–24, https://doi.org/10.1080/00039810500047417.
[140] Duranti, *Diplomatics*.
[141] Duranti.
[142] MacNeil, *Trusting Records: Legal, Historical and Diplomatic Perspectives*.
[143] Lemieux, "(PDF) Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems."
[144] InterPARES 2, dictionary/glossary approved August 19 2011, cited in ICA Multilingual Archival Terminology database. Retrieved from http://www.ciscra.org/mat/mat/term/307
[145] Luciana Duranti and Randy Preston, "International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records" (Associazione Nazionale Archivistica Italiana, 2008), http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf.
[146] See, Randolph C. Head, "Documents, Archives, and Proof around 1700," *The Historical Journal* 56, no. 4 (2013): 909-930, who explains the concept of *ius archivi* as follows: "Equally influential was the practice of Roman enshrinement of the *tabellio*, the forerunner of the notary. The late Roman *tabellio* was a government official who received, authenticated and kept records in a public archive, the *tabullarium*. Records produced from the *tabullarium* during litigation enjoyed special authority as evidence, which later came to be known as *publica fides*. Such documents, known as *instrumenta fides* or *instrumenta publica*, were still open to challenge in court, but the party challenging them bore the burden of proving they were flawed." (p. 914).
[147] For more on the archival bond, see Lemieux and Sporny, "Preserving the Archival Bond in Distributed Ledgers." The definition of integrity derives from Glossary of Records and Information Management Terms, 3rd ed. (ARMA International, 2007), cited in the ICA Multilingual Archival Terminology Database. Supra.
[148] See, for example, the State of Arizona's AZ HB2417, passed on March 29, 2017 (Retrieved from: https://legiscan.com/AZ/text/HB2417/id/1588180/Arizona-2017-HB2417-Chaptered.html), which reads: "SMART CONTRACTS MAY EXIST IN COMMERCE. A CONTRACT RELATING TO A TRANSACTION MAY NOT BE DENIED LEGAL EFFECT, VALIDITY OR ENFORCEABILITY SOLELY BECAUSE THAT CONTRACT CONTAINS A SMART CONTRACT TERM (capitalization in cited text)." (Chp. 44-7061, S. C.).
[149] W3C, "Verifiable Claims Working Group Charter," https://www.w3.org/2017/vc/charter.html (2019)
[150] See, for example, Ken Chasse, "Electronic Records as Evidence: From 'Paper-Originals' to 'System-Integrity'," *Joint Open Forum on Standardization Enablement in Electronic Commerce (JOFSEEC) March* (2001): 5-6. The importance of the operation of the system of recording has been ensconced in various standards including Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005, in particular s. 5.2.2, and the International Records Management Standard, ISO 15489: 2016-1.
[151] On this point, see Cohen, "A TALE OF TWO TRACES – DIPLOMATICS AND FORENSICS."
[152] Ibid. p.12.
[153] Lemieux and Sporny, 2017, p. 2.
[154] Giorgio Cencetti, "Il fondamento teorico ella dottrina archivistica," *Archivi VI* (1939), pp. 7–13 reprinted in Giorgio Cencetti, *Scritti archivistici* (Roma, 1970).
[155] Lemieux and Sporny, 2017, p. 4.

[156] Lemieux, Flores, and Lacombe, "Real Estate Transaction Recording in the Blockchain in Brazil."
[157] See, for example, S. Naqvi, "Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals." In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 63:1–63:5, ARES 2018. (New York, NY, USA: ACM, 2018), https://doi.org/10.1145/3230833.3233290 and Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan et al, "An Empirical Analysis of Traceability in the Monero Blockchain," *Proceedings on Privacy Enhancing Technologies* 2018, no. 3 (2018): 143-163. On new developments in the protection of privacy and identity in blockchain systems, see Ian Miers, "How Much Privacy is Enough? Threats, Scaling, and Trade-Offs in Blockchain Privacy Protocols," *Scaling Bitcoin* (Oct. 6-9, 2018), https://scalingbitcoin.org/presentations.
[158] See, Randalph C. Head, "Documents, Archives, and Proof around 1700," *The Historical Journal* 56, no. 4 (2013): 909-930, who explains the concept of *ius archivi* as follows: "Equally influential was the practice of Roman enshrinement of the *tabellio*, the forerunner of the notary. The late Roman *tabellio* was a government official who received, authenticated and kept records in a public archive, the *tabullarium*. Records produced from the *tabullarium* during litigation enjoyed special authority as evidence, which later came to be known as *publica fides*. Such documents, known as *instrumenta fides* or *instrumenta publica*, were still open to challenge in court, but the party challenging them bore the burden of proving they were flawed." (p. 914).
[159] State of Vermont. Act 157, Sec. I.1. 12 V.S.A. § 1913, "An act relating to miscellaneous economic development provisions." (July 1, 2016). Retrieved from https://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20As%20Enacted.pdf.
[160] Lemieux, "Trusting Records."
[161] This practice actually predates the founding of the first public blockchain, Bitcoin, by 13 years. For a discussion on this and how this process of "timestamping works," see Daniel Oberhaus. "The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995" *Motherboard*, Aug. 27, 2018, https://motherboard.vice.com/en_us/article/j5nzx4/what-was-the-first-blockchain
[162] State of Arizona. Chapter 97, Title 44, Section 7061, "Signatures; electronic transactions; blockchain technology" (March 29, 2017). Retrieved from https://legiscan.com/AZ/text/HB2417/id/1588180/Arizona-2017-HB2417-Chaptered.html.
[163] James Condos, William Sorrell, and Susan L. Donegan, "Blockchain Technology: Opportunities and Risks," January 15, 2016), http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf. The study committee concluded: "The study committee has not identified any specific legal or practical benefits from the legislation set forth in Appendix B. However, the group has also not identified any risk inherent in blockchain technology that would warrant withholding the recognition of validity set forth in the legislation. While the committee does not doubt that blockchain technology and the industry forming around it demonstrate significant economic activity and interest, it is unclear what steps Vermont could take to lure any of that activity to the state. Blockchain technology is already in use in the private sector, though clearly in the early stages of adoption, the most prevalent example being virtual currency known as Bitcoin. Further study is required before considering it for the regular business of the State, and moreover, any application would certainly need to support rather than replace the existing records management infrastructure. It is the belief of the study committee

that the benefits of adoption of blockchain technology by state agencies is, at this time, not outweighed by the costs and challenges of such implementation." (p. 20).
[164] Ibid.
[165] On this point, see Marcella Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?." *SSRN* (2015); Markey-Towler, Brendan. "Anarchy, Blockchain and Utopia: A Theory of Political-Socioeconomic Systems Organised using Blockchain." *Journal of the British Blockchain Association* (2018), and Hughes, Eric. "A Cypherpunk's Manifesto." (1993), https://www.activism.net/cypherpunk/manifesto.html and T.C. May. "A Crypto-Anarchist's Manifesto (1992), https://www.activism.net/cypherpunk/crypto-anarchy.html.
[166] Sterlin Lujan." Toward Techno-Anarchy: Blockchain Tech will Thwart Government, Transform Society." *Bitcoin.com News* (Oct. 16, 2018).
[167] Markey-Towney, 2018. Op Cit.
[168] Ibid, p. 13.
[169] Ben Quinn and Charles Arthur, "PlayStation Network Hackers Access Data of 77 Million Users," *The Guardian*, April 26, 2011, sec. Games, https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data.
[170] "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed," September 18, 2017, https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed.
[171] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, sec. News, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[172] "What Is a Personal Health Record?," HealthIT.gov, May 2, 2016, https://www.healthit.gov/faq/what-personal-health-record-0.
[173] "What is A Personal Health Record (PHR)?", American Health Information Management Association (AHIMA), accessed October 11, 2018, http://www.myphr.com/StartaPHR/what_is_a_phr.aspx
[174] "Myth Buster: Patients Own Their Health Information and Medical Records | Health Information & the Law," *Health Information & the Law*, August 27, 2015, http://www.healthinfolaw.org/article/myth-buster-patients-own-their-health-information-and-medical-records.
[175] Hofman et al., "'The Margin between the Edge of the World and Infinite Possibility.'"
[176] Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on Their Implications for the Future of Archival Preservation."
[177] Queen's Printer, "Freedom of Information and Protection of Privacy Act [RSBC 1996] CHAPTER 165," accessed March 20, 2019, http://www.bclaws.ca/Recon/document/ID/freeside/96165_00.
[178] Definitions for "custody" and "control" adapted from: "FOIPPA Policy Definitions," Accessed October 28, 2018, https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions#c
[179] The Sedona Conference, "The Sedona Conference Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control,'" *The Sedona Conference Journal* 17, no. 2 (2016): 467.
[180]Barbara Reed, "Recordkeeping System(s)" in Luciana Duranti and Patricia C. Franks, *Encyclopedia of Archival Science* (Lanham, MD, UNITED STATES: Rowman & Littlefield Publishers, 2015), http://ebookcentral.proquest.com/lib/ubc/detail.action?docID=2076364.

[181] Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on Their Implications for the Future of Archival Preservation."
[182] Lemieux.
[183] Juan Benet, "IPFS – Content Addressed, Versioned, P2P File System (DRAFT 3)," GitHub, accessed October 22, 2018, 3, https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf
[184] G. M., "Where does IPFS store all the data?", stackoverflow, accessed October 22, 2018, https://stackoverflow.com/questions/47450007/where-does-ipfs-store-all-the-data#
[185] jbenet, "Replication on IPFS – Or, the Backing-Up Content Model," GitHub, September 26, 2015, accessed October 24, 2018, https://github.com/ipfs/faq/issues/47
[186] Reed, "Recordkeeping System(s)," 325.
[187] Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on Their Implications for the Future of Archival Preservation."
[188] Lemieux.
[189] Lemieux.
[190] Lemieux.
[191] Chris Reed, "Information in the Cloud: Ownership, Control and Accountability," in *Privacy and Legal Issues in Cloud Computing* (Edward Elgar Publishing, 2015), http://www.elgaronline.com/view/9781783477067.00014.xml.
[192] Reed.
[193] The Sedona Conference, "The Sedona Conference Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control.'"
[194] The Sedona Conference.
[195] The Sedona Conference.
[196] Lemieux and Sporny, "Preserving the Archival Bond in Distributed Ledgers."
[197] The Sedona Conference, "The Sedona Conference Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control.'"
[198] Reed, "Information in the Cloud: Ownership, Control and Accountability."
[199] M L Badger et al., "Cloud Computing Synopsis and Recommendations" (Gaithersburg, MD: National Institute of Standards and Technology, 2012), https://doi.org/10.6028/NIST.SP.800-146.
[200] Badger et al.
[201] Badger et al.
[202] Examples of boundary mechanisms in a cloud computing environment are firewalls, guards and virtual private networks. Ibid.
[203] The cloud deployment models referred to in the NIST 800-146 definition are as follows: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud, Ibid, 2-2.
[204] Ibid, 4-3-4-4.
[205] Reed, "Information in the Cloud: Ownership, Control and Accountability."
[206] Some blockchains implement sidechains which act as a private channel between participants.
[207] Reed, "Information in the Cloud: Ownership, Control and Accountability."
[208] Reed.
[209] Dylan Yaga et al., "Blockchain Technology Overview" (National Institute of Standards and Technology, October 2018).
[210] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (December 15, 1890): 193.

[211] Office of the Secretary, “Records, Computers, and the Rights of Citizens” (U.S. Department of Health, Education, & Welfare, July 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
[212] Alan F. Westin, *Privacy and Freedom* (New York: IG Publishing, 2015).
[213] Westin.
[214] Pekka Henttonen, “Privacy as an Archival Problem and a Solution,” *Archival Science* 17, no. 3 (September 2017): 285–303, https://doi.org/10.1007/s10502-017-9277-0.
[215] A number of different models of privacy exist, including one that specifically focuses on contextual integrity (Helen Fay Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*), Book, Whole (Stanford, Calif: Stanford Law Books, 2010).
[216] Daniel Solove, “Introduction: Privacy Self-Management and the Consent Dilemma,” *Harvard Law Review* 126, no. 7 (2013): 1880–1903.
[217] Helen Nissenbaum, “A Contextual Approach to Privacy Online,” *Daedalus* 140, no. 4 (2011): 32–48, https://doi.org/10.1162/DAED_a_00113.
[218] Daniel J. Solove, “Access and Aggregation: Public Records, Privacy and the Constitution,” *Minnesota Law Review* 86, no. 6 (2002): 1137.
[219] Amy Phelps and Allan Watt, “I Shop Online – Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia,” *Digital Investigation* 11, no. 4 (2014): 261–72, https://doi.org/10.1016/j.diin.2014.08.001.
[220] Husam Al Jawaheri et al., “When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis,” arXiv, (January 2018): 1-11, https://arxiv.org/pdf/1801.07501.pdf.
[221] Ryan Henry, Amir Herzberg, and Aniket Kate, “Blockchain Access Privacy: Challenges and Directions,” *IEEE Security & Privacy* 16, no. 4 (2018): 38–45, https://doi.org/10.1109/MSP.2018.3111245.
[222] See, https://sovrin.org/
[223] See, https://www.hyperledger.org/projects/hyperledger-indy.
[224] See, https://orgbook.gov.bc.ca/en/home.
[225] W3C, “Decentralized Identifiers v0.11.” https://w3c-ccg.github.io/did-spec/ (2019).
[226] W3C, “Verifiable Claims Working Group Charter,” https://www.w3.org/2017/vc/charter.html (2019)
[227] Andrew Tobin, Drummond Reed, and Phillip J Windley, “The Inevitable Rise of Self-Sovereign Identity - White Paper,” (Sovrin Foundation, 2017), https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.
[228] Council of the European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," (General Data Protection Regulation) (Text with EEA Relevance).
[229] F.W.J. van Geelkerken and K. Konings, “Using Blockchain to Strengthen the Rights Granted through the GDPR,” in *Litteris et Artibus : Proceedings, 2017* (7th International youth science forum «Litteris et Artibus», Lviv, Ukraine: Lviv Polytechnic Publishing House, 2017), 458–61, http://ena.lp.edu.ua:8080/handle/ntb/40463.
[230] United States, “The Health Insurance Portability and Accountability Act (HIPAA),” Pub. L. No. 104–191, 1936 110 Stat. (1996), https://www.gpo.gov/fdsys/pkg/FR-2002-08-14/pdf/FR-2002-08-14.pdf.

[231] Gary LaFever, "Blockchain and Big Data Privacy in Healthcare," *IAPP Privacy Tech* (blog), May 2, 2016, https://iapp.org/news/a/blockchain-and-big-data-privacy-in-healthcare/.
[232] Ariel Ekblaw and Asaf Azaria, "MedRec: Medical Data Management on the Blockchain," *Viral Communications*, April 11, 2016, https://viral.media.mit.edu/pub/medrec.
[233] Lemieux and Sporny, "Preserving the Archival Bond in Distributed Ledgers."
[234] Darra Hofman and Alamir Novin, "Blocked and Chained: Blockchain and the Problems of Transparency," (2018 ASIS&T Annual Meeting, Vancouver, Canada, 2018).
[235] Darra L. Hofman, "Legally Speaking: Smart Contracts, Archival Bonds, and Linked Data in the Blockchain," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada: IEEE, 2017), 1–4, https://doi.org/10.1109/ICCCN.2017.8038515.
[236] Lemieux and Sporny, "Preserving the Archival Bond in Distributed Ledgers."
[237] Yaga et al., "Blockchain Technology Overview."
[238] See, https://www.iso.org/committee/6266604.html
[239] Victoria Lemieux is aware of this development in her role as ISO TC307 liaison to ISO TC46 SC11.
[240] CEN-CENELEC Focus Group on and Blockchain and Distributed Ledger Technologies (FG-BDLT), "Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies" (CEN-CENELEC, 2018), ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf.
[241] CEN-CENELEC Focus Group on and Blockchain and Distributed Ledger Technologies (FG-BDLT).
[242] See, https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
[243] ITU News. "Blockchain experts invited to highlight use cases to benefit from standards" (2018). https://news.itu.int/inviting-blockchain-use-cases/
[244] Abraham, "Whitepaper about the Concept of Self-Sovereign Identity Including Its Potential."
[245] Abraham.
[246] W3C Community Group. "Decentralized Identifiers (DIDs) v0.11: Data Model and Syntaxes for Decentralized Identifiers (DIDs) (2019). https://w3c-ccg.github.io/did-spec/
[247] W3C. "Verifiable Claims Working Group Charter." (2019). https://www.w3.org/2017/vc/charter.html
[248] Markus Sabadello et al., *Introduction to DID Auth* (2018; repr., Web of Trust Info, 2019), https://github.com/WebOfTrustInfo/rwot6-santabarbara.
[249] Samburaj Das. "China to Establish National Blockchain Standards by 2019: Govt. Official." *CCN* (2018). https://www.ccn.com/china-government-to-establish-national-blockchain-standards-by-2019-report/ and CryptoSomniac. "National Blockchain Standards will be Established in China by 2019." *Medium* (2018). https://medium.com/@cryptosomniac/national-blockchain-standards-will-be-established-in-china-by-2019-c7847b49626f
[250] Yaga et al., "Blockchain Technology Overview."
[251] Gaurav Agrawal, "All About ERC Token Standards," *Coinmonks* (blog), May 31, 2018, https://medium.com/coinmonks/all-about-erc-token-standards-9c759efdc791.
[252] "ERC: Token Standard · Issue #20 · Ethereum/EIPs," GitHub, accessed March 20, 2019, https://github.com/ethereum/EIPs/issues/20.

[253] See, https://www.cryptokitties.co/?gclid=EAIaIQobChMIls6i19Cd4AIVmONkCh2NBwY-EAAYASAAEgKXqPD_BwE
[254] Security Token Roundtable. “The Security Token Standard.” GitHub (2018). https://github.com/securitytokenstandard
[255] See, https://thesecuritytokenstandard.org/
[256] https://entethalliance.org/wp-content/uploads/2018/11/EEA-Architecture-Stack-Spring-2018-Updated-1.pdfEnterprise Ethereum Client Specification V2
[257] Daniel Burnett et al., “Enterprise Ethereum Client Specification V2” (Enterprise Ethereum Alliance, October 15, 2018), https://entethalliance.org/wp-content/uploads/2018/11/EEA_Enterprise_Ethereum_Client_Specification_V2.pdf.
[258] https://www.r3.com/
[259] https://www.hyperledger.org/
[260] https://blockchain.ieee.org/standards
[261] https://www.himss.org/himss-faqs
[262] See, https://www.himss.org/news/part-1-navigating-blockchain-landscape-opportunities-digital-health
[263] See, RDA, “Blockchain Applications in Health WG Case Statement.” (2019). https://www.rd-alliance.org/group/blockchain-applications-health-wg/case-statement/blockchain-applications-health-wg-case
[264] Ibid.
[265] Op. Cit.

Bibliography

14:00-17:00. “ISO 15489-1:2016 - Information and Documentation -- Records Management -- Part 1: Concepts and Principles.” International Organization for Standardization (ISO), 2016. http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/25/62542.html.

Abraham, Andreas. “Whitepaper about the Concept of Self-Sovereign Identity Including Its Potential,” n.d., 39.

Agrawal, Gaurav. “All About ERC Token Standards.” *Coinmonks* (blog), May 31, 2018. https://medium.com/coinmonks/all-about-erc-token-standards-9c759efdc791.

Badger, M L, T Grance, R Patt-Corner, and J Voas. “Cloud Computing Synopsis and Recommendations.” Gaithersburg, MD: National Institute of Standards and Technology, 2012. https://doi.org/10.6028/NIST.SP.800-146.

Baliga, Arati. “Understanding Blockchain Consensus Models.” Persistent, 2017. https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf.

Baran, P. “On Distributed Communications Networks.” *IEEE Transactions on Communications Systems* 12, no. 1 (March 1964): 1–9. https://doi.org/10.1109/TCOM.1964.1088883.

“Blockchain Land Registry Tech Gets Test in Brazil - CoinDesk.” *Coindesk* (blog), April 5, 2017. https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil.

Bralić, Vladimir, Magdalena Kuleš, and Hrvoje Stančić. “A Model for Long-Term Preservation of Digital Signature Validity: TrustChain.” *INFuture2017: Integrating ICT in Society*, 2017. https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain.

Brzica, Hrvoje, Boris Herceg, and Hrvoje Stan. “Long-Term Preservation of Validity of Electronically Signed Records.” *INFuture 2013: Information Governance*, 2013, 147–58.

“Building Trust in Government: Exploring the Potential of Blockchains.” Executive Report. Somers, NY: IBM Institute for Business Value, 2017. https://www.ibm.com/downloads/cas/WJNPLNGZ.

Burnett, Daniel, Robert Coote, Chaals Nevile, and Grant Noble. “Enterprise Ethereum Client Specification V2.” Enterprise Ethereum Alliance, October 15, 2018. https://entethalliance.org/wp-content/uploads/2018/11/EEA_Enterprise_Ethereum_Client_Specification_V2.pdf.

Buterin, Vitalik. “Ethereum White Paper - A Next-Generation Smart Contract and Decentralized Application Platform.” GitHub, March 19, 2019. https://github.com/ethereum/wiki.

Cadwalladr, Carole, and Emma Graham-Harrison. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” *The Guardian*, March 17, 2018, sec. News. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

CEN-CENELEC Focus Group on, and Blockchain and Distributed Ledger Technologies (FG-BDLT). “Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies.” CEN-CENELEC, 2018.

ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf.
Cohen, Fred. “A TALE OF TWO TRACES – DIPLOMATICS AND FORENSICS,” AICT-462:3–27, 2015. https://doi.org/10.1007/978-3-319-24123-4_1.
Coleman, Lester. “Georgia Expands Project to Secure Land Titles on the Bitcoin Blockchain.” *CCN* (blog), July 2, 2017. https://www.ccn.com/republic-of-georgia-expands-project-to-secure-land-titles-on-the-bitcoin-blockchain.
Collomosse, John, Tu Bui, Alan Brown, John Sheridan, Alex Green, Mark Bell, Jamie Fawcett, Jez Higgins, and Olivier Thereaux. “ARCHANGEL: Trusted Archives of Digital Public Documents.” *ArXiv:1804.08342 [Cs]*, April 23, 2018. http://arxiv.org/abs/1804.08342.
Deery, Brian. “The Blockchain & Future Of Business Records.” *Blockchain News* (blog), May 7, 2016. https://www.the-blockchain.com/2016/05/07/blockchain-future-business-records-brian-deery-chief-scientist-factom-inc/.
“Defensible Disposition: Real-World Strategies for Actually Pushing the Delete Button.” Los Altos, CA: Contoural, Inc., 2014. http://www.armaboston.org/images.html?file_id=t2tv5Y%2Fy%2BeI%3D.
Dingwall, Glenn. “Life Cycle and Continuum: A View of Recordkeeping Models from the Postwar Era.” In *Currents in Archival Thinking*, 1st ed. Santa Barbara, Calif: ABC-CLIO, LLC, 2010.
Director, Caroline Williams. “Diplomatic Attitudes: From Mabillon to Metadata.” *Journal of the Society of Archivists* 26, no. 1 (April 1, 2005): 1–24. https://doi.org/10.1080/00039810500047417.
Duranti, Luciana. *Diplomatics: New Uses for an Old Science*. Lanham, Md: Scarecrow Press, 1998.
———. “Preservation in the Cloud: Towards an International Framework for a Balance of Trust and Trustworthiness.” In *APA/C-DAC International Conference on Digital Preservation & Development of Trusted Digital Repositories*, 23–38. New Delhi, India: Centre for Development of Advanced Computing, 2014.
Duranti, Luciana, and Patricia C. Franks. *Encyclopedia of Archival Science*. Lanham, MD, UNITED STATES: Rowman & Littlefield Publishers, 2015. http://ebookcentral.proquest.com/lib/ubc/detail.action?docID=2076364.
Duranti, Luciana, and Randy Preston. “International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records.” Associazione Nazionale Archivistica Italiana, 2008. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf.
Duranti, Luciana, and Corinne Rogers. “Trust in Records and Data Online.” In *Integrity in Government through Records Management : Essays in Honour of Anne Thurston*, 2nd ed., 203–14. New York, NY: Routledge, 2016.
Duranti, Luciana, and Kenneth Thibodeau. “The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES*.” *Archival Science; Dordrecht*, 2006. http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/s10502-006-9021-7.
EDRM, LLC. *How the Information Governance Reference Model (IGRM) Complements ARMA International’s Generally Accepted Recordkeeping Principles (GARP®)*. EDRM, 2011. https://books.google.ca/books?id=h6wWrgEACAAJ.
Ekblaw, Ariel, and Asaf Azaria. “MedRec: Medical Data Management on the Blockchain.” *Viral Communications*, April 11, 2016. https://viral.media.mit.edu/pub/medrec.

"Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed," September 18, 2017. https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed.

"ERC: Token Standard · Issue #20 · Ethereum/EIPs." GitHub. Accessed March 20, 2019. https://github.com/ethereum/EIPs/issues/20.

Eyal, Ittay, and Emin Gün Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." *Communications of the ACM* 61, no. 7 (June 2018): 95–102. https://doi.org/10.1145/3212998.

Fazzio, Frank. "Blockchain for Information Governance: Vetting a Solution." *Zasio* (blog), April 4, 2018. https://www.zasio.com/blockchain-for-information-governance-vetting-a-solution/.

Findlay, Cassie. "Decentralised and Inviolate: The Blockchain and Its Uses for Digital Archives." *Recordkeeping Roundtable* (blog), January 23, 2015. https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.

Frings-Hessami, Viviane. "Looking at the Khmer Rouge Archives through the Lens of the Records Continuum Model: Towards an Appropriated Archive Continuum Model." *Information Research* 22, no. 4 (December 15, 2017): 1–14.

Geelkerken, F.W.J. van, and K. Konings. "Using Blockchain to Strengthen the Rights Granted through the GDPR." In *Litteris et Artibus : Proceedings, 2017*, 458–61. Lviv, Ukraine: Lviv Polytechnic Publishing House, 2017. http://ena.lp.edu.ua:8080/handle/ntb/40463.

"Generally Accepted Recordkeeping Principles." ARMA International, 2009. https://www.armavi.org/docs/garp.pdf.

Glover, Anne, Crystal O'Donnell, and David N Sharpe. "The Sedona Canada Principles Addressing Electronic Discovery, Second Edition." The Sedona Conference, 2015. https://www.canlii.org/en/info/sedonacanada/2015principles_en.pdf.

Grossman, Maura R., and Gordon V. Cormack. "Technology-Assisted Review in e-Discovery Can Be More Effective and More Efficient than Exhaustive Manual Review." *Richmond Journal of Law & Technology (Online)* 17, no. 3 (2011): 1.

Henry, Ryan, Amir Herzberg, and Aniket Kate. "Blockchain Access Privacy: Challenges and Directions." *IEEE Security & Privacy* 16, no. 4 (2018): 38–45. https://doi.org/10.1109/MSP.2018.3111245.

Henttonen, Pekka. "Privacy as an Archival Problem and a Solution." *Archival Science* 17, no. 3 (September 2017): 285–303. https://doi.org/10.1007/s10502-017-9277-0.

Hernandez, Steven, and Adam Gordon. *The Official (ISC)2 Guide to the SSCP CBK*,. 4th Edition. 2016: Sybex. Accessed March 20, 2019. https://learning.oreilly.com/library/view/the-official-isc2/9781119278634/.

Hofman, Darra L. "Legally Speaking: Smart Contracts, Archival Bonds, and Linked Data in the Blockchain." In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 1–4. Vancouver, BC, Canada: IEEE, 2017. https://doi.org/10.1109/ICCCN.2017.8038515.

Hofman, Darra, Victoria Louise Lemieux, Alysha Joo, and Danielle Alves Batista. "'The Margin between the Edge of the World and Infinite Possibility': Blockchain, GDPR and Information Governance." *Records Management Journal* 29, no. 1/2 (February 13, 2019): 240–57. https://doi.org/10.1108/RMJ-12-2018-0045.

Hofman, Darra, and Alamir Novin. “Blocked and Chained: Blockchain and the Problems of Transparency.” Vancouver, Canada, 2018.

“InterPARES Trust - Terminology.” Accessed March 19, 2019. https://interparestrust.org/terminology.

“InterPARES Trust Terminology: Blockchain Terminology,” 2017. http://arstweb.clayton.edu/interlex/blockchain/.

Jawaheri, Husam Al, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. “When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis,” no. Journal Article (2018).

Kahn, Randolph A. “Why Destruction of Information Is So Difficult and So Essential: The Case for Defensible Disposal.” *American Bar Association - Business Law Today*, 2018. http://go.galegroup.com.ezproxy.library.ubc.ca/ps/i.do?p=LT&u=ubcolumbia&id=GALE%7CA576220627&v=2.1&it=r&sid=summon.

Kochin, Dmitry. “Where Do Decentralized Applications Store Their Data?” GitHub, March 16, 2019. https://github.com/TiesNetwork/ties-docs.

LaFever, Gary. “Blockchain and Big Data Privacy in Healthcare.” *IAPP Privacy Tech* (blog), May 2, 2016. https://iapp.org/news/a/blockchain-and-big-data-privacy-in-healthcare/.

Lemieux, V. L. “A Typology of Blockchain Recordkeeping Solutions and Some Reflections on Their Implications for the Future of Archival Preservation.” In *2017 IEEE International Conference on Big Data (Big Data)*, 2271–78, 2017. https://doi.org/10.1109/BigData.2017.8258180.

Lemieux, Victoria, Daniel Flores, and Claudia Lacombe. “Real Estate Transaction Recording in the Blockchain in Brazil.” *Records in the “Chain” Project Publications* (blog), 2018. https://blogs.ubc.ca/recordsinthechain/2018/01/26/real-estate-transaction-recording-in-the-blockchain-in-brazil/.

Lemieux, Victoria L. “Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework.” *IEEE Future Technologies Conference*, 2017. https://www.researchgate.net/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework.

———. “Blockchain Recordkeeping: A Swot Analysis.” *Information Management; Overland Park* 51, no. 6 (December 2017): 20-22,24,26-27.

Lemieux, Victoria L. “Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective.” *European Property Law Journal* 6, no. 3 (2017): 392–440.

Lemieux, Victoria L., and Manu Sporny. “Preserving the Archival Bond in Distributed Ledgers: A Data Model and Syntax.” In *Proceedings of the 26th International Conference on World Wide Web Companion - WWW ’17 Companion*, 1437–43. Perth, Australia: ACM Press, 2017. https://doi.org/10.1145/3041021.3053896.

Lemieux, Victoria Louise. “Trusting Records: Is Blockchain Technology the Answer?” *Records Management Journal* 26, no. 2 (July 18, 2016): 110–39. https://doi.org/10.1108/RMJ-12-2015-0042.

Lima, Claudio. “Blockchain-GDPR Privacy by Design: How Decentralized Blockchain Internet Will Comply with GDPR Data Privacy.” IEEE Blockchain Standards, 2018. https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf.

Lin, Iuon-Chang, and Tzu-Chun Liao. “A Survey of Blockchain Security Issues and Challenges.” *International Journal of Network Security* 19, no. 5 (September 2017): 653–59. https://doi.org/10.6633/IJNS.201709.19(5).01.

Macneil, Heather. “Trust and professional identity: narratives, counter-narratives and lingering ambiguities.” *Archival Science* 11 (2011): 175–92. http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/s10502-011-9150-5.

MacNeil, Heather. *Trusting Records: Legal, Historical and Diplomatic Perspectives*. Springer Science & Business Media, 2000.

Manku, Gurmeet Singh, Arvind Jain, and Anish Das Sarma. “Detecting Near-Duplicates for Web Crawling.” In *Proceedings of the 16th International Conference on World Wide Web*, 141–150. WWW ’07. New York, NY, USA: ACM, 2007. https://doi.org/10.1145/1242572.1242592.

Maxwell, Winston, and John Salmon. “A Guide to Blockchain and Data Protection.” Hogan Lovells, 2017. https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf.

McKemmish, Sue. “Placing Records Continuum Theory and Practice.” *Archives & Museum Informatics* 1 (2001): 333–59. http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/BF02438901.

“Myth Buster: Patients Own Their Health Information and Medical Records | Health Information & the Law.” *Health Information & the Law*, August 27, 2015. http://www.healthinfolaw.org/article/myth-buster-patients-own-their-health-information-and-medical-records.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” www.bitcoin.org, 2008. https://bitcoin.org/bitcoin.pdf.

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. “Bitcoin and Cryptocurrency Technologies.” *Princeton University Press*, 2016, 308.

Nissenbaum, Helen. “A Contextual Approach to Privacy Online.” *Daedalus* 140, no. 4 (2011): 32–48. https://doi.org/10.1162/DAED_a_00113.

Nissenbaum, Helen Fay. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Book, Whole. Stanford, Calif: Stanford Law Books, 2010.

O’Dwyer, K. J., and D. Malone. “Bitcoin Mining and Its Energy Footprint.” In *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 280–85, 2014. https://doi.org/10.1049/cp.2014.0699.

Office of the Secretary. “Records, Computers, and the Rights of Citizens.” U.S. Department of Health, Education, & Welfare, July 1973. https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

Pearce-Moses, Richard. *A Glossary of Archival and Records Terminology*. Archival Fundamentals Series. II. Chicago: Society of American Archivists, 2005.

Phelps, Amy, and Allan Watt. “I Shop Online – Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia.” *Digital Investigation* 11, no. 4 (2014): 261–72. https://doi.org/10.1016/j.diin.2014.08.001.

Queen’s Printer. “Freedom of Information and Protection of Privacy Act [RSBC 1996] CHAPTER 165.” Accessed March 20, 2019. http://www.bclaws.ca/Recon/document/ID/freeside/96165_00.

Quinn, Ben, and Charles Arthur. “PlayStation Network Hackers Access Data of 77 Million Users.” *The Guardian*, April 26, 2011, sec. Games. https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data.

R Thomas Howell Jr, and Rae N. Cogar. “Developing And Implementing A Record Retention Program.” *Practical Lawyer* 50, no. 6 (2004): 21.

Reed, Chris. “Information in the Cloud: Ownership, Control and Accountability.” In *Privacy and Legal Issues in Cloud Computing*. Edward Elgar Publishing, 2015. http://www.elgaronline.com/view/9781783477067.00014.xml.

Rennie, Stuart. “Dispelling Myths About Records Retention in Canada.” *Canadian RIM, an ARMA Canada Publication* 1, no. 1 (Spring 2016). https://www.armacanada.org/index.php/resources-knowledge/documents2/canadian-rim/276-dispelling-myths-about-records-retention-in-canada/file.

Rodenburg, Brandon, and Stephen P. Pappas. “Blockchain and Quantum Computing.” Princeton, NJ: The MITRE Corporation., 2017. https://pdfs.semanticscholar.org/2284/08bf3c13f0d579f21a5d999e7d4967104c09.pdf.

Sabadello, Markus, Kyle Den Hartog, Christian Lundkvist, Cedric Franz, Alberto Elias, Andrew Hughes, John Jordan, and Dmitri Zagidulin. *Introduction to DID Auth*. 2018. Reprint, Web of Trust Info, 2019. https://github.com/WebOfTrustInfo/rwot6-santabarbara.

Sankar, L. S., M. Sindhu, and M. Sethumadhavan. “Survey of Consensus Protocols on Blockchain Applications.” In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 1–5, 2017. https://doi.org/10.1109/ICACCS.2017.8014672.

Smallwood, Robert F., ed. *Information Governance: Concepts, Strategies and Best Practices*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2015. https://doi.org/10.1002/9781118433829.

Solove, Daniel. “Introduction: Privacy Self-Management and the Consent Dilemma.” *Harvard Law Review* 126, no. 7 (2013): 1880–1903.

Solove, Daniel J. “Access and Aggregation: Public Records, Privacy and the Constitution.” *Minnesota Law Review* 86, no. 6 (2002): 1137.

Stapleton, Adam. “Continuum in Context: Post-Eighteenth Century Archival Theory and the Records Continuum Model.” *ARCHIFACTS* 1 (2005): 21–46.

Stephens, David O. “What Is Past Is Prologue: What History Reveals About the Future of RIM.” *Information Management* 51, no. 5 (October 2017): 34–38.

Szabo, Nick. “The Idea of Smart Contracts.” Nick Szabo’s Papers and Concise Tutorials, 1997. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

“The Land Registry in the Blockchain - Testbed.” Kayros Future, March 2017. https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf.

The Sedona Conference. “THE SEDONA CONFERENCE COMMENTARY ON INFORMATION GOVERNANCE.” *The Sedona Conference Journal* 15 (2014): 125–66.

———. “The Sedona Conference Commentary on Rule 34 and Rule 45 ‘Possession, Custody, or Control.’” *The Sedona Conference Journal* 17, no. 2 (2016): 467.

———. “The Sedona Conference Principles and Commentary on Defensible Disposition - Public Comment Version.” The Sedona Conference, 2018. https://thesedonaconference.org/sites/default/files/publications/Principles%20and%20Commentary%20on%20Defensible%20Disposition_0.pdf.

"The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production." *Sedona Conference Journal* 19 (2018).

Tobin, Andrew, Drummond Reed, and Foreword Phillip J Windley. "The Inevitable Rise of Self-Sovereign Identity - White Paper." Sovrin Foundation, 2017. https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

Union, Publications Office of the European. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)." Website, April 27, 2016. https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en.

United States. The Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104–191, 1936 110 Stat. (1996). https://www.gpo.gov/fdsys/pkg/FR-2002-08-14/pdf/FR-2002-08-14.pdf.

Upward, Frank. "Modelling the Continuum as Paradigm Shift in Recordkeeping and Archiving Processes, and beyond Ö a Personal Reflection." *Records Management Journal* 10, no. 3 (December 2000): 115–39. https://doi.org/10.1108/EUM0000000007259.

Vigna, Paul, and Michael J. Casey. *The Truth Machine: The Blockchain and the Future of Everything*. New York: St. Martin's Press, 2018.

Walch, Angela. "In Code (Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains," 2018.

———. "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk." *New York University Journal of Legislation and Public Policy* 18 (2015): 837–94.

Warren, Samuel, and Louis Brandeis. "The Right to Privacy." *Harvard Law Review* 4 (December 15, 1890): 193.

Westin, Alan F. *Privacy and Freedom*. New York: IG Publishing, 2015.

"What Is a Personal Health Record?" HealthIT.gov, May 2, 2016. https://www.healthit.gov/faq/what-personal-health-record-0.

Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain Technology Overview." National Institute of Standards and Technology, October 2018.

Yeo, Geoffrey. "Concepts of Record (1): Evidence, Information, and Persistent Representations." *The American Archivist* 70, no. 2 (2007): 315–43.

———. "Trust and Context in Cyberspace." *Archives and Records* 34, no. 2 (October 1, 2013): 214–34. https://doi.org/10.1080/23257962.2013.825207.

Appendix A

Table 4: A High-level Comparison of Some of the Features of Popular Blockchains (Source: Blocksplain[1], authors' own research)

Feature	Bitcoin	Ethereum	Ethereum/ Quorum	Hyper ledger Fabric	Hyper ledger Indy	Corda
Public/ Private?	Public	Public	Private	Private	Public/ Private	Private
Privacy Features	Operates Pseudo-nony mously	Operates Pseudo-nony mously	Private transactions Private tokens Experimental Zero Knowledge Proofs	Private channels Private transactions Zero Knowledge Proofs	Uses Decentral-ized Identifies Private trans-actions Zero Know-ledge Proofs	Only private transactions
Security	Strength of consensus mechanism	Strength of consensus mechanism	Node authent-ication	Node authent-ication	Public: consensus mechan-ism Private: Node authent-ication	Node Authent-ication Block-chain App. firewall
Consensus	Proof of Work	Proof of Work	Raft IBFT	Multiple approaches	RBFT Uses stewards	Trusted notary nodes
Transaction Performance	Limited to ~7 trans-actions per second	Limited to ~15 trans-actions per second	Very scalable	Very scalable	Highly Variable (depending on pool size ~16-41 transactions per second)	Very scalable
Transaction Finality	Yes	Yes	Yes	Yes	Yes	Yes
Smart Contracts	Bitcoin scripting	Yes	Solidity	Java, node.js, Go Higher-level abstraction= Composer, javascript	No	Kotlin, Java Legal Prose

[1] "Blockchain speeds & the scalability debate." *Blocksplain* (2018). https://blocksplain.com/2018/02/28/transaction-speeds/.

Appendix B

Overview of "Records in the Chain Project" Case Studies

Appendix B.1

Project Name: Records in the Chain

Case Title: Real Estate Transaction Recording in the Blockchain in Brazil

Case Number: RCPLAC-01 -- Case Study 1

Collaborators/Writers/Authors: Victoria Lemieux, Daniel Flores, & Claudia Lacombe; Real Estate Registry Office, Pelotas – RS, Brazil, Ubitquity LLC., & University of British Columbia (Blockchain@UBC).

Summary: The report presents a pilot study of the application of Blockchain technology to land transaction recording in the Municipality of Pelotas, Rio Grande do Sul, Brazil. It was carried out between May to September, 2017 as part of the University of British Columbia's "Records in the Chain" Project and CNPQ UFSM Ged/A Digital Records Research Group.

Findings/Conclusions: The report reviewed a solution designed to record transfers of land ownership in the Municipality of Pelotas, Rio Grande do Sul, Brazil, and assessed it using an archival science theoretic lens, since archival criteria for trustworthy records closely aligns to legal requirements for determining admissibility and weight of evidence and legal status of titles and given the requirements for long-term trustworthiness and accessibility of land title records. Though the potential benefits of applying blockchain technology in land registration are great – improved efficiency, reduced transactional friction, better security, etc. – the findings showed, at the time of the report's elaboration, that there were many aspects of the solution that needed further examination and, possibly, (re)design from an archival perspective.

The report analyzed the technology's impact upon long-term availability and evidential quality of blockchain records concluding that a reduction in evidential quality or loss of access to blockchain records may have a significant negative impact upon transparency and public accountability and deprive individuals of their entitlement to land. Changes to the legal, administrative and procedural rules were necessary by the time of the case study in order for such systems to work effectively.

Link: http://blogs.ubc.ca/recordsinthechain/files/2018/01/RCPLM-01-Case-Study-1_v14_English_Final.pdf

Appendix B.2

Project Name: Records in the Chain

Case Title: Centre of Excellence for Prevention of Organ Failure (PROOF)

Case Number: RCPCA-01 -- Case Study 1

Collaborators/Writers/Authors: Victoria Lemieux & Darra Hofman; PROOF Centre of Excellence, Providence Health Care, University of Nebraska Medical Center, Deloitte, University of British Columbia (Blockchain@UBC), & PROOF Centre of Excellence.

Summary: The report presents analysis of a project, carried out between January 2017 and December 2017, concerning the development of an application of Blockchain technology for the data sharing process for participants in health research. The University of British Columbia's "Records in the Chain" Project had a Ph.D. student, Darra Hofman, embedded in this project.

Findings/Conclusions: The solution in the study seeks to utilize some of the unique features of the Blockchain – its immutability, automatic timestamping, and distributed architecture – to solve some of the pain points in study participant enrollment, consent gathering, and data sharing in health research. The full implementation, if designed correctly, could reduce the work and cost of consent management and data sharing. However, a number of archival, technical, and ethical aspects of the system must be better understood before the system moves from Proof of Concept to fully functioning solution. An examination of the formal procedures controlling the creation of the records associated with the system, as well as a full diplomatic analysis of such records to identify their required physical and intellectual forms, is necessary to ensure that the systems can create reliable records. Given the extraordinarily sensitive nature of the data that will be stored and shared through the system, privacy protections should be implemented. Because of the light regulatory hand applied to health research (at the level of statute, as opposed to ethics board oversight), this use case offers an opportunity to explore the use of a blockchain solution in a high-impact, high-requirement, yet relatively free environment.

Link: http://blogs.ubc.ca/recordsinthechain/files/2018/06/PROOF-Case-Study_22-June_FINAL.pdf

Appendix B.3

Project Name: Records in the Chain

Case Title: Real Estate Transaction Recording on the Blockchain in British Columbia

Case Number: RCPCA-02 -- Case Study 1

Collaborators/Writers/Authors: Victoria Lemieux, Alysha Joo, & Darra Hofman; Land Title and Survey Authority of British Columbia (LTSA), Digital Identity and Authentication Council of Canada, LandSure Systems (subsidiary of LTSA), IdentityNORTH, & University of British

Columbia (Blockchain@UBC).

Summary: The report analyzes the solutions presented on a design challenge competition proposed by the Digital ID & Authentication Council of Canada (DIACC) and the Land Title and Survey Authority of British Columbia to offer students and professionals the chance to contribute ideas for a real world, industry application of digital identification in the context of land title transfers within the Canadian province of British Columbia. The design challenge was a collaboration between DIACC, the Land Title and Survey Authority of British Columbia, IdentityNORTH, and the University of British Columbia.

Findings/Conclusions: The reported analyzed the solutions presented on the design challenge competition proposed by the Digital ID & Authentication Council of Canada (DIACC) and the Land Title and Survey Authority (LTSA) of British Columbia and concluded that submissions mostly focused on leveraging blockchain technology, and not addressing the Digital ID aspect of the use case. Of the eight submissions, a variety of methods for embedding identity into an electronic state of title certificate (eSTC) were proposed. One of the lessons learned from the design challenge is that implementation of a blockchain-based solution will require thinking through whether changes would be needed to the LTSA's current business model and revenue streams (e.g., from issuance of eSTCs). None of the solutions presented covered every aspect of the reference architecture fully. The winning solution focused on the application layer, while the runner-up solution focused on the core blockchain processing layer. Given that each team focused on different aspects of the solution, with each generating novel ideas to support the use case, it may be that the best approach is to combine solutions to increase efficiency of the current eSTC system. The organizing team concluded that it would need to do further research because there is evolution in the technology, leading to a fair amount of change, and the technology is developing at a fast pace. A full understanding of how blockchain could be applied is still far away. Moreover, because blockchain is an ecosystem solution (i.e., intended to work across different organizations and business partners), it will not be something that the LTSA will be able to decide to implement on its own. Implementation will require building up and bringing along an entire ecosystem.

Link: http://blogs.ubc.ca/recordsinthechain/files/2018/08/Blockchain-Case-Study-_FINAL-1.pdf

Appendix B.4

Project Name: Blockchain Technology for Recordkeeping

Report Title: Blockchain for Recordkeeping: Help or Hype? Volumes 1 & 2

Collaborators/Writers/Authors: Victoria Lemieux, Darra Hofman, Mark Penney, Jessica Tung, Victor Liang, Steve Thompson, & Vikas Singh

Summary: This report in two volumes addresses the question of how blockchain technology, as an emerging technology, can be used for the benefit of Canadians. The report was funded by a grant from Social Science and Humanities Research Council (SSHRC) of Canada's Knowledge Synthesis Program.

Findings/Conclusions: The report concludes that blockchain technology could dramatically alter recordkeeping. Blockchain innovators envision the blockchain being entrusted with some of our most fundamental records. Proponents of blockchain recordkeeping point to the decentralized, allegedly immutable nature of the blockchain and the potential gains in transparency and efficiency when records are authenticated by code. However, there exists the possibility of significant risks to long-term authenticity of trustworthy digital records. There is a real need to enhance the relationship between the blockchain community and the archival science community. Specifically, archival science has developed theory and methods for the assessment of the accuracy, reliability and authenticity of records, as well as principles, standards and techniques of ensuring long-term authenticity and availability of records that could assist blockchain solution developers to build these features into their systems. Blockchain technology could change our paradigm for trusting records; instead of turning to trusted third parties, such as government registries, for evidence, we could find ourselves turning to the blockchain.

The vulnerabilities of blockchain technology do not make it useless. The biggest danger actually comes from blind trust in the blockchain from blockchain developers, lawmakers, law enforcement and the general public in this technology. By researching the risks, as well as the benefits, of blockchain technology, it will be possible to capitalize on the benefits while mitigating risks that come with this new recordkeeping technology.

Interdisciplinary research into blockchain, bringing legal, economics, archival, diplomatic, forensic, and computer and information academic researchers together with blockchain innovators, is a critical next step in blockchain recordkeeping. Canada is uniquely positioned to lead the way and benefit from the potential of blockchain recordkeeping.

Links:

Volume 1 http://blogs.ubc.ca/recordsinthechain/files/2018/06/FinalReport_Volume1.pdf

Volume 2 http://blogs.ubc.ca/recordsinthechain/files/2018/06/FinalReport_Volume2.pdf

Appendix C

Table 5: Some Examples of Types of Blockchain Risks

Risk: ***Core Processing Layer***	**Cause**	**Scope**	**Risk Mitigation Strategies**
Forks	Scalability/Governance	Primarily Public Blockchains	Governance models Blockchain design
Governance	Autonomous operating model	Primarily Public Blockchains	Use Consortium or private blockchain Governance model
Privacy leakage	Data linkage Transaction design flaw	Primarily public blockchains	Mixing Zero Knowledge Proofs
51% Attack	Colluding nodes	Blockchains using Proof of Work consensus mechanism	Prevent centralization mining power Monitor node behavior
Risk: Smart Contracts	***Cause***	***Scope***	***Risk Mitigation Strategies***
Transaction privacy leakage	Transaction design flaw	All smart contracts	Careful transaction design Use of encryption
Criminal smart contracts	Smart contract application	All smart contracts	Use permissioned blockchains Use blockchain intelligence services
Logical errors	Contract design flaw Failure to take account of all states	All smart contracts	Careful smart contract design Developer training & education
Smart contract vulnerabilities	Various (e.g.): *Call to the unknown* – the call function doesn't exist *Out of Gas send* – Fallback of the callee is executed	All smart contracts	Smart contract validation & testing Developer security training & education

	Exception disorder – irregularity of exception handling *Type casts* – type-check error in contract *Reentrancy vulnerability* – function is re-entered before termination *Field disclosure* – private value is published by the miner *Immutable bug* – Alteration of a contract after deployment *Coin lost* – sending coin to an orphan address *Stack overflow* – number of values in the stack exceeds 1024 bits (Ethereum smart contract limit) *Reentrancy error:* Attacker is able to repeat a process; recursive transaction loop without end		

About the Authors

Danielle Batista, B.A.R.M, MIS, is a PhD Student from the iSchool@UBC. Her research interests are digital diplomatics and records forensics, blockchain systems and smart contracts. She has 14 years of experience in records and information management. Her specialties are public records management, information systems development and implementation, creation/use of information governance policies, and records management training. She is an Archivist for the Federal Labor Prosecution Office in Brazil and also worked as an Archivist for the Federal District Prosecution Office and as an independent consultant for several organizations in Brasilia.

Darra Hofman, J.D., M.S.L.S., is a Ph.D. candidate at the University of British Columbia iSchool (School of Library, Archival, and Information Studies). Her research focuses on the intersection between records, technology, and human rights, with a special focus on blockchain technology and privacy.

Alysha Joo, MAS, MLIS, BA (hons.), is the Knowledge and Records Management Specialist at the Land Title and Survey Authority of British Columbia. Her research interests include information governance, digital preservation and blockchain technologies.

Victoria Lemieux is an associate professor of archival science at the iSchool and lead of the Blockchain research cluster, Blockchain@UBC at the University of British Columbia – Canada's largest and most diverse research cluster devoted to blockchain technology. Her current research is focused on risk to the availability of trustworthy records, particularly in blockchain record keeping systems, and how these risks impact upon transparency, financial stability, public accountability and human rights. Dr. Lemieux has organized two summer institutes for Blockchain@UBC to provide training in blockchain and distributed ledger technologies for undergraduate and graduate students from across UBC. She holds a doctorate from University College London (Archival Studies, 2002), and has been a Certified Information Systems Security Professional (CISSP) since 2005. She has received many awards for her professional work and research, including the 2015 Emmett Leahy Award for outstanding contributions to the field of records management, a 2015 World Bank Big Data Innovation Award, and both a 2016 Emerald Literati Award and 2018 Britt Literary Award for her research on blockchain technology. Dr. Lemieux is also a faculty associate at multiple units within UBC, including the Peter Wall Institute for Advanced Studies, Sauder School of Business, and the Institute for Computers, Information and Cognitive Systems.

The Foundation is a leading organization that that facilitates research, scholarship, and education for the information management profession.

The Mission of the Foundation is to provide current and relevant resources to information management professionals allowing them to advance the profession.

The Foundation is a non-profit corporation with 501(c)3 tax exempt status in the United States.

If you wish to fund any future research projects, please contact admin@armaedfoundation.org or visit the Foundation website www.armaedfoundation.org.

Additional Foundation financial and program information can be found at:

The National Database of Non-profit Organizations
http://www.guidestar.org/organizations/31-1556655/arma-international-educational-foundation.aspx