frontiers in Blockchain

REVIEW
published: 12 July 2019
doi: 10.3389/fbloc.2019.00005

Blockchain and Public Record Keeping: Of Temples, Prisons, and the (Re)Configuration of Power

*Victoria L. Lemieux**

School of Library, Archival and Information Studies, University of British Columbia, Vancouver, BC, Canada

This paper discusses blockchain technology as a public record keeping system, linking record keeping to power of authority, veneration (temples), and control (prisons) that configure and reconfigure social, economic, and political relations. It discusses blockchain technology as being constructed as a mechanism to counter institutions and social actors that currently hold power, but whom are nowadays often viewed with mistrust. It explores claims for blockchain as a record keeping force of resistance to those powers using an archival theoretic analytic lens. The paper evaluates claims that blockchain technology can support the creation and preservation of trustworthy records able to serve as alternative sources of evidence of rights, entitlements and actions with the potential to unseat the institutional power of the nation-state.

Keywords: blockchain, records, record keeping, trust, power

OPEN ACCESS

Edited by:
Massimo Bartoletti,
University of Cagliari, Italy

Reviewed by:
Marcella Atzori,
University College London,
United Kingdom
Jason Potts,
RMIT University, Australia

****Correspondence:***
Victoria L. Lemieux
v.lemieux@ubc.ca

Specialty section:
This article was submitted to
Non-Financial Blockchain,
a section of the journal
Frontiers in Blockchain

Received: *12 February 2019*
Accepted: *14 June 2019*
Published: *12 July 2019*

Citation:
Lemieux VL (2019) Blockchain and Public Record Keeping: Of Temples, Prisons, and the (Re)Configuration of Power. Front. Blockchain 2:5. doi: 10.3389/fbloc.2019.00005

1. INTRODUCTION

As a distributed ledger, blockchain technology is, at its heart, a record keeping technology. Without going into technical details of its operation, aspects of which will be discussed later in this paper, and which are quite varied across different blockchain platforms in any case, it is in large part due to the intended making and keeping of tamper-resistant and transparent recordings of transactions that is said to make blockchains trustworthy (Nakamoto, 2008; Peters and Panayi, 2016; Atzori, 2017). These characteristics are arguably what allow blockchain records to serve as a basis of trust (Vigna and Casey, 2019), in particular in human social, economic and political relations—the focus of this paper.

According to some, as a record keeping technology, blockchains could be truly revolutionary. They could reconfigure power away from nation states and traditional elites and redistribute it. One of the central mechanisms by which power may be reconfigured is by the use of blockchain technology to wrest control of states' monopoly over public record keeping (Markey-Towler, 2018). The central questions then become, in a world where governments, the supposed guarantors of trustworthy public record keeping, may no longer be trusted to deliver trustworthy public records, does blockchain technology offer a viable trusted alternative to state-backed record keeping? To whom is power redistributed in a world of blockchain record keeping and what kind of socio-political power dynamics may this configure?

This paper offers an archival theoretic discussion of these questions. Its central argument is that, though some proponents of blockchain technology make strong claims about offering a trusted alternative to the current public record keeping monopoly of nation-states, on close examination there are many aspects of how public blockchain record making and keeping currently operate-or are envisioned to operate-that raise questions about blockchains as trustworthy forms of public record keeping. Moreover, public blockchain record keeping tends to concentrate power in the hands of a few social actors—a techno plutocracy—without the guarantees and protections afforded by the rule of law and democratic principles of governance. Finally, in some cases blockchain technology's operation is premised upon the self-sovereignty of the individual when, in fact, social relations are interlinked by familial and community bonds, bonds which may be unsupported or require further development in blockchain public record keeping solutions.

To advance these arguments, the paper is organized into several sections. Section 1 discusses the historical relationship that exists between writing and record keeping, on the one hand, and institutionalized power, on the other hand. Section 2 discusses the basis of claims about the legitimacy of state-backed public record keeping with the power to confer rights and entitlements upon social actors within state-backed juridical frameworks and points to the similarity of some claims about public blockchain record keeping. In section 3, the paper addresses recent state-backed measures to "co-opt" blockchain record keeping into state frameworks for public record keeping and existing institutionalized power structures. Section 4 presents an archival theoretic analysis of the trustworthiness of blockchain record keeping, problematizing some of the claims made about the inherent trustworthiness of blockchain records and record keeping. Finally, section 5 explores the implications of blockchain-based self-sovereign identity and data self-sovereignty as an alternative form of public record keeping. The paper concludes with a call to address the shortcomings in designs and implementations of blockchain record keeping so as to be better able to realize the worthy vision of blockchains as offering alternative trustworthy public record keeping and a (re)configuration of power that enhances public trust and protects individuals and social groups from exploitation.

2. BUILDING TEMPLES: A BRIEF HISTORY OF POWER AND PUBLIC RECORD KEEPING

Public record keeping and writing, which enjoy a symbiotic relationship, have for centuries provided the foundation for society's institutional systems of government, education, and so on (Duranti, 1989a,b). Public record making relies upon the technology of writing, which is arguably one of the greatest inventions of human history (Robinson, 1995, p. 7). Moreover, the keeping of writings (i.e., record keeping), establishes and provides evidence of rights, entitlements and decisions that breathe life into society's juridical systems and socio-political and economic institutions (Latour, 1986; De Soto, 2000). Writing and record keeping together have configured and re-configured humanity's social institutions from the outset by putting agreements, laws, and commandments on record. According to H. G. Wells, writing, and associated processes of record keeping, made the growth of states larger than the old city states possible. He writes, "The command of priest or king and his seal could go far beyond his sight and voice and could survive his death" (Wells, 2005). Writing and record keeping extend human memory from the individual to the collective and social (Brothman, 2001). Moreover, it is through the "everyday techne" of writing and record keeping that the seemingly mundane task of inscribing and keeping ledgers constitutes and represents power relations and social negotiations (Latour, 1986; Orlikowski, 1992; Walters, 2002). Thus, though records contain data, they are not conceptually equivalent to data. Data embeds and conveys information; whereas, records embed and convey power.

As with all technology, those with the technological capability—the kings, the priests, the nation states, and more recently, global tech companies—have used writing and record keeping to grasp, exercise, and consolidate power, power which can always be used for good or ill. Who would disagree that the use of writing in state-funded education has not been socially beneficial? On the other hand, writing and record keeping also has been used throughout millennia to control and suppress: "Babylonian and Assyrian cuneiform, Egyptian hieroglyphs and the Mayan glyphs of Central America, carved on palace and temple walls, were used much as Stalin used posters about Lenin in the Soviet Union: to remind the people who was the boss, how great were his triumphs, how firmly based in the most high was his authority" (Robinson, 1995, p. 9). In recent times, the assembly of great repositories of records containing data—so called big data—has given rise to powerful platforms, such as Facebook and Google (Kenney and Zysman, 2016). These uses of writing and record keeping remind us that control over the recording of memory is at the heart of political and economic power (Derrida, 1996; De Soto, 2000). Where there is writing and records, there also have been "temples" of historical writings or houses of record keeping—archives and public registries—whether kept by priests in temples or nation states in public institutions of "cultural memory" (Posner, 1972; Duranti, 1989a,b). These houses of record keeping have preserved writings as a means of producing and reproducing social institutions and their embedded power relations beyond space and time (Jimerson, 2009). Such physical repositories funded as they were by powerful social institutions often held a special legitimacy as bastions of "The Truth," or at least, facts comprising assemblages of truth that could be extracted (Cunningham, 2017). Archival theorist Rand Jimerson invokes three metaphors for these houses of memory, or archives: temples, prisons, and restaurants. He writes,

> The temple reflects the power of authority and veneration. The prison wields the power of control. The restaurant holds the power of interpretation and mediation. These represent the trinity of archival functions: selection, preservation, and access. Archives at once protect and preserve records [the temple]; legitimize and sanctify certain documents while negating and destroying others [the prison]; and provide access to selected sources while controlling the researchers and conditions under which they may examine the archival record [the restaurant] (Jimerson, 2009, p. 2).

Invading marauders and those who have sought to topple existing power structures have long understood the power of houses of record keeping as seats of socio-political and economic power, and fought to seize or destroy them—from the destruction of the Library of Alexandria, to the capture of the archives during the US invasion of Grenada, to more recent destruction of records in Iraq and Afghanistan (see e.g., Posner, 1972; Seabury and McDougall, 1984; Zgonjanin, 2005; Deutch and Habal, 2018). Thus, to take aim at the function of the archives and record keeping, which many blockchain solution developers overtly do, is to take aim at the very seat of a political regime's (or its opponents') base of power.

Bitcoin exemplifies the use of record keeping—the ledger—as both a form of protest and path of resistance to existing power structures. The first block of the Bitcoin blockchain contains a reference to an article that appeared in the January 3rd, 2009 edition of The Times concerning the bailout of banks during the global financial crisis and the third block contains a tribute to a cryptography researcher associated with the Cypherpunk movement (Anduck, 2018). These entries in the Bitcoin public ledger allude to a belief in the use of cryptography and cryptocurrency as countering the misuse of power by society's elite—the 1%. This belief can be traced to intellectual roots in Ted Hughes' A CypherPunk Manifesto, which influenced a number of the early blockchain developers (Bandyopadhyay, 2018). In his manifesto, Hughes asserts,

> We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. . . The technologies of the past did not allow for strong privacy, but electronic technologies do. We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money (Hughes, 1993).

In a similar vein, in 2014 the president of Factom, a company developing blockchain technology, was quoted as saying,

> Factom creates permanent records that can't be changed later. In a Factom world, there's no more robo-signing scandals (referring to US mortgage foreclosures during the financial crisis). In a Factom world, there are no more missing voting records. In a Factom world, you know where every dollar of government money was spent. Basically, the whole world is made up of record keeping, and as a consumer, you're at the mercy of the fragmented systems that run these records. . . The dream of many is to extend the honesty inherent to an immutable ledger validated by math to chaotic, real-world interactions. By allowing the construction of unbounded ledgers backed by the blockchain (Higgins, 2014).

Projects, such as BitNation[1], which bills itself as providing governance as a service and jurisdictional sovereignty, seek to circumvent existing nation states to provide "do-it-yourself government services" (Atzori, 2015, p. 5), such as registration of marriage licenses, land transfers, and identities.

The above examples can be understood in the context of efforts throughout history led by those with less socio-political or economic power and authority to use writing and record keeping to resist social control or re-configure existing societal power relations (Foucault, 1980; Tyacke, 2001; Blouin and Rosenberg, 2012). Other examples of the use of writing and recording in resistance to power through records and record keeping can be seen in the application of freedom of information laws around the world to gain access to public records (Neuman and Calland, 2007; Lemieux and Trapnell, 2016), or controversially, leaking of documents to uncover state, corporate and elite abuse of power (e.g., Wikileaks, Anonymous) (Sifry, 2011). In Power/Knowledge, Foucault writes that there is no relationship of power without the means of escape or possible flight (Foucault, 1980). It is not just a question of one person or group having power or knowledge. Power and knowledge exist in dynamic relationship to one another. The person or group with less power can resist, can take power back, or change the power dynamic, because power and knowledge are intertwined.

Observers of blockchain technology have noted the revolutionary implications of blockchain record keeping's potential to reconfigure socio-political and economic power relations. In 2015, Swan saw blockchains as being as "fundamental for forward progress in society as Magna Carta or the Rosetta Stone" (Swan, 2015, p. viii). In a 2018 article in Newsweek, Paul Casey, co-author of the book the Truth Machine, is quoted as saying, "The entire global system of record keeping is going to go through a 5,000-years paradigm shift. . . We've tracked and checked records, and records are the foundational layer of economic exchange systems, they go right back to Sumerian tablets. We had centralized versions of that for 5,000 years. Now, we're doing a decentralized thing that is a game changer" (Piore, 2018). Brendan Markey-Towler, an Australian institutional economist, has observed that Blockchain technology unsettles existing centers of power because it allows everyone to keep records and update them by collective assent (Markey-Towler, 2018). This raises the question: could blockchain public record keeping unseat legitimate state-backed public record keeping, and by extension, states themselves? To answer this question, it is necessary to understand the basis of the legitimacy of public records and record keeping.

3. THE TEMPLE AS BESTOWER OF LEGITIMACY: THE BASIS OF TRUSTED PUBLIC RECORD KEEPING

Archival theorist Luciana Duranti has written of the basis of archives as trusted repositories of public records in Roman law. In the Justinian code, an archives (synonymous with an archival institution) is defined as *locus publicus in quo instrumenta deponuntur* (i.e., the public place where deeds are deposited), *quatenus incorrupta maneant* (i.e., so that they remain uncorrupted), *fidem faciant* (i.e., provide trustworthy evidence), and *perpetua rei memoria* sit (i.e., be continuing memory of that to which they attest) (Duranti, 1996, 2007, p. 447).

It is not only the deposit of public records in archival repositories—temples of records, if you will—that renders them

[1] https://tse.bitnation.co/

trustworthy and capable of serving as evidence of socio-political and economic rights and entitlements, but the fact that these repositories embody juridical power. The German jurist Ahasverus Fritsch first commented on this in 1664, observing that archival documents did not acquire their authenticity by the mere fact of being set aside in an archival repository but rather by the fact that the repository in which they were placed belonged to a public sovereign authority, that the officer depositing them was a public officer, that the documents were, by their placement in the archives, associated both physically (i.e., by location) and intellectually (i.e., by description) with related authentic documents, and that this association was meant to endure (Duranti, 2007, p. 448). For example, in ancient Rome, the *tabellio* was a government official who received, authenticated and kept records in a public archives, the *tabullarium*. Records produced from the *tabullarium* during litigation enjoyed special authority as evidence. Such documentary evidence, known as *instrumenta fides* or *instrumenta publica*, held such status that the party challenging them bore the burden of proving they were untrustworthy (Head, 2013, p. 914). Moreover, such was the power of public archives to legitimize records as trustworthy evidence that even those records not produced by the state, that is, even those of private origin, once they had been deposited in a public archives were deemed to be authentic (Duranti, 1989a). This legitimacy bestowed upon records by means of archival preservation came to be known as 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) and accorded special legitimacy under a juridical system (Head, 2013).

Thus, when the power and legitimacy of the state is diminished, so too is the power of the archives to legitimate evidence of rights and entitlements. Such rights and entitlements may, therefore, be challenged and even overturned, which, recursively, further diminishes the power of the state. This is most obvious in cases of war or revolution. For example, after Fidel Castro assumed political leadership in Cuba, many individuals who had held title to land under the existing regime lost that title when the old regime was toppled, which enabled the new regime to consolidate its power base (Fisher, 2014). Moreover, competing powers may establish archives that contain documentary evidence asserting different or competing versions of truth. In essence, this was the case with South Africa's Truth and Reconciliation Commission in which the supremacy of the state-backed national archives was challenged and alternative archives comprising both documentary and oral evidence were established (Hamilton et al., 2005). Similarly, in Canada, processes of Truth and Reconciliation involving the "decolonization" of Canada's First Nations peoples problematize the trustworthiness of government records as evidence of the lived-experience of Indigenous individuals and pave the way for new memory institutions that stand as challenges to the previously dominant representation of "facts" (TRC, 2018). Diminishment of the power and legitimacy of the state, and thus the evidentiary legitimacy of the records it holds, also derives from reduced public trust in the state and its officials seen over recent years (Levi and Stoker, 2000; Tolbert and Mossberger, 2006; Keele, 2007; Edwards, 2015). This growing mistrust leaves the door open for challengers to state-backed authority, challengers who may choose to offer more "trustworthy" alternatives to perceived untrustworthy state public record keeping as a more indirect modality of resisting state power and authority than a direct attack.

Analogies may be drawn between these processes and the rise of blockchains as challengers to existing power structures, including those of the nation state, through their role as new public notaries, public record keepers, and archives. Alston (2019, p. 14), for example, likens the system of rules that govern blockchains to constitutional systems: "The participants, or network nodes, in a given blockchain play the role of government," he writes, and "users of a given blockchain can be seen as constituents." In this emergent juridical system, which instantiates a new socio-political and economic order, code becomes law and a new *lex cryptographia* challenges existing legal frameworks (De Filippi, 2018; Yeung, 2019). As Markey-Towler (2018) observes, public record keeping has, for centuries, provided the foundation for society's institutional systems (i.e., government, education, and so on). Thus, blockchain, in staking a claim to disintermediate and replace the traditional public archives, registry, and notary (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" (Markey-Towler, 2018, p. 13).

Atzori (2017), however, questions the ability of blockchains to usurp nation-state legitimacy. She points out that open, permissionless blockchains have several limits for public administration and e-government. The first limit is that they can turn out to be weak and fragmented, while the second is that they do not necessarily provide for democratic government. Atzori makes the point that democracy is more complex than a set of rules established by core developers around consensus. It is, she asserts, as much about adequate quality and ability to participate, the legitimacy of procedures, protection of minority rights, freedom of participants, and equal opportunity to access decision making (Atzori, 2017, p. 8), Alston (2019, p. 16) makes similar arguments, pointing out that blockchain governance differs from democratic constitutional government in the lack of separation between legislative and judicial powers; that is, core developers both write the laws and decide upon their interpretation. Moreover, unlike in constitutional governments where constituents may dispute a law without having to revoke their citizenship, constituents (i.e., users of public blockchains) face high exit costs if they disagree with the governance rules: either they accept the new rules and continue to participate in the blockchain system, or they reject them and have to exit the blockchain system entirely (i.e., in cases of a "hard fork" in the blockchain). Current blockchain governance arrangements create a techno plutocracy that foments imbalances of power between developers and users and a tendency toward economic individualism over a common good (Gervais et al., 2013; Atzori, 2017). Since the legitimacy of blockchains as keepers of public records depends on the legitimacy of blockchain juridical systems, it would seem that public, permissionless blockchains still have a far way to go to be fully worthy of public trust to a degree that would topple the nation state as the dominant juridical system and public record keeper. Lawrence Lessig's warning is worth heeding: "To push the antigovernment button is not to teleport us to Eden. When the interests of government are gone, other interests take their place. Do we know what those interests are? And are we so certain they are anything better?" (cited in Atzori, 2015).

4. COOPTING BLOCKCHAIN RECORD KEEPING: THE DEFENSE OF STATE-BACKED PUBLIC RECORD KEEPING AGAINST DISRUPTION

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. These jurisdictions' motivation for passing such laws appear to be rooted in economics, however, rather than in an overriding concern for the creation and preservation of reliable and authentic records or fear of being overtaken as public record keepers by public blockchains as a form of challenge to state authority (State of Vermont, 2016). Thus, their actions are better explained as co-option of blockchain for public record keeping rather than as a consciously direct defense against a perceived threat to the legitimacy of the state as public record keeper. Nevertheless, the result is that by co-opting the power of blockchains and conferring state-backed legitimacy on blockchain public record keeping, these states avoid immediate disruption of their role as legitimate keepers of the public record.

As examples, a law passed in 2016 in the State of Vermont (2016), an act relating to miscellaneous economic development provisions, provides that a digital record electronically registered in a blockchain is to be considered authentic, provided that 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 if it is accompanied by the date and time at which the record entered the blockchain, the date and time at which the record was received from the blockchain, and evidence that the record was maintained in the blockchain in the usual and ordinary course of business.

There are several problematic aspects of the provisions of the Vermont legislation. The first is the question (and even irony) of who would be considered to be a "qualified person" pursuant to the act. Would it be the designers of the blockchain system? They could hardly be said to be disinterested but could be cross-examined under oath about the mode of record keeping in their ledger as many information professionals have been called to do (see e.g., California Public Utilities Commission and Consumer Protection and Safety Division, 2012). Or, should it be an independent third party, such as an auditor, or some state-appointed official, with greater disinterest but less direct knowledge of the system? Or, should it be a combination of these approaches? In any case, certification would rely on expertise that, though trusted, may not, in fact, be trustworthy. The jury is still out on how to build a legal foundation for certification of the authenticity of records generated in blockchain systems, but such standards of evaluation would provide some clarity about how to interpret legal provisions, such as those passed in Vermont. Another problematic aspect is the requirement for there to be a date and time of recordation. Some blockchain systems use timestamps, some do not, relying instead on the sequential ordering of transactions in the chain as a proxy for time. Even when a timestamp is used, it may rely on system generated time which may vary from calendar time, and moreover, may be subject to error or manipulation (Lemieux, 2016). To address this variance, some blockchains publish transaction hashes out to public media, such as newspapers or Twitter, to link the transaction order to calendar time (see e.g., Anduck, 2018). Similar to the Vermont law, a law passed by the State of Arizona (2017) gives recognition to smart contracts, conferring upon them the status of an electronic record, and specifying that a contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term. The provisions of the Arizona law do not make it clear, however, as to what should be considered to be a fully executed smart contract and when a smart contract should be considered to be fully in force. Following the norms and laws applicable to other types of contracts, a smart contract might be considered technically complete as a record (i.e., in effect) when it is digitally signed (and witnessed), validated, confirmed and entered into a blockchain ledger by a predetermined number of nodes; that is, when it can no longer be repudiated. Non-repudiation in this context is synonymous with confirmation of the transaction. There is no definitive answer to the question of how many nodes must update their copies of a distributed ledger before a transaction is considered confirmed; the answer will vary according to the design of the blockchain, for example, the type of consensus mechanism it uses and who operates the nodes that participate in validation and confirmation (Bitcoin Wiki, 2016). Not only does the Arizona law fail to provide guidance on when a smart contract should be considered fully executed and in force, the definition of smart contract it establishes adds confusion. The Act defines a smart contract as "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." To use the expression "that runs," as the Arizona law does, instead of "has run" might be likened to giving a draft contract full legal status, since, in a blockchain context, the expression does not imply a contract that has been validated and confirmed on a distributed ledger, and thus could be considered to be beyond repudiation.

The above discussion outlining difficulties with applying existing legal principles to novel blockchain-based records suggests that legislating the same presumption of authenticity for blockchain records as is given to more traditional forms of records kept by public bodies is premature. Indeed, this view is supported in a 2016 report prepared by the State of Vermont's own public archives at the time that the state's blockchain legislation was under discussion. The committee noted that further study is required before considering blockchains for the regular business of the State, and moreover, any application would certainly need to support rather than replace the existing records management infrastructure (Condos et al., 2016, p. 20). Despite the lack of maturity of the technology, some state law makers nevertheless seem intent on capturing the economic advantage that a permissive approach to assessment of the trustworthiness of blockchain records may bring. But, at what cost to the public record?

5. BLOCKCHAINS AS TRUSTED PUBLIC RECORD KEEPERS

The inability to trust supposedly trusted record keepers is not a new problem. While archives and public registries are supposed to be trusted repositories which, in liberal democracies, operate in the interests of "the people," in reality, there are many occasions when they have been shown to operate in the interests of powerful political and social elites that have their own interests in mind (Hamilton et al., 2005). Countless examples throughout history that one could point to exist but two recent examples will serve to illustrate the point. Archivist Verne Harris has written of how the South African National Archives became an instrument of the Apartheid regime, noting that many documents that would have provided evidence of human rights violations perpetrated by South Africa's Apartheid government, and which later came to light in oral testimony given to a South African Truth and Reconciliation Commission, were suppressed by the National Archives (Hamilton et al., 2005, p. 31). In a similar vein, British officials are said to have tampered with and falsified the historical record in many former colonies during the period of decolonization in order to avoid political and economic responsibility for some of the effects of colonization (Cobain, 2016). Nor has meddling with the public record necessarily stopped. On this activity, Ian Cobain writes in *The History Thieves*, of how documents relating to the involvement of the British SAS in the Indian military's 1984 attack on the Golden Temple in Amritsar were reviewed for transfer to the UK National Archives at Kew not as a means of identifying records of historical value but as an opportunity to weed out documents that contained embarrassing material about the government (Cobain, 2016, p. 147).

Indeed, the problem of lack of trustworthiness of legitimate public record keeping authorities is timeworn. This very problem gave rise to the seventeenth century theories and principles developed by Jean Mabillon which even today underpin the education of the archivist. Jean Mabillon was a French Benedictine monk and scholar of the Congregation of Saint Maur who is considered to be the father of the disciplines of paleography and diplomatics. In 1681 he wrote *De re diplomatica*, which laid out the tenants by which documents could be examined to determine their authenticity (Mabillon, 2004). Mabillon's text was a direct response to arguments over authenticity of documents held within the Abbey of St. Denis, one of the perceived legitimate record keepers of the time by virtue of being part of the dominate juridical system of the day—the Catholic Church. In describing his work, Mabillon rejected the notion that he should accept the legitimacy of documentary sources preserved in the Abbey simply by virtue of their placement there. Instead, he undertook a careful and scientific study of ancient documents over a period of 20 years with a view to being able to objectively determine which ones were authentic and which were inauthentic.

A similar attitude would serve well in the face of some blockchain developers' claims to offer trustworthy, immutable record keeping. If the existing institutions of public record keeping are to be replaced or overthrown, with implications for political power and juridical legitimacy, not to mention the rights, entitlements, claims and identities of individual people, then a critical examination of the evidentiary quality offered by any replacement systems of record keeping is in order so as to avoid swapping one untrusted system of record keeping with another. With this goal in mind, the observations that follow are based on an analysis of a number of different blockchain systems designed for record keeping use cases, such as land title recording, health record keeping and identity management, which draw upon the principles and techniques of documentary critical analysis (i.e., diplomatics) developed by Mabillon and elaborated upon by many archival theorists since then (see e.g., Duranti, 1998; Storch, 1998; Duranti and Michetti, 2012).

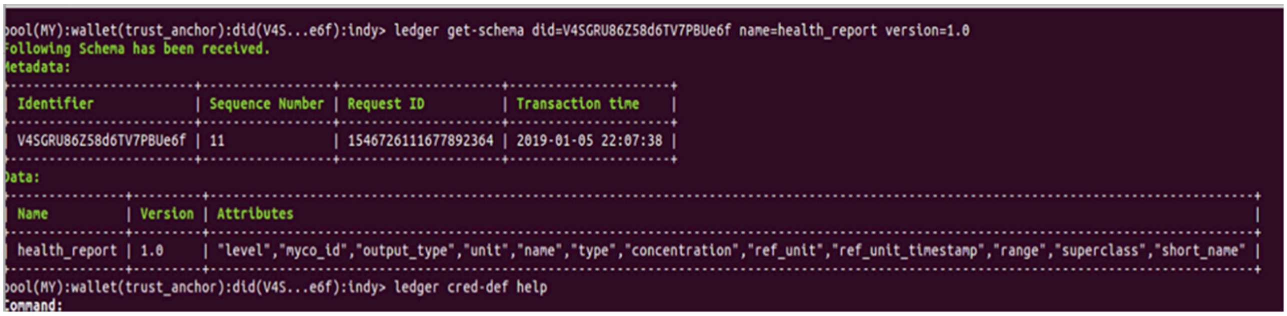
In distributed computing technologies records are distributed across infrastructural and system components. Though scattered, in most of these distributed systems—like cloud computing, for example—a record remains a largely unitary object: a single digital file (with attached metadata) or a composite Binary Large Object (BLOB). Most of a record's intellectual elements travel through space and time together, even if the software required to render the object accessible and interpretable does not (i.e., the object must be transformed in a way that renders it readable and presentable with new technology through processes of digital preservation).

This is not so in the case of records generated and recorded using blockchain technology. In blockchain-based record keeping, the intellectual aspects of the record are rendered as many distinct components, often existing in technical systems under autonomous and geographically distributed control. As a consequence, it may be very difficult to establish the authenticity of a record and to use it as trustworthy evidence of juridical acts. A high-level diplomatic analysis, drawing upon concepts first articulated by Mabillon, serves to illustrate the point.

The "Protocol" of a record typically begins with entitling—in modern terms the letterhead, containing the name, title, capacity, and address of the person who issued the document (Storch, 1998). This has no real equivalent in the blockchain world since most blockchains are designed to operate pseudonymously. In some cases, a blockchain address can serve the same purpose as entitling, at least in a partial way. The title of a record is an indication of the action of the subject (Storch, 1998). It is essential to identify and disambiguate one record from another, a crucial part of being able to establish authenticity (because you cannot prove an entity authentic if you cannot differentiate its identity from the identity of that which you are proving is inauthentic). This intellectual component is often completely missing from blockchain records, though it may be gleaned from some elements of the text if not encrypted. In some blockchains, this may be provided by the use of signed schemas that link the ledger record back to an ontology from which its semantic meaning can be inferred (Lemieux and Sporny, 2017). Dates are an important part of putting records that express contracts or rights and entitlements into force, and may refer to both the chronological date and the topical date or place where the document was issued (Storch, 1998). In blockchain record keeping solutions, dating of a record is often achieved by the embedded timestamp in the block header, but also by the publishing of hashes in external reference sources, such as newspapers or social media (Anduck, 2018). In contractual documents, the superscription is the mention of the first party by name (Storch, 1998). Of course, parties are not identified by name in blockchain transactions but are only known by their addresses which, depending on the type of blockchain and its design, may or may not be associated with a legal or digital identity. It is often the case, however, that identifying information may be embedded as clear text into transactions i.e., in OpCodes or in unused multisig fields (Sward et al., 2018). The inscription, in an epistolary or letter form, is the name, title, and address of the addressee (Storch, 1998). In a contractual document, it is the mention by name of any party but the first party. Similar to identification of first parties, other parties in a record are not identified by name in blockchain transactions but are only known by their blockchain addresses, unless such information has been specifically inserted into a blockchain transaction by some means. The subject of a record—often preceded in modern documents by the indicator, "in reference to" or "re" (Storch, 1998)—is often only identified by inference in blockchain solutions, that is, by means of a blockchain only being used for a single purpose, such as supply chain management in the production of coffee beans, or because some explanatory cleartext has been embedded into a transaction (see e.g., Flores et al., 2018).

The written body of a document usually contains a preamble and other elements, such as clauses (Storch, 1998). Preambles typically provide the motivation for the action, and its ethical or juridical principle (Storch, 1998). In modern documents this section may contain a citation of the laws or regulations which pertain to the document or mandate its creation (Storch, 1998). It is not found in records entered into most blockchain solutions, unless embedded into smart contracts or transactions using opcodes or unused multisig fields (Flores et al., 2018). Notifications communicate that the transaction has been communicated to interested parties that must be made aware of its real-world outcomes (Storch, 1998). It usually begins with the phrase, "be it known" or "know you" (Storch, 1998). In blockchain records, this is not explicitly included in the intellectual content of the record; rather, it may be implied by the act of entering a "proof of fact" into the ledger, as in the case of an artwork that an individual may wish to assert is their creation and for which they are claiming intellectual property rights or other provenance tracking use case (see e.g., Kim and Laskowski, 2018). Also, not evident in blockchain records is the exposition—the narration of the concrete and immediate circumstances generating the act and/or the document (Storch, 1998). In contemporary documents it often begins with "whereas" (Storch, 1998). The part of the record known as the disposition contains the expression of an author's will or judgement and communicates the nature of the action and the function of the document. This is often not evident in blockchain records either, which only show that an act has been carried out. It must often be inferred from supporting documents kept elsewhere (Flores et al., 2018). In some cases, explanatory text may be embedded in opcode/multisig fields but often this is just a hash link out to supporting documents (Flores et al., 2018; Sward et al., 2018), as one might expect of a simple ledger. Without this element the semantics of the record cannot be determined or instantiated, and its usefulness as evidence is limited (since it is impossible to determine what action the document actually represents without reference to the supporting documents). Finally, most traditional records contain formulaic phrases—called clauses—which ensure the execution of an act, guarantee its validity, protect against violation, preserve the rights of third parties, and indicate the means by which the document has value as evidence (Storch, 1998). Clauses also enunciate the means used to validate the document and guarantee its authenticity. In blockchain record keeping, this is handled very differently, being almost entirely determined by the consensus mechanism and how it operates to ensure records are valid and well-ordered before the ledger is updated (see e.g., Narayanan et al., 2016).

The eschatocol of a record contains the elements which authenticate the document: the means of its validation, an indication of responsibilities for documentation, and the final formulae (Storch, 1998). In this aspect of the intellectual components of a blockchain record, it is possible to see many differences from traditional paper or digital records. Traditionally, records contain attestations, which are a means used to validate a document. These usually take the form of the signature of those who took part in issuing it: the author, writer, and countersigner (Storch, 1998). In blockchain records, however, attestations take the form of the digital signature that the addresser of a transaction produces by signing the transaction with their private key. In traditional documents, there may also be a qualification of signature that will mention the title and official or juridical capacity of the signer (e.g., Queen's representative, President of the Republic, etc.) (Storch, 1998). This is usually not provided in blockchain record keeping, since blockchain systems operate pseudonymously. However, in some blockchains, such as Hyperledger Indy, where there are "Trust Anchors" and "Issuers" of credentials, this type of attestation may be represented by the public key of the trusted issuer of a credential (see **Figure 1** and Hyperledger Indy, 2018) Traditional documents may also contain secretarial notes—the initials of the typist, mention of enclosures, and an indication that other persons have received copies of the document (Storch, 1998). Such information may be found in opcodes or the use of unused signature fields (Sward et al., 2018). Formal public documents are also known to contain *formula perpetuitatis* declaring that the rights put into existence by the document are not circumscribed by time (Storch, 1998). In blockchain ledgers, this aspect is implied by the very act of recording a transaction on an "immutable ledger." Finally, traditional records will often end with a corroboration that enunciates the means used to



```
ool(MY):wallet(trust_anchor):did(V4S...e6f):indy> ledger get-schema did=V4SGRU86Z58d6TV7PBUe6f name=health_report version=1.0
ollowing Schema has been received.
etadata:
+------------------------+-----------------+---------------------+---------------------+
| Identifier             | Sequence Number | Request ID          | Transaction time    |
+------------------------+-----------------+---------------------+---------------------+
| V4SGRU86Z58d6TV7PBUe6f | 11              | 1546726111677892364 | 2019-01-05 22:07:38 |
+------------------------+-----------------+---------------------+---------------------+
ata:
+---------------+---------+----------------------------------------------------------------------------------------------------------------------------------------+
| Name          | Version | Attributes                                                                                                                             |
+---------------+---------+----------------------------------------------------------------------------------------------------------------------------------------+
| health_report | 1.0     | "level","myco_id","output_type","unit","name","type","concentration","ref_unit","ref_unit_timestamp","range","superclass","short_name" |
+---------------+---------+----------------------------------------------------------------------------------------------------------------------------------------+
ool(MY):wallet(trust_anchor):did(V4S...e6f):indy> ledger cred-def help
ommand:
```

FIGURE 1 | Example of a credential schema signed by an issuer in Hyperledger Indy (source: original screenshot for Hyperledger Indy blockchain prototype).

validate the document and guarantee its authenticity (Storch, 1998). In blockchain record keeping, this may be spelled out in a whitepaper or other technical document that explains how the system operates, specifically, an explanation of the consensus mechanism (see e.g., Nakamoto, 2008). In Bitcoin, this may also be represented by SegWit which includes witness data stored at the end of a transaction as a list (Trubetskoy, 2017).

The point of this analysis is not to hold blockchain records to the same standard as medieval or even contemporary record making and keeping, nor to find blockchain records wanting if they lack elements of early documentation. Rather, the purpose is to note that many intellectual elements of records traditionally used to understand and authenticate them have been transformed by the application of blockchain technology. It is necessary, therefore, to critically analyze blockchain records, just as Mabillon studied medieval records, in order to be able to determine their authenticity and trustworthiness. Blanket statements about the reliability and authenticity of blockchain records are likely to be inaccurate or unsatisfactory until this analytic work is done.

With respect to accuracy of records, evidence supports the assertion 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. Concern about the accuracy of records comes as a result of claims about the accuracy of blockchain record keeping 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 of the accuracy of the original records, the security of the record's transmission to the blockchain, and the ongoing integrity of the records to ensure, at the point of creation, or subsequently determined through examination of the records, would need to be made. With respect to reliability, there may exist in any given blockchain solution, a number of problematic aspects of the processes of records creation, any of which may impact upon the reliability of ledger records. The degree of reliability of records often is based on three key factors: (1) the degree of control exercised over the procedure of creation, (2) the degree of control exercized by the authors, and (3) the degree of completeness of the documents themselves (Duranti, 2007). 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, the introduction of blockchain technology presents a new dimension that is not yet fully incorporated procedurally (Flores et al., 2018). To illustrate, in the pilot of a blockchain system for land transaction recording in Brazil, the blockchain record keeping system was running in parallel to the existing registry system. In addition, the pilot involved transcribing existing records into the new blockchain ledger. We noted that 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 record (Lemieux, 2017; Flores et al., 2018).

In terms of the authority of the records creator, 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 it (e.g., able to consent to use of health data). Uncertainty surrounding the question of competence exists in blockchain record keeping environments because addresses might not be explicitly linked to the legal identity of a competent juridical authority (Nakamoto, 2008; Flores et al., 2018). Indeed, in permissionless, 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 (Nakamoto, 2008; Narayanan et al., 2016). In many cases (e.g., Monero[2]), 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 (Miers, 2018). As a result, in such systems, it is safe to say that 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 two 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 (Hofman et al., 2018). Another approach is 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

[2] https://www.getmonero.org/

with this information, preferably in encrypted form to protect personally identifiable information and privacy (Flores et al., 2018). Each design choice has its pros and cons in relation to the operation of the system, and compliance, for example, with privacy regulations.

A second issue concerning competence relates to proving that a transacting party is, indeed, competent to engage in a transaction. To the best of our knowledge, this is not a determination that can be made simply by examining the records or the record keeping system itself, whether or not it is a blockchain record keeping system (Lemieux, 2017). It must be determined by examining facts surrounding the context of records creation (Flores et al., 2018). Typically, however, in a traditional record keeping environment, attestations about the competence of the transacting party are made by means of witnessing the signature (Storch, 1998). 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) (Lemieux, 2017; Flores et al., 2018).

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 record keeping environment as to whether transactions expressed as smart contracts should be considered complete when a transaction record is digitally signed, when that record is validated 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. These are important distinctions, 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 record keeping.

With respect to authenticity—the trustworthiness of a record as a record—most blockchain solution developers understand authenticity in terms of integrity (Higgins, 2014; Lemieux, 2016). 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" (Cohen, 2015, p. 357–358). Indeed, it is usual for record keepers 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 over long periods of time (ISO/IEC, 2012). 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 subsequently check the integrity of the record (Lemieux, 2016).

Blockchain systems typically miss instantiating the archival bond as well. The archival bond establishes the unique identity of a record by linking the content of a document to the context of the juridical transactions that give rise to the record's existence, and to other records created in the same context (Cencetti, 1970). It is the link back to the source of a record's power. This linkage also enables a record to serve as evidence of the juridical context to which it is connected. In traditional, centralized digital record keeping systems, the archival bond is instantiated by associating descriptive metadata, such as a classification code that intellectually connects the record 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 and the provision of evidence. 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. Contextual information needed to establish the provenance (in an archival sense) and unique identity of ledger records therefore may not exist or be disconnected from the records (Lemieux and Sporny, 2017), which ultimately may render the information quite useless as evidence. There are ways to instantiate the archival bond in blockchain systems to overcome this weakness: Lemieux and Sporny (2017) 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. Another solution that has been used is to apply 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 (Flores et al., 2018). 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 application 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 there is no 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 (Möser et al., 2018;

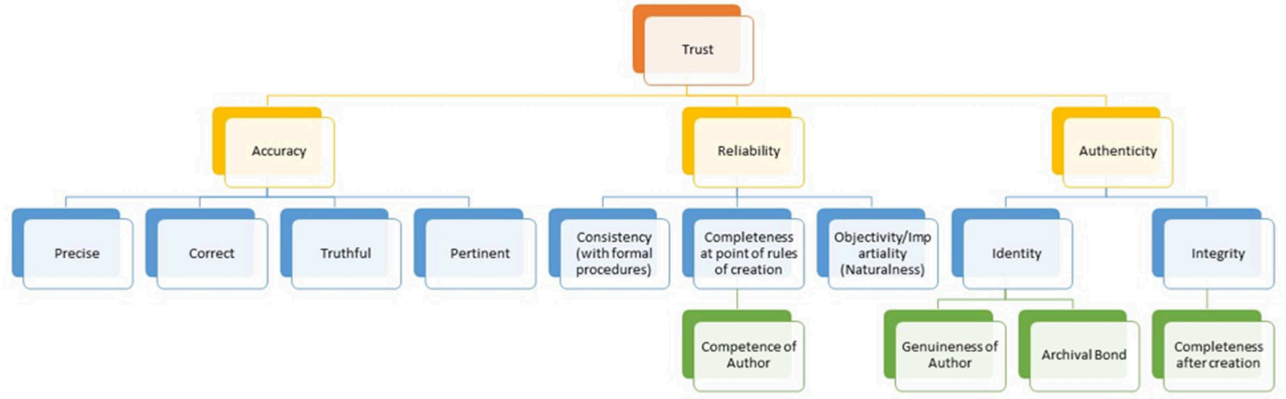

Trust
Accuracy
Reliability
Authenticity
Precise
Correct
Truthful
Pertinent
Consistency (with formal procedures)
Completeness at point of rules of creation
Objectivity/Impartiality (Naturalness)
Identity
Integrity
Competence of Author
Genuineness of Author
Archival Bond
Completeness after creation

FIGURE 2 | A taxonomy of key archival concepts and their relationship to trust (source: reproduced from Hofman et al., 2018).

Naqvi, 2018). 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 record keeping system, since such systems routinely employ identification and authentication as part of their design.

As the above analysis suggests, many of the traditional methods which record creators and keepers have used to assure the accuracy, reliability and authenticity of records to best enable records to serve as trustworthy evidence have not yet been adapted to blockchain record keeping (see **Figure 2**). Where previously the evidentiary quality of records was aided by physically signing and dating documents, registering them, and placing them in proximity to one another within a file folder or registry, in a blockchain environment, the signatures are digital, dates are replaced with computer-generated timestamps, registration is transformed into cryptographic hashes, and physical proximity of records becomes linked transactions, chained together into blocks over a decentralized network (Lemieux, 2018). Transformations in the modality of records creation and keeping require a rethinking of what is required for the production of accurate, reliable and authentic records using blockchain technology. At this point in time, archives and records professionals are only beginning to ponder this.

6. A SELF-SOVEREIGN FUTURE: FROM TEMPLES TO PRISONS?

The association of traditional archives and public registries with existing, often mistrusted, power structures has led many to call for a reconfiguration of record keeping, whether public or private, from a centralized model to a radically decentralized model that puts ownership, custody and control of records into the hands of individuals, a model that some refer to as data self-sovereignty or informational self-determination (Allen, 2016; Baars, 2016). This has found greatest expression in calls for the protection of individual's personal privacy, as in Hughes' Cypherpunk Manifesto, and more recently, Christopher Allen's (2016) ten principles of self-sovereign identity, as a direct response to the aggregation and exploitation of individuals' personally identifiable information.

In his essay, "Life with Alacrity", Allen (2016) recounts the history of identity on the internet in four phases: (1) the Internet's early days of centralized authorities who became the issuers and authenticators of digital identity (e.g., IANA, which determined the validity of IP addresses and ICANN, which arbitrated domain names); (2) beginning in 1995, certificate authorities (CAs) that helped Internet commerce sites prove identity; (3) the establishment of hierarchies within these organizations; and (4) the establishment of root controllers that could confer rights upon organizations to each oversee their own hierarchy. Allen points out that gradual decentralization of control of digital identity in the online world did not truly decentralize power, however, because users remained beholden to a single root authority that could deny their identity or even confirm a false identity (Allen, 2016). With the self-sovereign identity that blockchain enables, Allen sees the possibility of escaping reliance upon such root authenticators of identity.

Similarly, archival software developer Peter Van Garderen (2016) has put forth a vision of self-sovereign data and posited the notion of "decentralized autonomous collections" (DACs). Van Garderen defines DACs as "a set of digital information objects stored for ongoing re-use with the means and incentives for independent parties to participate in the contribution, presentation, and curation of the information objects outside the control of an exclusive custodian." Van Garderen's proposal sees DACs as an antidote to a number of the problems associated with traditional, centralized institutional repositories: shortage of resources, political interference, and elitism. For Van Garderen, blockchain technology has the potential to displace traditional institutional archives as curators of digital content (Van Garderen, 2016).

Whether blockchain platforms and solutions as currently implemented can easily fulfill the vision of providing individuals with the true power of meaningful data self-sovereignty, informational self-determination and political exit remains an open question. So far, there are open source or proprietary blockchain platforms in which individuals may choose to record transactions (e.g., BitNation). While individuals may choose to use a public blockchain to record their marriage certificates, land titles, or other documents rather than a traditional public registry, the problem is that this may be where choice ends. Once relying upon these systems, there may be no opportunity for individuals to remove their documentation to another platform or to exercise a "right to be forgotten" (Gabison, 2016), particularly if they disagree with the rules of governance (Alston, 2019). These solutions lack both the means to give users portability—the notion that information and services about identity [or personally identifiable information (PII)] must be transferable—or support for systems interoperability—the notion that individuals' identities (or PII) must be as widely usable by them as possible. Thus, individuals may be as locked in as they would be had they entered their data into a traditional repository operated by a central authority, perhaps even more so, as at least traditional centralized repositories fall under the purview of an array of privacy laws and regulations that require "information controllers" to meet specified requirements for processing of PII and provide "data subjects" with some rights and protections. Allen (2016) explains the problem that arises when identity records are held and authenticated by a singular third-party entity: such entities can disappear—and on the Internet, most eventually do. Outside of the online world, political regimes change and users may be forced to flee or move to different jurisdictions, leaving behind identity records. Allen argues, therefore, that a twenty-first century digital identity system must make authentic identity information widely available, crossing international boundaries to create global identities, without losing user control (Allen, 2016). The key is to give individuals ownership, custody, control, and choice—real choice.

These challenges cannot be overcome with existing blockchain governance arrangements. Angela Walch (2015) notes that even public blockchain platforms and systems are run by a small cadre of developers who, despite the decentralized nature of blockchain technology, often assume the mantel of and wield an increasing amount of power. Walch, observes of Bitcoin that it operates in a rather contradictory way—it is decentralized in some ways but not in others and because there is no "official" power structure, it is not possible to hold those in power accountable for their actions (Walch, 2015). Private or consortium-style blockchains may be even less likely to encourage portability and interoperability. Indeed, some solutions may actively discourage such capabilities for economic reasons (i.e., protecting intellectual property, client "capture," etc.). Put simply, it may not be in the interests of those who currently hold power to reconfigure and redistribute power out into the hands of individuals. As in so much of the case with blockchain technology, the solution may lie in coming up with creative ways to incentivize these socio-economic actors to push power out to the edges, but this has not happened yet.

Thus, as Atzori posits, there is a real danger of a future state emerging that looks like Neal Stephenson's "Franchulates" (Atzori, 2015; Swan, 2015). Franchulates are a combination of "franchise" and "consulate" in which public policy has been replaced by business membership and private corporations have replaced the State in all its functions, competing with each other to provide goods and services (Atzori, 2015). Atzori paints a bleak picture of this future state, suggesting that it would disrupt nation-state constitutions and deprive citizens of their rights (Atzori, 2015). Atzori concludes that: "It is the conscientious application of principles and rights enshrined in law that can really empower individuals—rather than the privatization of government services through market driven decentralized platforms" [(Atzori, 2015), p. 32].

Even if a Franchulate model is avoided, and power is redistributed successfully to individuals who are self-sovereign owners of their own identities and data, there is another challenge that rears its head: persistence—identities should last forever. Though private keys might need to be rotated and data might need to be changed, the identity should remain. Allen (2016) suggests that this goal may not be entirely reasonable in the fast-paced online world, so at the least identities should last until they've been outdated by newer identity systems. In addition, he suggests that users should be able to dispose of an identity if they wish, and claims based on identities should be modified or removed as appropriate over time in order to respect the "right to be forgotten" (Allen, 2016). There are two interconnected aspects to this challenge: (1) what should be made persistent and be preserved, and who decides, and (2) how to achieve persistence and for how long.

On the question of what should be made persistent and preserved, and who decides, Allen places the rights of users above all others. As such, the user should, at all times, decide how long an identity would last and how and when to dispose of it. This assumes that users are always competent to make those decisions, and that such decisions are always well-planned. As the recent case of crypto-currency exchange QuadrigaCX CEO's sudden death reveals, this may not be a wise assumption to make, since none of us can predict the future (De, 2019). If we suddenly become unable to manage our private keys, those who depend upon our identities or the claims supported by our identities, may be left stranded. We live in a world of relationships, a network of interdependent social, economic, and political relationships that are both created and inextricably bound together by records. Thus, if a user decides to dispose of an identity (or data) but another identity has a dependency on that identity (or data), ways must be found to allow for the continuation of the identity (or data) that has the dependent relationship. An example might be the dependence of a child's citizenship on the persistent identity (and citizenship documentation) of a parent. Moreover, there are not just hereditary or familial relationships, but community relationships to consider as well. A question arises as to how the interests of individual users should be weighed against those of the community. Different social groups will have very different answers to the question. For example, perpetrators of serious crimes may wish to assert a "right to be forgotten" but some may say that a broader social good is served by remembering the crimes of these individuals. Archivists also typically wrestle with the question of a future state "collective" interest in the preservation of cultural memory, but different groups may have different requirements for authenticity and evidentiality of social memory depending on their experience of the trustworthiness of the dominant culture (Battley, 2019). How might these interests figure into the mix?

Even assuming society can answer these questions, if individuals hold and control access to their own identities and personal information, the technical challenges of digital preservation will be great, since current models of digital preservation, such as the Open Archival Information System (ISO/IEC, 2012), are premised upon archival documents passing across "the archival threshold" into that special, centralized place where they will become inviolate and immutable memorials of human activity (i.e., archives). There are no guarantees that particular blockchain platforms will still be operative or even exist in the future (Atzori, 2015). DuPont and Maurer (2015) further point out with respect to smart contracts that if the electronic network were shut off, or if everyone moved on to a new system, there is no backup to establish the existence (or execution) of these contracts. What happens to notions of archives as place and all the technical tools, techniques, principles, and practices that are premised upon this notion, when the conceptual framework of data ownership, custody, and control is entirely flipped on its head? There will be a need to radically rethink and transform digital preservation concepts for use in a world of data self-sovereignty and self-determination or be faced with a fragmented and confused public record with attendant possibilities for the unraveling of social, political, and economic cohesion. Collectively, we may be inclined to put off thinking about these issues; however, to avoid negative unintended consequences for the institutions that hold human social relations together, it would be better if we think about them now lest we find ourselves in record keeping prisons of our own making.

7. CONCLUSION

This paper has discussed blockchain technology as a record keeping system, linking record keeping to power of authority, veneration (temples), and control (prisons) that configure and reconfigure our social, economic, and political relations. It has discussed the ways that some blockchain developers construct blockchain technology as a mechanism to counter institutions and social actors that currently hold power, but whom are nowadays often viewed with mistrust. This analysis has sought to problematize claims that blockchain systems, at least in their current form, inherently address the ills of public record keeping, identifying shortcomings in the design, implementation and governance of blockchain platforms that fall short of the ideal of trustworthy public record keeping. This is not to suggest that existing public record keeping is without flaws, and that blockchain technology should be jettisoned as a possible means to address such flaws. However, while there are certainly many problems with existing public record keeping, especially in predatory states, and because of the privacy and security issues to which centralized record keeping gives rise, what the analysis presented in this paper suggests is that the road ahead for blockchain public record keeping is only partially constructed and requires major ongoing construction efforts to produce records that would be sufficiently trustworthy to truly serve as effective alternatives to state-backed public record keeping, or in other cases, to challenge the monopoly of the state over this function. Despite claims to the contrary, public blockchains also currently lack the juridical legitimacy needed to convey power, rights and entitlements and confer authenticity upon records simply by virtue of the records' addition to the ledger in the same way that nation states have been able to confer a presumption of authenticity upon public records. Only time will tell if one or more of the public blockchains is able to gain the juridical power, authority, and veneration needed to become a new temple of public record keeping.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

Allen, C. (2016). *The Path to Self-Sovereign Identity*. Life with Alacrity [blog]. Available online at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Alston, E. (2019). *Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets*. Working paper 2019.003. Center for Growth and Opportunity, Utah State University, Logan, UT.

Anduck (2018). *Blockchain in Words*. Available online at: https://bitcoinstrings.com

Atzori, M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*

Atzori, M. (2017). *Blockchain Governance and the Role of Trust Service Providers: The TrustedChain® Network*. Available online at: https://trustedchain.it/wp-content/uploads/2017/11/ATZORI_-TrustedChainWhite-Paper.pdf

Baars, D. (2016). *Towards Self-sovereign Identity Using Blockchain Technology* (Master's thesis). University of Twente, Enschede, Netherlands.

Bandyopadhyay, P. (2018). The origin of blockchain–from cypherpunks to Satoshi to IBM. *Medium*. Available online at: https://medium.com/datadriveninvestor/cypherpunks-to-satoshi-to-ibm-819ebcfdd674

Battley, B. (2019). Archives as places, places as archives: doors to privilege, places of connection or haunted sarcophagi of crumbling skeletons? *Arch. Sci.* 19, 1–26. doi: 10.1007/s10502-019-09300-4

Bitcoin Wiki (2016). *Confirmation [wiki]*. Available online at: https://en.bitcoin.it/wiki/Confirmation

Blouin, F. X. Jr., and Rosenberg, W. G. (2012). *Processing the Past: Contesting Authority in History and the Archives*. Oxford: Oxford University Press.

Brothman, B. (2001). The past that archives keep: memory, history, and the preservation of archival records. *Archivaria* 51, 48–80.

California Public Utilities Commission and Consumer Protection and Safety Division (2012). Rebuttal Testimony to Pacific Gas and Electric Company's Response to the Consumer Protection and Safety Division's Report: Records Management With the Gas Transmission Division of PGE Prior to the Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California.

Cencetti, G. (Ed.). (1970). "Il fondamento teorico della dottrin archivistica," in *In Scritti Archivistici* (Rome: Il Centro di Recerca), 7–13.

Cobain, I. (2016). *The History Thieves: Secrets, Lies and the Shaping of a Modern Nation*. London: Portobello Books.

Cohen, F. (2015). "A tale of two traces–diplomatics and forensics," in *IFIP International Conference on Digital Forensics* (Cham: Springer), 3–27.

Condos, J., Sorrell, W. H., and Donegan, S. L. (2016). *Blockchain Technology: Opportunities and Risks*. Available online at: http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf

Cunningham, A. (2017). "Archives as a place," in *In Currents of Archival Thinking*, eds H. MacNeil and T. Eastwood (Toronto, ON: Libraries Unlimited), 53–80.

De Filippi, P. (2018). *Blockchain and the Law: The Rule of Code*. Boston, MA: Harvard University Press.

De Soto, H. (2000). *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*. New York, NY: Basic Civitas Books.

De, N. (2019). Quadrigacx owes customers 190 million court filing shows. *Coindesk*. Available online at: https://www.coindesk.com/quadriga?creditor?protection?filing

Derrida, J. (1996). *Archive Fever: A Freudian Impression*. Chicago, IL: University of Chicago Press.

Deutch, J., and Habal, H. (2018). The syrian archive: a methodological case study of open-source investigation of state crime using video evidence from social media platforms. *State Crime J.* 7, 46–76. doi: 10.13169/statecrime.7.1.0046

DuPont, Q., and Maurer, B. (2015). *Ledgers and Law in the Blockchain*. Kings Review. Available online at: http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/

Duranti, L. (1989a). The odyssey of records managers: part 1: from the dawn of civilization to the fall of the roman empire. *Inform. Manage.* 23, 3–11.

Duranti, L. (1989b). The odyssey of records managers: part 2: from the middle A. *Inform. Manage.* 23:3.

Duranti, L. (1996). Archives as a place. [Paper presented at a half day seminar in Sydney on 19 October 1995.]. *Arch. Manuscripts* 24, 242–255.

Duranti, L. (1998). *Diplomatics: New Uses for an Old Science*. Lanham, MD: Scarecrow Press.

Duranti, L. (2007). Archives as place. *Arch. Soc. Stud.* 1, 445–466.

Duranti, L., and Michetti, G. (2012). "Archival method," in *Archival Multiverse*, eds A. Gilliland, S. McKemmish, and A. Lau (Victoira: Monash University Publishing), 75–95.

Edwards, M. (2015). "The trust deficit-concepts and causes of low public trust in governments," in *United Nations Committee of Experts on Public Administration, Fourteenth Session* (New York, NY), 20–24.

Fisher, D. (2014). *Cuba Opening Could Reopen Fight Over Billions in Seized Property*. Jersey City, NJ: Forbes.

Flores, D., Lacombe, C., and Lemieux, V. (2018). *Real Estate Transaction Recording in the Blockchain in Brazil (RCPLAC-01)–Case Study 1*. Available online at: https://blogs.ubc.ca/recordsinthechain

Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*. New York, NY: Pantheon.

Gabison, G. (2016). Policy considerations for the blockchain technology public and private applications. *SMU Sci. Tech. L. Rev.* 19:327. Available online at: https://scholar.smu.edu/scitech/vol19/iss3/4

Gervais, A., Karame, G., Capkun, S., and Capkun, V. (2013). Is bitcoin a decentralized currency? *IEEE Secur. Privacy* 12, 54–60. doi: 10.1109/MSP.2014.49

Hamilton, C., Harris, V., Taylor, J., Pickover, M., Reid G., and Saleh, R. (eds.). (2005). *Refiguring the Archive*. Dordrecht: Springer.

Head, R. C. (2013). Documents, archives, and proof around 1700. *Hist. J.* 56, 909–930. doi: 10.1017/S0018246X12000477

Higgins, S. (2014). Factom outlines record-keeping network that utilises bitcoin's blockchain. *Coindesk*. Available online at: https://www.coindesk.com/factom-white-paper-outlines-record-keeping-layer-bitcoin

Hofman, D., Batista, D., and Lemieux, V. L. (2018). *Centre of Excellence for the Prevention of Organ Failure (Proof)–(RPCCA-01)–Case Study 1*. Available online at: https://blogs.ubc.ca/recordsinthechain

Hughes, E. (1993). *A Cypherpunk's Manifesto*. Available online at: http://www.activism.net/cypherpunk/manifesto.html (accessed August 3, 2004).

Indy, H. (2018). *Getting Started With Indy*. Available online at: https://buildmedia.readthedocs.org/media/pdf/hyperledger-indy/docs/hyperledger-indy.pdf

ISO/IEC (2012). *ISO 14721: 2012–Space Data and Information Transfer System–Open Archival Information System (OAIS)–Reference Model*. Geneva: ISO.

Jimerson, R. C. (2009). *Archives Power: Memory, Accountability, and Social Justice*. Chicago, IL: Society of American Archivists.

Keele, L. (2007). Social capital and the dynamics of trust in government. *Am. J. Polit. Sci.* 51, 241–254. doi: 10.1111/j.1540-5907.2007.00248.x

Kenney, M., and Zysman, J. (2016). The rise of the platform economy. *Issues Sci. Technol.* 32, 61–69. Available online at: https://issues.org/the-rise-of-the-platform-economy/

Kim, H. M., and Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intell. Syst. Account. Finance Manag.* 25, 18–27. doi: 10.1002/isaf.1424

Latour, B. (1986). Visualization and cognition. *Knowl. Soc.* 6, 1–40.

Lemieux, V. L. (2016). Trusting records: is blockchain technology the answer? *Records Manage. J.* 26, 110–139. doi: 10.1108/RMJ-12-2015-0042

Lemieux, V. L. (2017). Evaluating the use of blockchain in land transactions: an archival science perspective. *Eur. Property Law J.* 6, 392–440. doi: 10.1515/eplj-2017-0019

Lemieux, V. L. (2018). "The future of arhives as networked, decentralized, autonomous and global," in *Archival Futures*, ed C. Brown (London: Facet Publishing), 7–13.

Lemieux, V. L., and Sporny, M. (2017). "Preserving the archival bond in distributed ledgers: a data model and syntax," in *Proceedings of the 26th International Conference on World Wide Web Companion* (Perth: International World Wide Web Conferences Steering Committee), 1437–1443.

Lemieux, V. L., and Trapnell, S. E. (2016). *Public Access to Information for Development: A Guide to the Effective Implementation of Right to Information Laws*. Washington, DC: The World Bank.

Levi, M., and Stoker, L. (2000). Political trust and trustworthiness. *Annu. Rev. Polit. Sci.* 3, 475–507. doi: 10.1146/annurev.polisci.3.1.475

Mabillon, J. (2004). "De re diplomatica," in *Treatise on Monastic Studies*, ed J. P. McDonald (Lanhan, MD: University Press of America).

Markey-Towler, B. (2018). Anarchy, blockchain and utopia: a theory of political-socioeconomic systems organised using blockchain. *J. Br. Blockchain Assoc.* 1:13. doi: 10.31585/jbba-1-1(1)2018

Miers, I. (2018). *How Much Privacy is Enough? Threats, Scaling and Trade-offs in Blockchain Privacy Protocols*. Scaling Bitcoin. Available online at: https://www.reddit.com/r/pivx/comments/9m1cpa/howmuchprivacyisenoughthreatsscalingand/?depth=1

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., et al. (2018). An empirical analysis of traceability in the Monero blockchain. *Proc. Privacy Enhancing Technol.* 2018, 143–163. doi: 10.1515/popets-2018-0025

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online at: https://bitcoin.org/bitcoin.pdf.

Naqvi, S. (2018). "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. doi: 10.1145/3230833.3233290

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press.

Neuman, L., and Calland, R. (2007). *Making the Access to Information Law Work: The Challenges of Implementation. The Right to Know*. New York, NY: Columbia University Press.

Orlikowski, W. J. (1992). The duality of technology: rethinking the concept of technology in organizations. *Organ. Sci.* 3, 398–427. doi: 10.1287/orsc.3.3.398

Peters, G. W., and Panayi, E. (2016). "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century*, eds P. Tasca, A. Tomaso, L. Pelazzon, and N. Perony (Cham: Springer), 239–278.

Piore, A. (2018). *How Blockchain Technology Could Help Us Take Back Our Data From Facebook, Google and Amazon*. Newsweek. Available online at: https://www.newsweek.com/2018/11/16/new-internet-blockchain-technology-could-help-us-take-back-our-data-facebook-1222860.html

Posner, E. (1972). *Archives in the Ancient World*. Boston, MA: Harvard University Press.

Robinson, A. (1995). *The Story of Writing: Alphabets, Hieroglyphs and Pictograms*. New York, NY: Thames and Hudson.

Seabury, P., and McDougall, W. A. (1984). *The Grenada Papers*. Washington, DC: ICS Press.

Sifry, M. L. (2011). *WikiLeaks and the Age of Transparency*. New York, NY: OR Books.

State of Arizona (2017). *Chapter 97, Title 44, Section 7061. Signatures; Electronic Transactions; Blockchain Technology*. Available online at: https://legiscan.com/AZ/text/HB2417/id/1588180/Arizona-2017-HB2417-Chaptered.html (accessed March 29, 2017).

State of Vermont (2016). *Act 157, Sec. I.1. 12 V.S.A.* § *1913. An Act Relating to Miscellaneous Economic Development Provisions*. Available online at: https://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20As%20Enacted.pdf (accessed July 1, 2016).

Storch, S. (1998). Diplomatics: modern archival method or medieval artifact. *Am. Arch.* 61, 365–383. doi: 10.17723/aarc.61.2.h0358316qn85p2lm

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

Sward, A., Vecna, I., and Stonedahl, F. (2018). Data insertion in bitcoin's blockchain. *Ledger* 3, 1–23. doi: 10.5195/LEDGER.2018.101

Tolbert, C. J., and Mossberger, K. (2006). The effects of e-government on trust and confidence in government. *Public Admin. Rev.* 66, 354–369. doi: 10.1111/j.1540-6210.2006.00594.x

TRC (2018). *Truth and Reconciliation Commission of Canada*. Available online at: https://www.rcaanc-cirnac.gc.ca/eng/1450124405592/1529106060525.

Trubetskoy, G. (2017). *Notes to Self*. Available online at: https://grisha.org/blog/2017/10/20/blockchain-in-postgresql-part-2/

Tyacke, S. (2001). Archives in a wider world: the culture and politics of archives. *Archivaria* 52, 1–25.

Van Garderen, P. (2016). Decentralized Autonomous Collections. *Medium On Archivy*.

Vigna, P., and Casey, M. J. (2019). *The Truth Machine: The Blockchain and the Future of Everything*. London: Picador.

Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: a consideration of operational risk. *NYUJ Legis. Pub. Poly* 18:837. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579482

Walters, W. (2002). The power of inscription: beyond social construction and deconstruction in european integration studies. *Millennium* 31, 83–108. doi: 10.1177/03058298020310010501

Wells, H. G. (2005). *A Short History of the World*. New York, NY: Cosimo, Inc.

Yeung, K. (2019). Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law. *Mod. Law Rev.* 82, 207–239. doi: 10.1111/1468-2230.12399

Zgonjanin, S. (2005). The prosecution of war crimes for the destruction of libraries and archives during times of armed conflict. *Libr. Cult.* 40, 128–144. doi: 10.1353/lac.2005.0041

Conflict of Interest Statement: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.