Blockchains for Public Recordkeeping and for Recording Land Records

A White Paper of the Vermont State Archives and Records Administration Office of the Vermont Secretary of State

Prepared in collaboration with:

Vermont Agency of Digital Services

Vermont Municipal Clerks and Treasurers' Association

Vermont League of Cities and Towns

Version 1.0

January 15th, 2019

Contents

Executive Summary

- Public recordkeeping is a pillar of government and provides evidence of the actions and decisions of governmental officials. Open inspection of public records ensures that the government is accountable to the people it serves. Trust in government begins with trust in public records. Land records are extremely valuable as permanent evidence of land use and ownership. Land records have legal, environmental, and financial value that can extend for hundreds of years or forever.

- The technologies and processes that comprise public recordkeeping must ensure that records remain authentic, reliable, integral, and accessible, especially for archival records, which must be retained indefinitely. Technology selected for use in government applications must be thoroughly vetted and must adhere to the requirements that underpin essential functions of government.

- Blockchains, as systems of recording transactions, can reduce or eliminate some drawbacks and pitfalls of traditional transactional models, such as processing time, cost, and data integrity.

- Blockchains that feature "trustless" models might not be fundamentally compatible with public recordkeeping requirements. Additionally, not enough research has been done on the long-term preservation of records in blockchains to meaningfully evaluate their fitness as systems of record with permanent retention (as is true for Vermont's land records).

- The State of Vermont should invest in building its knowledge base about blockchains and other digital recordkeeping systems, which would be greatly beneficial in the short and long term.

- Vermont's land records are largely stored in paper or other analog formats such as microfilm, and many municipalities, as the primary custodians, have little in the way of digital infrastructure to support electronic recording or preservation of records, even if they were able to accept them.

- For blockchains to be a candidate for Vermont's land recordings, some major overhauls would need to be made to State law and standard operating procedures. Inserting blockchain technology into existing processes would add additional complexity with little additional value gained.

- Uniform laws could be leveraged to enable transacting more business through blockchains; adoption of the Uniform Real Property Electronic Recording Act could pave the way for more sophisticated electronic recording of land records in Vermont.

I. Introduction and Background

Pursuant to Section 8 of Act 205 of 2018, An act relating to blockchain business development, this paper seeks to:

1. Evaluate blockchain technology for the systematic and efficient management of public records in accordance with 1 V.S.A. § 317a and 3 V.S.A. § 117;

2. Recommend legislation, including uniform laws, necessary to support the possible use of blockchain technology for the recording of land records pursuant to 24 V.S.A. § 1154 and for other public records; and

3. Submit its findings and recommendations to the House Committee on Commerce and Economic Development; the Senate Committee on Economic Development, Housing and General Affairs; and the House and Senate Committees on Government Operations.

This white paper by the Vermont State Archives and Records Administration, a division within in the Office of the Vermont Secretary of State, with consultation from the Vermont League of Cities and Towns, the Vermont Municipal Clerks' and Treasurers' Association, and the Agency of Digital Services, attempts to address these questions in depth. This paper provides a broad overview of the current state of public recordkeeping in Vermont and requirements for systems that support it, an overview and evaluation of blockchain technology and its potential impact on the operations of state government, including its potential use as a system of recordkeeping, with a specific look at land records broadly as a primary use-case.

Previously, the Office of the Secretary of State, Office of the Attorney General, and Department of Financial Regulation were given a similar charge by Act 51 of 2015, the results of which were published in the 2016 Legislative Report titled *Blockchain Technology: Opportunities and Risks*. That report provided a more in-depth overview of blockchain technology, and similar technical reports by the National Institute of Standards and Technology (NIST)[1] of the basic elements that comprise blockchain technology, and those findings will be summarized here but not completely revisited.

The requirements for public records in Vermont have not changed substantially, and many of the questions facing blockchains and technology utilizing blockchains have yet to be sufficiently answered. Much of the development of blockchain technology, especially in public organizations, has been

[1] NISTIR 8202, Blockchain Technology Overview.

evidenced by many pilot projects and feasibility studies, but few concrete solutions that have made it to production. Furthermore, since 2016, blockchain markets have experienced major volatility and several prominent blockchains such as *Bitcoin* and *Ethereum* have experienced major forks. Thus, since little has changed, the conclusions of this white paper echo those of the 2016 report. Deeper study into what those requirements are and what blockchains might be able to do to meet those requirements are found herein. Furthermore, additional examination is given to land records specifically.

This paper does not aim to evaluate any specific blockchain, present or proposed, nor does it seek to evaluate the quality or sustainability of companies and other interests involved with the development of technology or services that utilize blockchains. Instead, focus is given to the method by which a technological solution that includes blockchain technology might meet or not meet the requirements the State of Vermont and similar public institutions have for their recordkeeping systems and processes.

II. Public Records in Vermont

> *"The General Assembly finds that public records are essential to the administration of State and local government. Public records contain information that allows government programs to function, provides officials with a basis for making decisions, and ensures continuity with past operations. Public records document the legal responsibilities of government, help protect the rights of citizens, and provide citizens a means of monitoring government programs and measuring the performance of public officials. Public records provide documentation for the functioning of government and for the retrospective analysis of the development of Vermont government and the impact of programs on citizens."*[2]

The role of government of the State of Vermont, at the State and local level, is multi-faceted; citizens rely on public agencies for a variety of tasks, including the assurance of public safety and welfare, the stimulation and development of the economy, the protection and assurance of rights and freedoms of its citizens, and the provision of essential services made effective through economies of scale.

Public records capture the essential evidence that allows the citizens to audit the actions and decisions of public officials, and to see if the mandate of the people is faithfully legislated, executed, and adjudicated. Public records are the foundation upon which any analysis of the effectiveness of government programs, expenditures, and mandates can be done, and thus any requirements for ensuring

[2] 1 V.S.A. § 315(a)

the authenticity, reliability, and accuracy of public records must be intrinsically strict. Public records serve as essential evidence in legal proceedings, are routinely relied upon in private business for establishment of identity and residence, and underpin international travel, among countless other contexts. Cooperative agreements and grant relationships with the US Federal Government, other US States, and the regulatory oversight of international corporations are dependent upon the reporting and transmittal of information through public records as well.

Technology plays a large part in the management of public records, especially in the last few decades as Vermont, both at the state and municipal level, has been making its transition from traditional paper-based recordkeeping systems to those that are fully digital and often web-based or remotely hosted. The acquisition of technology in order to better manage information and records is an area of particular interest to State and local government, as a significant amount of expense is undertaken in the purchase, maintenance, and operation of such systems. Many business systems in the State of Vermont have complex workflows and processes, but ultimately every system that records data or information is responsible for the management of public records.

The timeframe in which the government needs to retain information – whether for administrative, legal, or informational value – can span decades or centuries. Records, electronic records especially, must remain accessible to the populations throughout the entire life of record[3], even if the disposition of a record is permanent preservation. Indeed, a significant portion of public records are scheduled or legally required to be preserved indefinitely. Technologies that create, receive, store, and preserve public records thus must be able to faithfully protect and provide access to those records for as long as they are needed.

Vermont's public records law (1 V.S.A. §§315-320) is derived directly from the Constitutional principle that "all officers of government…are…at all times, in a legal way, accountable to" the people[4]. The Public Records Act (PRA) and subsequent amendments and revisions codify and enumerate this specific foundational requirement. A public record is thusly defined through the PRA as "any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of public agency business."[5]

[3] The lifecycle of a record is defined first in active use (supporting current business processes), followed by a period of inactivity, followed then by its final disposition, which includes either destruction or permanent retention.

[4] Constitution of the State of Vermont, Article 6

[5] 1 V.S.A. § 317(a)(1)

Vermont's public records play a vital role in a variety of legal and administrative processes occurring in both the public and private spheres: vital records are an essential part of identity management and protection, licensure provides regulatory oversight for professions and operations and provides public confidence, and land records provide continuity of ownership and a complete historical record that ensures accountability throughout time. Private entities have long relied on government at all levels to record information, provide regulatory oversight, and otherwise govern the flow of information through records. Mandates specific to the creation, management, and retention of public records are scattered throughout State statutes, administrative rules, and Federal laws and regulations, including exemptions to public inspection and copying. Since nearly all governmental functions involve the collection or creation of information, public records play a significant role in all or nearly all governmental processes. It is hard to conceive of a governmental function that does not record or receive information in any way.

The law mandates that a custodian of public records "shall not destroy, give away, sell, discard, or damage any record or records in his or her charge, unless specifically authorized by law or under a record schedule, as defined in 3 V.S.A. § 117(a)(6), that has been approved by the State Archivist."[6] Vermont public records law recognizes that not all information should be retained indefinitely. Instead, the ultimate disposition of public records, when they can be destroyed, and when they must be retained permanently, is at the discretion of the State Archivist, through the analysis of requirements and publication of *records schedules*, or the General Assembly through its legislative authority. Both require significant understanding and attention to not only the legislative expectations for the function that creates or receives records as part of its business, but also the requirements and expectations of the various processes, public and private, that consume those same. That is, records are not solely utilized by the function responsible for their genesis; indeed, some of the most historically significant examinations of public records have used information collected in one area to provide greater context or meaning in another. State and local government do not operate in a vacuum; different functions (and their records) interact and intersect, with outputs from one function serving as inputs to another.

At the Statewide level, the responsibility of executive agency and department heads to manage their records systematically is set out in 3 V.S.A. § 218 which states that "public records in general and archival records in particular need to be systematically managed to preserve their legal, historic, and

[6] 1 V.S.A. § 317a

informational value, to provide ready access to essential information, and to promote the efficient and economical operation of government." As the PRA applies to all branches and subdivisions of government, the same requirements are present at the municipal level. Indeed, the systematic management of records and information is crucial to the efficient operation of government, transparency in the actions and decisions of governmental officials, and ensuring that public bodies can meet the outcomes which are mandated to them. In this context, "records and information management" means the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of public records, including the processes for capturing and maintaining evidence of, and information about, public agency business activities and transactions in the form of public records.[7]

Since the ecosystem of public recordkeeping is so complex and broad, the State Archivist is tasked with "administering and implementing a records management program for state government in accordance with professional records and information management practices and principles is in 3 V.S.A. § 117 and reinforced in 1 V.S.A. § 317a, which prohibits the destruction of public records unless "specifically authorized by law or under a record schedule approved by the state archivist pursuant to 3 V.S.A. § 117(a)(5)." While individual agencies are required to develop and manage their own records and information management programs, the existence of a statewide program ensures consistency, integrity, and adherence to and use of standards and best practices and improve the outcomes of those programs. For example, records schedules, as defined in 3 V.S.A. § 117(a)(6), provide a consistent and coherent framework for articulating the retention, disposition, and public access requirements for records created or received as part of a governmental function.

The work of the Vermont State Archives and Records Administration as conducted with State agencies (through the Statewide Records and Information Management Program) and municipalities (through the Vermont Local Records Program) is to collaboratively collect, analyze, and summarize the requirements for individual governmental functions to promote accountability, transparency, and integrity in the recordkeeping process. However, this statewide effort to analyze and determine appropriate retention is merely the foundation upon which records management programs are built. Each agency, state or local, must manage its own records at the point of creation through its final disposition.

As previously stated, public records often serve as the essential evidence of the actions and decisions of State officers in legal proceedings, and many of those actions involve the oversight and monitoring of

---

[7] 3 V.S.A. § 117(a)(1)

private and public entities alike. The offering of records as evidence in legal proceedings has a long-standing and concrete body of law build around it, as one of the essential functions of government is the collection of information (stored in public records) which can subsequently be used in said proceedings. Thus, there is a prima facie assumption that records produced directly by a public agency are genuine and authentic[8], that allows the courts to function. Historically, various governmental entities throughout State and local government, most specifically the Secretary of State and the Municipal Clerks, have been empowered to certify the authenticity of governmental records for this purpose:

> "Unless otherwise provided, a certified or photographic copy of a record or document required by statute to be kept by a public official shall be competent evidence in a court in this State. Such official shall be the certifying officer for such purpose."[9]

Typically, when records are entered into evidence, they must be authenticated. This authentication process allows the court to trust that the data contained within the record is accurate. This allows the court to substitute the validation of the authority of a public official for the validation of the authenticity of the record which has been presented before it. To wit:

> "The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct in accordance with Rule 902 [see below] or testified to be correct by a witness who has compared it with the original."[10]

However, the court must be able to trust those processes that create, receive, store, manage, and preserve those records. Without reliable recordkeeping processes, the value of records as evidence is questionable at best, and nonexistent at worst. Trust in public records in legal proceedings is vital for the judicial system to operate, and thus trust in the processes that create and control public records and information is paramount.

---

[8] V.R.E. Rule 902. Self-authentication
[9] 12 V.S.A. § 1692
[10] V.R.E. Rule 1005. Public Records

Government functions are not the only processes that require public records to function smoothly and efficiently. Numerous private business processes rely on governmentally-collected or produced data to operate. Establishment and verification of identity is one such process; proof of residence is another. Opening bank accounts or applying for loans, applying to universities or participating in sports, traveling to foreign countries, applying for health insurance or receiving medical care – all of these might require a proof of identity or residence which often takes the form of a certified copy of a public record (or another government-issued record such as a driver's license).

Thus, as both public and private institutions rely on public records for vital functions, it follows that public records are extremely important in modern society. Trust in these records is paramount and ensuring that trust is the role of government officials at every level of authority and in every agency. Without trust in public records, there can be no trust in government.

III. Electronic Recordkeeping Systems

The State of Vermont has used technology to improve efficiency or outcomes of essential governmental functions for decades. Even as early as 1958, a number of State departments had already employed automated data processing, and the State considered creating centralized data processing (something that it did shortly afterward by creation Central Data Processing Services).[11] Computing technology especially has proliferated greatly through the State of Vermont and many of these functions are now fully or partially automated.

Technologies ultimately are tools, and like any tool, and technology can be effective if used appropriately; when misapplied, however, it can cause cost overruns, inefficiencies, long-term dependencies, and consequences that require even more investment to undo. A good process automated creates efficiencies; a bad process automated creates inefficiencies. Technology cannot easily fix poor business practices, and the State of Vermont and its political subdivisions are not immune to poor or wasteful processes. Thus, the evaluation and improvement of process is essential, and the acquisition of technology is secondary.

The use of technology in public recordkeeping has exploded in the past 15 years, and all public agencies today utilize electronic systems to manage their information. Records which were originally kept in analog format, such as books or ledgers, are now routinely scanned into electronic records

---

[11] Vermont Data Processing Study, Committee to Study State Government, 1958; Act 328 of 1960.

management systems, keyed or digitally processed into databases, or simply begin life as electronic data. As the sophistication of Vermont's technological infrastructure grows, more and more of these processes become automated with pre-programmed workflow steps that transform data from one format to another or from one view to another. The challenge of recordkeeping in the electronic domain is the increasing expectation to provide, on-demand, data reorganized and made accessible in diverse formats and contexts, as well as adapting to the ever-changing needs of the public. Indeed, in recent years the State of Vermont has expanded the number of roles devoted to Enterprise Architecture and Data[12], reflecting the growing importance of managing information and the complex ecosystem in which it is stored and used.

The consequence of this transmutation of data through different forms and formats is often that quite a few remnants are left behind—paper applications whose value has been exhausted after entry into the database, excess reports or collected data that no longer serves any purpose, and so on. Managing this great preponderance of data has become increasingly complex and burdensome to public agencies in every jurisdiction. Indeed, it is quite likely that the State of Vermont today collects or creates public records at a rate exponentially higher than the drafters of the original Public Records Act could have foreseen.

Furthermore, the scope of this transformation of data does not only include the physical or digital characteristics of the record itself, but also the environment in which the records reside. A filing room in one agency or vault in a town likely presents a very similar storage environment to another filing room at a different agency, or another vault in another town. However, even within divisions and units of the same organization, two electronic systems may have vastly different storage environments, considering that the operating system, database format, file formats, and other aspects can vary. Ensuring interoperability between electronic systems is a challenge, especially when data is being transmitted regularly between different agencies and different jurisdictions. The Agency of Digital Services, the Vermont State Archives and Records Administration, individual government agencies, and municipal bodies share the responsibility to ensure that these systems are interoperable; when they are not, data can be lost, processes can be delayed, and services interrupted. Every additional file format, or software environment, or hardware need, adds another requirement to the complex web of interacting technology solutions.

---

[12] Creation of a Chief Data Officer as part of the Information Technology reorganization through Governor Phil Scott's Executive Order 06-17.

This articulation of needs is the requirements-gathering process that underpins the governmental procurement process. This requirements-gathering process is complex enough that an entire body of knowledge is built around it. In the State of Vermont, the Enterprise Project Management Office (EPMO), a division of the Agency of Digital Services, is responsible for the oversight, monitoring, and ultimately management of projects that have been deemed especially important due to reach and impact, risk, or expense. Additionally, the State of Vermont has developed rigorous contracting requirements that seek to ensure that enough information is gathered as part of the procurement process to ensure that technologies selected for purchase and use are able to meet the baseline requirements.

Following the gathering of requirements, each candidate technology must then be evaluated to determine whether the capabilities of the technology are able to meet the procedural, financial, legal, technological, or other requirements. Some are not mandatory, and compromises can be made, while many (especially those that are statutory or otherwise regulatorily mandated) must be satisfied and may require complex solutions. The set of requirements (commonly broken into functional and non-functional categories) can easily be hundreds or thousands of items, depending on the size, reach, and impact of the system. Contracting and procurement in the State of Vermont are heavily scrutinized as they involve the expenditure of large amounts of public monies with sometimes negative outcomes. Ensuring that the solutions meet the needs is crucial to ensuring that the process functions well.

Requirements for Recordkeeping Systems

Systems for the maintenance, preservation, modification, control, and provision of access to public records, especially electronic records, could have many requirements. While it is beyond the scope of this paper to outline at a granular level all requirements of recordkeeping systems[13], chief among them is the ability to ensure that records are trustworthy. Ultimately, public records, and all records, lose value if they are not trustworthy. If the records, for whatever reason, cannot be trusted, then the information contained within also cannot be trusted, making it valueless as a legal instrument, as part of a business process, or as evidence of the actions, transactions, and decisions of public officials.

[13] For a more in-depth examination of electronic recordkeeping systems, standards like the US Department of Defense *Design Criteria Standard for Electronic Records Management Software Applications*, DOD 5015.2-STD and *Modular Requirements for Recordkeeping Systems* (commonly known as MoReq) are commonly accepted industry standards to examine and are cited in the references of this report.

A broad standard for requirements for records management systems can be derived from the international standard for records management, *ISO 15489: Records Management*. Based on this standard, the trustworthiness of a record can be measured on three primary axes: authenticity, reliability, and integrity.[14] Furthermore, the ISO standard defines a fourth key aspect, useability, which is not integral to the trustworthiness of a record, but rather the practical usefulness of that record in context. Any system that manages or contains public records or information must have requirements that address each of these factors to the utmost degree, since loss of fidelity in public records is of great consequence.

The authenticity of records is essential to their value as evidence, as legal instruments, and as documentation of the facts contained within. A record can be said to be authentic if it can be proven:

a) To be what it purports to be
b) To have been created or sent by the person purported to have created or sent it, and
c) To have been created or sent at the time purported[15]

Record authenticity is thus across three dimensions; the first is identity, the second is authorship, and the third is temporal. Proving the authenticity of records has become more complex as the sophistication of computing technology has grown; while it is exceptionally difficult to make a near-identical copy of a paper record, an electronic record is, fundamentally, nothing more than an ordered sequence of bits stored on a disk, and that sequence can be copied exactly by almost every personal computer in the world. Anyone can draft a letter in a word processing application and insert a screenshot of a public official's signature, but that is alone is not enough to make that document an authentic public record. An entire set of parameters (including tracking of the creators, the systems of origin or record, the time of creation among them) are needed to verify that a record was authentically created or received as part of a governmental function.

This is most often and most easily accomplished through an unbroken chain of provenance from record creator to record custodian, oftentimes known as "chain-of-custody". A record that has complete provenance can be said to be authentic; if it can be demonstrated to have been created or received as part of a governmental function, and then the custodianship of that record remained with the agency or officially designated successors, the record itself has an unbroken chain of custody. It is through this

[14] ISO 15489: Records Management
[15] Ibid.

chain of custody that the trustworthiness of the custodian can be imbued into the record. A record held by an untrustworthy source (one known for altering records, perhaps), can itself no longer be trusted. A record with a compromised chain of custody broken has lost its authenticity because it cannot be verified that it was not altered at some point when it was not in the custody of a trustworthy source.

Reliability is a measurement of how much a record can be "trusted as a full and accurate representation of the transactions, activities, or facts to which they attest."[16]Records are most reliable when they are created proximally and temporally close to the events, actions, and decisions they record. Just as a firsthand account of an event recorded by a witness shortly after it occurred is more reliable than a thirdhand account of an event recorded years later, a record that is created during or shortly after the process in which it was used is most likely to be reliable. Similarly, records that are created by sound business or recordkeeping processes (such as having good control over records creation) have greater reliability than those which are created by inconsistent or haphazard processes. It may never be possible to ensure 100% reliability of records given that records creators are fallible, but robust processes that control the creation of records can maximize this requirement.

A record's integrity is a measurement of both its completeness and the knowledge that the record is unaltered from its original form. Maintaining integrity in electronic recordkeeping can be extremely difficult. Since even small changes can cause significant damage to electronic records, even rendering them completely unreadable, maintaining the integrity of a record is paramount to ensuring that the record is usable at all. Additionally, with the ease of both inadvertent and intentional alteration of digital files, and the difficulty of tracing changes to records in systems that are not designed to fully audit the actions of their users, it can be difficult or impossible to detect alterations to records without robust systems that monitor the integrity of those records. Furthermore, without the complete record, valuable context can be lost, rendering the meaningfulness of the record void. A simple example might be a document with a missing page; it would be hard to judge that record as fully valuable since that page could contain any manner of missing information that changes the entire context of the document. A record without integrity, or that comes from a system without integrity, cannot be trustworthy since it might lack important details or context that could change the entire interpretation of a record.

Finally, the useability of a record is defined by how easily it can be "located, retrieved, presented, and interpreted,"[17] and often this can be the most challenging requirement. Specifically, for records to be

---

[16] ISO 15489: Records Management
[17] Ibid.

useful, they must be available and interpretable. Records in unreadable languages, encoding, or legacy file formats certainly can be authentic, reliable, and have integrity, yet may no longer be useable. A great challenge of both records management and long-term digital preservation is continuing to provide the same quality of access to information despite changing environments. All of these elements are critical to measuring and maintaining the value of records for any purpose. Maintaining the authenticity, reliability, and integrity of records keeps them trustworthy; maintaining their useability keeps them useful. Furthermore, the complexities of modern records management often mean sacrificing quality in one of these elements for greater fidelity in another. Easily useable records often have light integrity controls. Strict chain-of-custody rightfully impedes broad access to records.

The standards for public recordkeeping system requirements are necessarily high. The potential consequences of untrustworthy records entering into legal proceedings are disastrous; loss in faith in government recordkeeping would undermine trust in government itself. Data breaches in government over the past several years have caused legislative bodies to implement sweeping protections such as the EU's General Data Protection Regulation (GDPR), seeking to restore trust in the government's ability to manage data.

No technology will meet every single requirement, since not every requirement is binary. Additionally, even efforts like the Department of Defense requirements[18] are not strictly prescriptive because high degrees of fidelity in each of these areas can often be expensive or complex. Many requirements are measured by achieving goals to the highest degree practicable, and often there is a tradeoff between perfect adherence to a requirement or standard and a significantly cheaper solution. No system is perfect, so establishing several key metrics helps frame and make systems implementation achievable. It is through this lens that any technological solution should be evaluated.

IV. Overview of Blockchain Technology

While the fundamental concepts and technologies that underpin Blockchain technology have been around since at least the early 1980's, the technology's development and substantial public interest began in earnest ten years ago on October 31, 2008, with the publication of the Bitcoin white paper by Satoshi Nakamoto.[19] In it, Nakamoto described the concept of *Bitcoin* as a peer-to-peer currency

[18] *Electronic Records Management Software Applications Design Criteria Standard*, DoD 5015.02-STD. United States Department of Defense. (2007)

[19] Nakamoto, 2008.

transaction model. Since then, hundreds of other currencies as well as other services have launched using Blockchain technology, as well as having billions of dollars invested in coins, services, corporations, and interests utilizing it.

In 2016, the State of Vermont analyzed Blockchain Technology broadly, and in the report of that analysis, provided an overview of the technology. Rather than re-iterating the overview of that workgroup, herein we shall provide a similar overview with the specific context of Blockchains as systems of record, and in the context of the requirements of all recordkeeping systems.[20]

Additionally, due to the continued interest in blockchain technology, cryptocurrency, smart contracts, and other services that rely on Blockchain technology, further development and study has brought a greater understanding and sophistication to both the technology itself as well as the frameworks and models for processes that can leverage the technology. Continued interest by private firms including banks and other financial institutions, information technology leaders, defense contractors, manufacturers, and others have funded pilots to gauge the interest and effectiveness in utilizing blockchain challenges including corporate governance, financial transacting, and identity management. In government, the State of West Virginia recently piloted the use of blockchains for absentee voting in primary elections, the State of Colorado has created a Blockchain Council[21] for the study of uses of blockchains in government, and the State of Delaware recently entered into large contract with IBM to develop and pilot blockchain solutions.

However, the fundamentals of blockchain technology have not changed. Though each implementation may vary, a few key elements are characteristic of all blockchains:

- transactions are made electronically between parties
- data about the transactions, including the identity (or address) of each party, a timestamp, and a reference to a previous block, are hashed (distilled to a short digest through an encryption algorithm); then
- these transactions are then broadcast to the network; then
- individual nodes in the network perform validation or verification of those transactions; and
- once “consensus” is reached, each set of transactions (block) is then added to the electronic register or ledger (the chain); then
- the process is repeated for each subsequent transaction, continually adding to the chain

[20] Blockchain Technology: Opportunities and Risks, State of Vermont, 2016.
[21] https://choosecolorado.com/blockchain/

Bitcoin, and the technology that came to be known as blockchain, was created to solve a very specific problem: a method was needed to transact business over the internet for parties who

a) don't necessarily know each other's identities
b) don't trust each other
c) don't wish to rely on a middleman (since on the internet, you might not be able to trust the third party either)

As transacting business with unknown entities is inherently risky, historically people have relied upon trusted intermediaries like banks, brokerages, and governments to assist with the transaction. Traditional methods of identity verification (such as displaying an ID) are too easy to defeat in an environment where anything can be replicated. Thus, blockchain was created by synthesizing existing methods such as public-key cryptography and peer-to-peer networking to provide a solution that purports to be based in cryptographic proof rather than trust in organizations or individuals.

Public-key cryptography provides a secure method for solving the first challenge presented above. Each user has two sets of keys[22], one public and one private, both of which are linked mathematically to each other. The user's private key is used to sign (encrypt) messages and is kept secret, while the public key, which is publicly broadcast, can be used to decrypt those messages. Others can be sure of the origin of messages so long as the messages are signed with the user's private key. This technology and technique is robust and essentially has created the backbone of the internet.[23] This method allows anonymous or otherwise unknown users to identify themselves unerringly through use of their private keys (though theft of private keys and through it identity theft is still a significant issue).

Historically, trust in transactions has been provided in several ways: by a legal framework that protects good actors and punishes bad actors (contract law), or by relying on those with either a legal, fiduciary, or other duty to one or all parties. These duties arose from common law[24] and provide a framework for trust in transactions. If both parties can agree to use the same broker, they can establish some common ground and the broker's role is to guarantee, facilitate, underwrite, or otherwise assist in the transaction. In some contexts, the government itself plays the role of this intermediary. One of the

---

[22] A key in this case is a unique cryptographic signature, essentially the same technology used in e-signature platforms, web certificates, and more.

[23] For further reading, refer to the Secure Sockets Layer (SSL) or Transport Layer Security (TLS), which are implemented more commonly known as web certificates and allow users to visit web sites and know that their traffic has not been intercepted or captured.

[24] Siepp, David. (2011) Trust and Fiduciary Duty in the Early Common Law. Boston University Law Review, Vol 91, No. 3, 2011.

primary goals, if not the primary goal, of blockchain technology is the removal of the need for this trusted third party[25]. Requiring the services of an intermediary adds cost and processing time and exposes parties to the transactions to a new risk: malicious or predatory behavior on behalf of that intermediary. As the power of private individuals shrinks and the power of institutions grows, the individual becomes more and more reliant on these services, putting them at greater risk, and the need for trust grows.

By utilizing peer-to-peer transaction verification, the intermediary is replaced by a network of peers, as if everyone who wanted to transact business agrees to share in the burden of being that intermediary. Since transactions are encrypted, the natural role of members of this network (known as *nodes*) is to decrypt these transactions thereby verifying them (since they would not decrypt properly to well-formed transactions were they created incorrectly). These nodes in the *Bitcoin* blockchain are compensated for this work through the "mining" of additional coins. Thus, the network, through the blockchain protocol, replaces the intermediary.

The final piece of this method is the so-called "consensus protocol" which forces the network to agree on correctness and ordination of transactions to proceed. Put more plainly, the work of verifying transactions cannot be completed by a single node, but rather a majority must verify individual transactions before they become valid and can be added to the chain. Requiring multiple verifications greatly reduces the possibility of incorrect transactions. Each transaction is generally comprised of:

a) a list of inputs (references to previous transactions)
b) a list of outputs (results of the transactions)
c) verifications
d) timestamps

These data together provide a succinct transaction record; a bundle of records together that has been verified and has subsequent transactions after it becomes a block. All the blocks together comprise a blockchain. These blocks are saved, stored, and referenced by the nodes when adding new blocks. As transactions in the *Bitcoin* blockchain specifically reference previous transactions, it becomes necessary to be able to refer to those transactions to prove that an asset or coin is owned.

Bitcoin may have been the first blockchain, but its successors now number in the thousands or tens of thousands, and that number includes only public blockchains. There could be countless private or

[25] Nakamoto, p.1

consortial blockchains to which the public might not have access. Parameters such as transaction size, encryption algorithm, consensus model, block structure, and more vary from blockchain to blockchain. A change in some of the parameters fundamentally changes the nature of the blockchain; for example, a fully public blockchain might have any number of users voluntary operating as nodes, while the same might only be available through invite in a private blockchain. Due to the wide variance in the possible design and trust models of blockchains, it is imperative to evaluate its functionality broadly against the baseline requirements for public recordkeeping.

V. Evaluation of Blockchain Technology for Public Recordkeeping

Bitcoin, as originally conceived, and blockchains generally, were designed specifically as systems of record. But how do they meet the requirements for public recordkeeping? As there is so much variability in proposed blockchain solutions, this paper will focus primarily on broadly-defined classes of blockchain technologies. Additionally, that are a countless number of technological products or proposed solutions that feature blockchains as merely one part of their technology stack, in conjunction with traditional document management platforms, databases, or other software or hardware. It would be impossible to meaningfully evaluate all the possible ways that blockchains *could be* utilized by government agencies for recordkeeping purposes. Rather, the fundamentals will be evaluated on their own merit based on the legal requirements and industry best practices described above.

Blockchain implementations as it pertains to recordkeeping, generally fall into one of three categories:

a) registration of records themselves in blockchains
b) registration of "fingerprints" or other identifiers of records in blockchains
c) registration of "stand-ins" or "tokens" in blockchains[26]

The difference between these three methods is the content of the data within the blockchain transaction. Ultimately blockchains are tools for the broadcast, decryption, and registration of transactions; individual implementations define explicitly the form and content of those transactions. For example,

[26] These types of blockchains are outlined in *A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation*, by Victoria Lemieux of the University of British Columbia. This typology provides a useful framework for discussing, realistically, how blockchains might be used as recordkeeping systems.

Bitcoin transactions contain references to previous transactions (proving that the sender possesses the coin), addresses for the parties to the transaction, timestamps, and other structural information.

The first is the most straightforward, but also the most uncertain. Most often referred to as "smart contracts", these records are self-executing code contained within a blockchain that triggers when certain criteria are fulfilled, and the records of those transactions are also stored within the blockchain. Smart contract protocols primarily use the *Ethereum* blockchain due to processing capabilities and its development as a blockchain application network rather than explicitly as a peer-to-peer cryptocurrency. Thus, in this case essentially the transactions themselves and the parameters of those transactions are all contained within the blockchain. The legal status of smart contracts and their enforceability is questionable; efforts in Vermont and other states to recognize, regulate, and build a body of law around smart contracts are currently underway.

The second method uses the blockchain for an immutable registration of a digital fingerprint of a record held outside of the chain in another recordkeeping system. As part of the *Open Archival Information Standard* (OAIS)[27] and other records management and archival standards, the cryptographic hashing of electronic records provides a reliable way to monitor the integrity of a record. When a digital file is hashed, its sequence of bits is run through a mathematical algorithm that produces a unique 256-bit (or other size, perhaps) hash. It is mathematically unlikely that any other sequence of bits would produce this hash, and furthermore, the alteration of any single bit in the original record would cause the hash to change. In this case, these hashes would then be stored in a blockchain.

This method relies heavily on other recordkeeping systems, but that is by design. Blockchains are inherently not designed to have massive block sizes as those blocks would take far too much computational power to make a system like this practical. This then requires a robust method for preserving provenance and the contextual linkage between the object and its fingerprint. Generally, the separation of records from their context runs against traditional archival practices for good reason; loss of context is loss of information, and blockchains come with no guarantees.

The third method involves the creation of objects in the blockchain which are themselves transactable; this might be known as the "token" approach. These tokens are tied to specific objects and the titles to those objects outside of the blockchain. Transacting business in the chain involves the transference of these tokens, and along with them, the interest in whatever they represent (currency,

[27] ISO 14721:2012, *Space data and information transfer systems – Open archival information system (OAIS) – reference model.*

property, records, etc.). An example for illustration might be for a set of collectibles of a fixed quantity. Each is represented by a token, and whenever ownership over a collectible is desired to be changed, the token is transacted in the blockchain, providing a chain of custody for those tokens.

Regardless of the individual models, parameters for how blockchain networks "solve" blocks, what percentage of nodes are required for "consensus", block size, block metadata, encryption algorithm, and others will certainly have great variation depending on the blockchain solution in question. Thus, measuring the efficacy of blockchains with regard to record authenticity, integrity, reliability, and useability will provide the clearest understanding.

The findings and work of the *International Project on Preservation of Authentic Records in Electronic Systems* (InterPARES) examined the baseline requirements needed to ensure the authenticity of a record in an electronic context. The attributes that allow one to assess the authenticity of a record are the ability to establish unerringly the *identity* of a record, and the *integrity* of a record. [28] The *identity* of a record is a measurement of its uniqueness when compared to other records; how can we know that this record is different and unique from other records? The details and evidence (usually captured in metadata) recorded about the creation of a record are the key pieces of information that establish the true identity of a record. Blockchains do well when measuring the identity of records: timestamping and contextual linking to previous blocks (in conjunction with the cryptographically signed transaction), as well as the collection of the parties involved provide enough detail to distinguish one record from another. Based on the way blockchains are designed, it would be nearly impossible for two blocks or transactions to be identical in this way.[29]

Additionally, the *integrity* of blockchain records is sound, considering the methodology that is used to complete transactions. First, there is the required hashing of transactions, which adds a level of cryptographic security (as previously described). It is extremely difficult given current computing technology and processing power that these cryptographic schemes could be compromised, though not impossible. More important is the confirmation by the network of nodes that the transaction is well-formed; that is, it adheres to the rules of that blockchain. A record without integrity would not pass this simple test and instead would be rejected by the network and never added to a block. Once the record is added to the blockchain, it becomes distributed in the *authoritative* version of that chain. That version of

[28] Authenticity Task Force Report, InterPARES.

[29] It is possible for multiple transactions to be broadcast to the network simultaneously, even multiple transactions by the same parties. The consensus protocol saves the day in this case, as whichever transactions are validated first by the majority (if they are well-formed) will be added to the chain and others will not be validated (and will need to be resubmitted or abandoned).

the blockchain then will be distributed across the network, making it essentially impossible to alter (since thousands of records in disparate systems would need to simultaneously be altered). The archival community has focused on the concept of distributed storage, especially through projects like LOCKSS ("lots of copies keeps stuff safe").[30]

There is a substantial risk when it comes to the assignment of "authoritativeness" of individual blockchains. Since blockchains are generally comprised of voluntary actors, at any point those actors might decide to stop contributing. Or they may decide that a block or set of blocks is important enough to spin off into a new chain beginning at that point. This is known as a *fork* and this has occurred multiple times in *Bitcoin's* history. It's unclear how a fork would affect the long-term reliance on blockchains as systems of record. Since there is not necessarily any long-term commitment to participation in any blockchain network, a fragmentation of a blockchain could pose a significant challenge: when verifying a record's authenticity in one of the above models, users would have to know which of the various different forks of any one blockchain are authoritative. While these scenarios are unlikely, the high degree of volatility in the largest blockchains calls into question the sustainability models.

Another area of major concern is the ownership model of data in blockchains. Since most blockchains are inherently trustless, there is no accountable party who would be responsible for preserving blockchain records. While it might be difficult to forge a blockchain record, it could be possible to lose the records of old blocks, and it would likely be exceptionally challenging to rebuild lost blocks (a block that is easy to rebuild is probably easy to forge), once gone they might be gone forever. Many blockchain technologists purport that the biggest chains are duplicated in enough places for this to be unlikely, but proliferation is not a substitute for preservation. All digital data degrades over time. Long-term preservation of data thus requires dedication and commitment as well as technical expertise. Accountability is a key factor in the governance of information, and with no accountable party there is great risk to long-term sustainability.

Additionally, allowance of anonymous submission of transactions to blockchains could pose a significant challenge to ensuring authenticity in records. One of the core aspects to assessing the authenticity of a record is the identification and confirmation of the agents (typically people or organizations) involved in its creation. For example, part of ensuring the authenticity of a government

---

[30] https://www.lockss.org/

record would be a demonstration that the record was created or received by a government official in the course of public business. Not only can agents in blockchains can be hidden behind potentially many layers of anonymity, maturation in legal frameworks for smart contracts can create a complex web of relationships and authority within blockchains themselves. Due to these questions, it is hard to view blockchains as compatible with the traditional model of record custodianship, especially as it pertains to public recordkeeping.

Since many blockchains allow anonymous submission, additional protections would be necessary to ensure that public officials were acting in their official capacity when submitting records to the network to be verified and recorded in the blockchain. And if inauthentic records were submitted but were well-formed, it would likely be very costly to reverse or remove incorrect transactions that were not immediately discovered (since subsequent transactions would be build off contextual references to previous, possibly incorrect, blocks or transactions.)

Reliability of records in blockchains is difficult to measure. Blockchains with very small transaction sizes might be missing a great deal of essential context that speaks to the reliability of a record. A transaction that is well-formed between Party A and Party B to transfer Asset C might be submitted to the network and verified; but the network doesn't know (or doesn't care) that they are dealing instead with Public Key A behind which a malicious actor might be operating. This isn't an issue that is unique to blockchains, as identity theft is a major source of concern in electronic communications. What is unique to blockchains is the limited amount of information contained within a single transaction. Limited information is necessary for computational efficiency. Decrypting more data costs more. Thus, models like the fingerprinting or token models were devised to register only a small amount of information in the blockchain, and instead store the rest of the detail somewhere else.

Of course, this somewhat circumvents the value of using blockchains, as these solutions often rely on a single-source oracle or storage system, which may or may not be protected by distributed data or from alteration. As another example, a record is hashed and the hash stored in the blockchain. That hash is protected, but if the record is altered it will no longer validate. The system works, but it doesn't allow for the recovery of the original record. It has still been changed, and the custodian knows it, but doesn't know how and due to the nature of public key cryptography, they intentionally can't reverse-engineer the record from the hash.

Perhaps the most difficult hurdle to overcome for Vermont and government in general is in the useability of blockchain recordkeeping systems. Information transfer between public agencies and their constituents occurs daily. While the use of a technology by private parties does not necessarily compel the government to utilize that same technology, it would be a challenge for a government agency to accept a record in a blockchain as evidence of a transaction without taking a copy for its own records. What would this entail? Assuredly, the State of Vermont would need a method for evaluating blockchains and the records therein which is likely well beyond its current capabilities.

What would constitute the minimum amount of information necessary to comprise a full blockchain record? A transaction? Would the entire block be required, so that future citizens could individually verify the authenticity of a particular record? How about the entire blockchain on which it was stored, so that the public could fully audit the chain itself to ensure that it was not at some point built on false pretenses? Furthermore, it's not clear how much of the blockchain would need to be preserved to satisfy a legal baseline of validity. Merkle trees[31] provide users with the ability to verify transactions within blocks or segments of blocks without needing the entire chain, but there is no clear standard for establishing the validity or reliability of a blockchain as a whole. In a typical legal proceeding, a record presented may asked to be authenticated, and the testimony of an official might help establish the authenticity of a record. While blockchains might be internally consistent, there would presumably still need to be an agent that creates the contextual link between record and blockchain. It's not sufficient to present a transaction and claim that it is a valid transaction on a blockchain; or is it?

As public records are often entered into evidence in the State's adjudicative proceedings, the methodologies and technologies available in Vermont's courts will need considerable updating and modernization to be able to accept records from a blockchain into evidence, validate them, and use them in proceedings. While some public records in electronic format can be converted to an analog format, through printing or playback, it is hard to conceptualize how blockchain records can be converted to different formats. Merely printing the data from a blockchain is somewhat akin to printing an electronic signature; what matters less is the content of the record (since it is mostly non-human-readable cryptographic hashes and other metadata) but rather the ability to trace the validity of the record. This would need to be done fully in an electronic environment, and for a copy of a record to be admitted into evidence, even a single bit changing through accidental or intentional means would be disruptive.

If blockchains are not captured and continuously preserved by government institutions responsible for long-term recordkeeping, what safeguards does the public have to ensure that public records

[31] For a good primer on Merkle trees and the methods for using them to validate records in blockchains, see Becker, Georg. (2018) *Merkle Signature Schemes, Merkle Trees and their Cryptanalysis*. Ruhr University Bochum.

transacted and recorded in blockchains continue to exist in perpetuity? Such a guarantee would be impossible unless the government itself guaranteed the existence or operation of that blockchain. Since there is no accountable organization or person, there can be no designated or legal successor to that organization. Private institutions might claim to be able to guarantee perpetual existence, but even the longest-existing private organizations in the world can trace lineages a few centuries. And if the government is required to maintain a complete copy of the blockchain so that transactions could always be verified --- has anything been gained, or has a burdensome layer of additional technology been added with little commensurate value?[32]

Worse still than the threat of loss is the threat of capture or control by malicious actors, which could theoretically occur should someone gain control of a majority of nodes in the network. Proponents of blockchain technology purport that such capture is impossible; the computational power necessary would be astronomically large.[33] However, even large companies have been victim of hostile takeovers (involving the acquisition of large swaths of shares); as long as technology continues to improve, it is impossible to completely rule out capture of a blockchain network in this way, especially as quantum computing, machine learning, and similar technologies mature. Blockchains are inherently reliant on the networks and the protocols that set the parameters of their operation; if those protocols and networks can be controlled, the integrity of the blockchain itself could be called into question. The example of the fate of the Distributed Autonomous Organization should be in the forefront as well, where a small exploit discovered in the protocols of the technology permitted malicious attackers the ability to defraud over 50 million dollars and eventually leading to a fork of the Ethereum blockchain.[34] There will never be a solution to poorly designed or implemented technology, and not even blockchain is immune to flawed design or implementation.

Ultimately, information contained within blockchains is not inherently human readable; of course, this is true of most electronic information but since blocks and transactions are natively encrypted, an additional layer of abstraction is present. Hashes are representations of other records that have been run through a mathematical algorithm. They are merely representation of information stored somewhere

---

[32] Of course, government itself is not immune from tampering, capture, corruption, or many other threats that face private organizations. However, government even in Vermont is large enough and theoretically possesses enough checks and balances to prevent widespread capture or corruption.

[33] In January of 2019, the blockchain Ethereum Classic was reportedly the victim of a "51% attack" described above, which allowed circumvention of the network's integrity and essentially allow for "brute force" double-spending of Ethereum.

[34] Popper, Nathaniel. *A Hacking of More Than $50 Million Dashes Hopes in the World of Digital Currency.* New York Times, June 17, 2016.

else. From a recordkeeping perspective, storing two inherently linked pieces of information (this being the original record and the hash thereof) in different systems can be beneficial, but often severs the context of the original record, damaging its authenticity. One of the benefits of blockchains is their immutability; a distributed ledger held in dozens of places is unlikely to be compromised, so any document can be hashed and compared against a record within the blockchain to verify its veracity. But if that original document is lost, or the link is otherwise missing, it would be potentially very challenging to rebuild that context. This level of technical sophistication would pose a significant barrier for many Vermont citizens. Considering the additional technological sophistication required simply to use blockchains (such as having a permanent, secure, personal set of keys) is another layer of requirements on citizens that could pose risks (as loss of such keys would be akin to losing control of one's digital identity). It is difficult to sell blockchains in their current form as a simple technology that all Vermonters could use to verify the integrity of their own transactions without a substantial education effort.

Blockchains are, by themselves, antithetical generally to the fundamental model of public recordkeeping. If government is ultimately accountable to the people, it might seem natural that the recording of data in publicly-accessible blockchains would be a boon. However, there is a significant difference between a model of custody involving distributed data in many hands and government custody. Blockchain networks are accountable to no one. Companies that provide blockchains or technology stacks that incorporate blockchains are accountable to perhaps their shareholders; even now, governments around the world are considering how to provide oversight and regulation for blockchains. The 2016 legislative report recommended further study and here we will again recommend the development of knowledge and expertise in government in blockchain technology. Careful study and consideration will be required to judge the efficacy of blockchains for their stated purpose. Even if blockchains were completely flawless, its users must still rely on either the network or the protocol, or both, and whether those entities can be trusted is questionable. The substitution of government for either private vendors or faceless networks is a net loss for transparency, accountability, and trust.

The long-term sustainability of current blockchain models is questionable at best. There has yet to be any long-term sustainability study of blockchain technology or infrastructure. The current model of the world's largest blockchain, Bitcoin, is sustained through voluntary participation. That is, each node in the network voluntarily contributes to transactional verification and is compensated for that participation through the discovery of new coins. Since coins have value, this is a fair trade; the cost of equipment and power necessary for the computations necessary are smaller than the reward for that work, then profit can be achieved, and voluntary participation is effective. It is unclear whether volatility in the valuation of Bitcoins (which have dropped north of 50% in value between the passage of the act leading to this white paper and its publication) could substantially affect participation in the network. Total network failure seems incredibly unlikely, but reduction in the number of actors also presents a threat: since consensus protocols dictate the creation of new blocks, capture of a substantial portion of the network could allow capture of control of such consensus, which would most likely result in fragmentation of blockchains through forking, or worse, a loss of trust in the chain itself.

Similarly, the failure of the network infrastructure would not only impact the ability for the chain to continue growing through the addition of new transactions but would also call into question the preservation of previous blocks. Due to capabilities provided by Merkle roots, the integrity of single blocks, or even groups of blocks can be maintained in isolation, but the actual digital preservation and storage of such blocks would be called into question. In the example of "digital fingerprinting" provided above, any record held outside the blockchain would still need to be compared against a hash within it. But where does one source the comparison? If one must rely on a single point of trust to maintain a copy of the entire chain for preservation purposes, that somewhat defeats the purpose of distributed ledgers since trust is once again reduced to a single point-of-failure. Distribution of trust across the entire network (say, comparing the digital fingerprint against two or three or ten or forty or one hundred nodal copies of said block) then relies on the continued voluntary participation of all those actors.

To guarantee the long-term sustainability of records fingerprinted or stored in a blockchain, a significant number of actors within the network would likely need to commit to storage of blocks as long as required. In a so-called "public" blockchain such as Bitcoin, such guarantees seem unlikely but not impossible. Perhaps "private" blockchains, whose networks are comprised solely of actors who themselves can be trusted and who can form cooperative agreements (e.g. networks of State Archives, State Libraries, State IT shops, etc.), might be considered for indefinite preservation. Perhaps groups of governments like States, or municipalities, could band together and cooperatively contribute resources to a true publicly-controlled blockchain that has the accountability and recordkeeping requirements met to satisfy public needs.

VI. A Case Study: Land Records in Vermont

Land records have a vital place in the body of Vermont's public records. The government has served an essential role in the recording of land transactions since the founding of the State; that role is outlined briefly in the Constitution: "All deeds and conveyances of lands shall be recorded in the Town Clerk's Office in their respective towns; and, for want thereof, in the County Clerk's Office in the same county."[35] The founders recognized the necessity of recording the ownership of land even before statehood; indeed, the initial charters of many Vermont towns were issued by New Hampshire Governor Benning Wentworth in the 1760s, the ownership of which was much disputed with the colony of New York in the ensuing decades.

> *And whereas, the territory which now comprehends the State of Vermont, did antecedently, of right, belong to the government of New Hampshire; and the former Governor thereof, viz. his excellency Benning Wentworth, Esq., granted many charters of lands and corporations, within this State, to the present inhabitants and others. And whereas, the late Lieutenant Governor Colden, of New York, with others, did, in violation of the tenth command, covet those very lands; and by a false representation made to the court of Great Britain (in the year 1764, that for the convenience of trade and administration of justice, the inhabitants were desirous of being annexed to that government), obtained jurisdiction of those very identical lands, ex-parte; which ever was, and is disagreeable to the inhabitants.*[36]

One of the first laws enacted in the State of Vermont was concerned with the recording of deeds and conveyances at the Municipal level, the purpose of which was very plainly explained in the subtitle of the aforementioned act: *For preventing fraudulent sales and incumbrances of real estates, and to the intent that it may be better known what title or interest persons have in or to such estates as they shall offer for sale.*[37]

The founders and early legislators of Vermont understood both the importance of preventing fraudulent sales of property but also that the ownership interest of parcels of land be publicly known.

---

[35] Constitution of the State of Vermont, Chapter 2, Section 62
[36] 1777 Constitution of the State of Vermont, Preamble
[37] An act for authenticating and registering deeds and conveyances, State of Vermont, Acts of 1787

Thus, a body of law has been developed and refined over the last several centuries that has articulated and codified expectations for municipalities when recording the conveyances of land, and the instruments that subsequent sessions of the General Assembly have deemed essential to be recorded along with those conveyances. Many of the requirements for recording land transactions and related records are found in Title 24, Chapter 35 and are assigned to the Clerk of each Town; similar requirements for County Clerks can be found in Title 27, Chapter 5.[38] These requirements set out the specific instruments that must be recorded in the municipal land records. *Instruments* in this context are formally executed written documents that can be formally attributed their authors, that are legally enforceable as evidence. These instruments frequently serve as evidence in proceedings in the Vermont courts, especially in the context of the Probate Division and Environmental Division of the Superior Court, where instruments such as these are used to determine ownership, liability, oversight, and more.

The instruments that comprise, at its core, a municipality's set of land records are:

> (a) A town clerk shall record in the land records, at length or by accurate, legible copy, in books to be furnished by the town:
>
> (1) deeds;
>
> (2) instruments or evidences respecting real estate;
>
> (3) writs of execution, other writs or the substance thereof, and the returns thereon;
>
> (4) hazardous waste site information and hazardous waste storage, treatment, and disposal certifications established under 10 V.S.A. chapter 159;
>
> (5) underground storage tank information under 10 V.S.A. chapter 59;
>
> (6) municipal land use permits (as defined in section 4303 of this title) or notices of municipal land use permits as provided for in subsection (c) of this section, notices of violation of ordinances or bylaws relating to municipal land use, and notices of violation of municipal land use permits;
>
> (7) denials of municipal land use permits;

[38] 27 V.S.A. § 402

(8) permits, design certifications, installation certifications, and other documents required to be filed by the provisions of 10 V.S.A. chapter 64 and the rules adopted under that chapter;

(9) other instruments delivered to the town clerk for recording.[39]

Additionally, trust mortgages may also be recorded:

> Trust mortgages may be recorded by furnishing the clerk with a printed copy thereof on not smaller than 8 1/4 by 10 3/4 nor larger than 10 1/2 by 16 ledger paper of good quality with good cloth binding which volume after being duly compared with the original mortgage shall be filed, attested by him or her and kept in his or her office as a trust mortgage record. The clerk shall also certify on a blank page of the then current mortgage record book the recording of such mortgage under the provisions of this section and index the same as provided in section 1154 of this title.[40]

The landmark environmental planning and conservation bill, Act 250 of 1970, added additional requirements, but most important is the broad requirement that "no person shall sell or offer for sale any interest in any subdivision located in this State, or commence construction on a subdivision or development, or commence development without a permit."[41] Furthermore,

> Except as to transfers which are exempt pursuant to subdivision 9603(17) of this title, no town clerk shall record, or receive for recording, any deed to which is not attached a properly executed transfer tax return, complete and regular on its face, and a certificate in the form prescribed by the Natural Resources Board and the Commissioner of Taxes that the conveyance of the real property and any development thereon by the seller is in compliance with or exempt from the provisions of 10 V.S.A. chapter 151. The certificate shall indicate whether or not the conveyance creates the partition or division of land. If the conveyance creates a partition or division of land, there shall be appended the current "Act 250 Disclosure Statement," required by 10 V.S.A. § 6007.[42]

---

[39] 24 V.S.A. § 1154
[40] 24 V.S.A. § 1155
[41] 10 V.S.A. § 6082
[42] 32 V.S.A. § 9608

Additionally, the State of Vermont levies a tax on the transfer of property[43], wherein the property transfer tax return[44] is also required to be filed and recorded in the land records by the Town Clerk.

While not completely comprehensive, these comprise a typical set of records that would be found in a Town Clerk's land records. The intent of the legislature is clear: governmental areas of accountability such as taxation and finance, environmental protection and conservation, consumer protection, public safety, and tort law are supported and recorded in land records. There is substantial public and private interest in understanding how land is used, who owns it, and the consequences of the actions of land owners and users. Furthermore, many towns and their land records predate the establishment of Vermont as a state and might be the single longest complete record of a legal process in it. Records of land use are among the most valuable longstanding assets in the State of Vermont.

The process for recording these conveyances and instruments holds a central place in ensuring the validity of these transactions. Nothing is official in terms of ownership until a "conveyance of land or of an estate or interest therein may be made by deed executed by a person having authority to convey the same, or by his or her attorney, and acknowledged and recorded as provided in this chapter [Title 27, Chapter 5]."[45] Thus, the conveyance is not made until it is acknowledged [by the Town Clerk] and recorded [in the land records]. Thus, the *act of recording* is the act that makes the conveyance official; until such time as the transaction is recorded, it is not yet valid. "An estate or interest in lands shall not be assigned, granted, or surrendered unless by operation of law or by a writing signed by the grantor or his or her attorney."[46] 27 V.S.A. § 342 requires that "a deed of bargain and sale, a mortgage or other conveyance of land in fee simple or for term of life, or a lease for more than one year from the making thereof **shall not be effectual** to hold such lands against any person but the grantor and his or her heirs, unless the deed or other conveyance is acknowledged and recorded." To wit:

> Deeds and other conveyances of lands, or of an estate or interest therein, shall be signed by the party granting the same and acknowledged by the grantor before a town clerk, notary public, master, or county clerk and recorded at length in the clerk's office of the town in which such lands lie. Such acknowledgment before a notary public shall be valid without an official seal being affixed to his or her signature.[47]

---

[43] **32 V.S.A. § 9602**
[44] 32 V.S.A. § 9606(a)
[45] 27 V.S.A. § 301
[46] 27 V.S.A. § 302
[47] 27 V.S.A. § 341

Historical context aside, including these records in the custody of the town clerk helps to preserve the *marketability of title* to parcels of land. Marketability in this case indicates that a title is unencumbered by anything that would cause a reasonable threat of litigation, such as liens, mortgages, easements, zoning violations, and more. Since property, especially real estate, can carry a significant monetary value, it is often used to secure substantial loans (mortgages) and generally can comprise a significant portion of an individual's net worth investment.

While the role of the municipal clerk is small, it is essential. The municipal land records serve as the consolidated record of the ownership, development, and use of land. Much context for these records is found elsewhere: Act 250 permits and related documentation with the Natural Resources Board, property tax and transfer tax information with the Department of Tax, zoning and permitting at the municipal level (and sometimes State level). But in no other place is there a complete record of both the chain of ownership (necessary to prove marketability of title) and the actions taken on that land. Due to this, and due to the legislature's understanding that uniformity in recording would serve Vermonters well, these requirements are in place to ensure a consistent and reliable source of information that can be trusted.

Blockchain Technology and Vermont's Land Records

Blockchains and land transactions might seem like a natural fit: individual parcels of land change hands and since the monetary and legal stakes are so high, the various parties to a land transaction (grantor, grantee, issuers of mortgages and other loans, permitting agencies) have come to trust in the government standing as the third party to the transaction. That role is assigned in law to the Town Clerk, as the agent of the government in this scenario, who has the responsibility to record the transaction and associated instruments. There is very little to no oversight role; the clerk does not judge whether the transaction is valid, only whether the proper instruments have been filed and recorded appropriately.

A blockchain on its face seems like it could accomplish the same task. The grantor and grantee could come to terms and record all necessary records of the conveyance, along with any other instruments, in a blockchain. Blockchains could, through a token model perhaps, prevent the "double-spend" issue of ownership, only allowing rightful owners (as evidenced through the chain of ownership that could be demonstrated in the entirety of the register) the ability to convey their title. Furthermore, the immutability of the chain itself would prevent any alteration to the records. To utilize blockchains for land records, some changes to the legal framework in Vermont would need first need to occur to pave the way for more widespread use of modern technology.

One such legal framework can be found in the Uniform Real Property Electronic Recording Act (URPERA), finalized by the National Conference of Commissioner on Uniform State Laws in 2004 and subsequently adopted by a number of US States. Following closely after the Uniform Electronic Transactions Act (UETA), which has already been enacted and codified into Vermont law, URPERA seeks to update and standardize the body of legal requirements surrounding the recording of land transactions in a world where parties are able to transact business, by agreement, electronically. Enacting URPERA and updating Vermont's real estate recording laws would untie the hands of many of the actors involved in the recording process, allowing more widespread adoption of electronic systems for the recording of real estate transactions, possibly paving the way to utilize blockchains or other technologies.

The first major provision of URPERA is that any requirement for analog or paper recording would be fulfilled by "an electronic document satisfying this [act]," an electronic document having essentially the same meaning as it does in the context of UETA. Additionally, like UETA, the law would allow for electronic signatures to replace wet-ink signatures on the various instruments that are required and comprise the documentary evidence of the land transaction.

Additionally, URPERA allows the recorder, in Vermont's context the Clerk of the municipality, the following:

> (b) A [recorder]:
>
> (1) who implements any of the functions listed in this section shall do so in compliance with standards established by the [Electronic Recording Commission] [name of state agency].
>
> (2) may receive, index, store, archive, and transmit electronic documents.
>
> (3) may provide for access to, and for search and retrieval of, documents and information by electronic means.
>
> (4) who accepts electronic documents for recording shall continue to accept paper documents as authorized by state law and shall place entries for both types of documents in the same index.
>
> (5) may convert paper documents accepted for recording into electronic form.
>
> (6) may convert into electronic form information recorded before the [recorder] began to record electronic documents.

(7) may accept electronically any fee [or tax] that the [recorder] is authorized to collect.

(8) may agree with other officials of a state or a political subdivision thereof, or of the United States, on procedures or processes to facilitate the electronic satisfaction of prior approvals and conditions precedent to recording and the electronic payment of fees [and taxes].[48]

One significant obstacle are other requirements to the recording of land records which currently require an analog process. For example, 27 V.S.A. § 341 requires that the grantor and grantee shall sign the deed before a notary public; since Vermont law does not provide for electronic notarization, the ability of parties to e-record land records might be hindered as the scan or facsimile of a notarized document is not automatically itself similarly notarized. If these laws were updated, it would pave the way to allow fully-electronic transacting of land conveyances and pave the way for electronic recording at municipal offices.

However, even with these changes, the majority of land recordkeeping has been done in an analog format that is almost completely disconnected from the web or any electronic system. If Vermont were to choose to move to a digital recording system, changes would need to be made to this technological infrastructure. Firstly, the State would need to strongly consider beginning with an electronic accounting and set of electronic records that comprised a record of land ownership, encumbrances, and other documentary evidence that was complete. That is, the relevant instruments related to every unit or parcel would need to be available electronically. For example, if using a blockchain, one might be able to assign a parcel to a specific "unit" registered in the chain. This would then allow the owner to transact business with that unit, either conveying it to another party or registering additional instruments in the chain related to it. Doing so would allow the State to begin with a comprehensive new system rather than a piecemeal one that bifurcates new and existing land records.

However, doing so would require true statewide coordination and collaboration, as well as a statewide standards body that oversaw the paper to electronic transition to ensure that the efforts to digitize or at least begin with some set of records were done with consistency. Additionally, if blockchains were to be utilized for this purpose, it calls into question the value or role of the Town Clerk. Certainly, if only hashes were to be stored within the blockchain, the original records from which those hash values were derived would need to be stored somewhere that was publicly accessible (if the role of the blockchain is not to validate but instead to store for posterity the transactions so that the

---

[48] Uniform Real Property Electronic Recording Act

public can audit their veracity); while that storage of records could be at the town level, given the funding level and technological resources available to most Vermont towns, it would make more sense for these master records to be stored in a statewide repository. Secondly, if there is no electronic recordkeeping requirement, and if the State truly wishes to push the transacting of land entirely to blockchains not controlled by the State, there is no role here for the Town Clerk to fill except perhaps to provide a computer and web access through which citizens could access the blockchain to verify transactions themselves.

Blockchains could be leveraged as part of a suite of technologies to better manage land transactions; for example, each town in the State of Vermont could participate as a node in a blockchain and verify transactions submitted by private parties transacting land. Additionally, the Department of Tax, Secretary of State, and other statewide entities could similarly participate and fulfill their individual roles either through reading transactions in this blockchain or registering their own instruments. This effectively would make fully electronic and public (and unalterable) the register of all land transactions in the State of Vermont. However, private blockchains and government-controlled or –operated blockchains specifically, beg the question: why even use blockchain technology at all? The State would be better served by developing a unified State and Municipal collaboration to unify and digitize the methods and records associated with recording land transactions.

Furthermore, updating Vermont's laws to allow for e-recording and e-notarization would allow private citizens to transact business in whatever manner they might like, while not compelling the State or its municipalities to substantially invest in new technology. Citizens can make any number of financial transactions using blockchains currently, but this doesn't mean that the State is required to allow pointers to blockchain transactions when citizens file their taxes. The State can modify its recording requirements to allow the submission of electronic records that are *also* registered in blockchains; the law can allow for state and municipal requirements to be met while still allowing citizens the freedom to transact business how they wish.

In this case, blockchains do not solve any problems that the State of Vermont and its political subdivisions have. Many of the issues with land records in Vermont are related to the formats in which they are held (volumes and indexes of paper) or process. Vermont should seek to modernize its entire infrastructure before aiming to replace one piece (transactions) with a fully-digital replacement. In fact, more problems might be introduced with having a set of records stored in a blockchain that now, too, must be preserved and have access provided to it. Any issues that might face Vermont's system of recording land transactions are better solved by modernizing the technological infrastructure available to those tasked with this work (town clerks), and centralizing and unifying requirements, standards, and methodologies for coordination at the State level, as to better serve the citizens of Vermont, rather than interjecting a new technology at this problem.

VII. Recommendations

Blockchains are built off fundamentally sound technology and principles. Public-key cryptography is a mathematically-proven method of encrypting data and is widely implemented across the web; however, hundreds of security incidents per year have been the result of phony certificates, or poor encryption, or poor implementation of this technology. Similarly, having redundant copies of records has provided enhanced protection for essential records for archives and other institutions around the world, but contextual loss and irreconcilable errors remain possible. Timestamping and ordination of transactions create internal consistency, but even the consensus requirements can be defeated with enough resources. No system is perfect and blockchains are no different.

For blockchains to be useful for public recordkeeping, public agencies must be able to guarantee the long-term preservation and continued access to public records recorded within. Even for records with short-term value, the need to preserve digital records in blockchains is essential. Fear of long-term sustainability did not prevent the government from using massive ledgers for court dockets, or complex proprietary mainframe systems for data analysis. Rather, it is that commitment, that accountability to continue managing information for its entire lifecycle that is the essential element to public recordkeeping. Technologies come and go. Public records, especially archival records, must endure.

Further, for the government of the State of Vermont to be trustworthy, the citizens must trust its recordkeeping practices, and introducing any element or technology that undermines that trust is exceptionally risky, despite any financial or other gains that might be realized. Based on these requirements, Vermont State Archives and Records Administration, in collaboration with the Vermont League of Cities and Towns, the Vermont Municipal Clerks' and Treasurers' Association, and the Agency of Digital Services recommend the following:

1. Clarifying if recording public records in public or “trustless” blockchains conflicts with 1 V.S.A. § 317a(b) and other sections of the Vermont Public Records Act as State and local governments do not either own or control blockchains.

2. Investing or participating in in-depth technical study, preferably with Federal and state partners, on the long-term preservation requirements of (and the ability to continue to provide access to) permanent records recorded in blockchains;

3. Vetting or otherwise certifying the technical protocols, sustainability, and trust models of any blockchain before records sourced from it are used in an evidentiary process. Any government-utilized blockchain would similarly need to be vetted, much as the Agency of Digital Services currently provides oversight and consultation on technology contracting.

4. Promoting broader collaboration between the archival and records and information management communities and the blockchain community. If blockchain technology is going to offer trust and security in recordkeeping, collaboration between technologists and archivists will be essential to ensuring that requirements are met.

5. Establishing a formal collaboration between blockchain users (including State agencies, especially the Agency of Digital Services) and those responsible for long-term digital preservation of electronic records to assure recordkeeping requirements are met.

Any technical solution that public agencies in the State of Vermont pursue should be free from any contractual or technological burden; that is, any system of record, by necessity, must be extensible, interoperable, and most of all, the data within these systems must have a simple, straightforward, and lossless migration pathway to new systems. Government is already burdened with legacy technology and should seek to reduce its technological debt whenever possible.

Extensibility and flexibility when choosing systems, especially recordkeeping systems, should also be a priority for the State of Vermont. The lifecycle of public data can be long and possibly much longer than the life of the technology providers or public officials involved in its creation. It is of minimal value for the State to modernize its recordkeeping infrastructure only to become reliant on a single vendor, or a single technology, that might soon become outdated or obsolete (or worse, insecure).

Further, any mandate to digitize or otherwise allow electronic recording of land records will need to be adequately funded; most municipal clerks do not have modern technological infrastructure or training to be able to design, implement, contract, or sustain an initiative on this scale without additional funding and other resources. Similarly, the State would be well-served by having a statewide body coordinating this effort given that there are many actors (state, municipal, and private) that have a stake in the outcome of this process.

Therefore, the Vermont State Archives and Records Administration, in collaboration with the Vermont League of Cities and Towns, the Vermont Municipal Clerks' and Treasurers' Association, and the Agency of Digital Services also recommend the following:

1. Adopting the Uniform Real Property Electronic Recording Act (URPERA). This legislation would modernize Vermont statutes and allow individual municipalities electronic record land records when they are able to provide the necessary guarantees that they can preserve, protect, and provide access to these records in perpetuity as required by law. Towns without such ability would be able to continue operating without any changes to current processes.

2. Developing and implementing a sustainable infrastructure for electronic notarization and authentication to ensure that the entire scope of a land transaction can be captured in the same environment, preserving necessary context. Any practical solution should not have both analog and digital records stored in multiple locations without contextual links.

3. Re-examining the role of municipal clerks in this context to ensure that repetition and duplication is eliminated whenever possible.

4. Charging the land records governing body established by URPERA, which establishes the requirements, policies, and procedures for creating, managing, and preserving land records, regardless of the technology utilized, to evaluate blockchains for these purposes.

If blockchain technology is deployed, the Vermont State Archives and Records Administration and its collaborators on this report further recommend:

1. Implementing a succession plan, in case of any compromise or obsolescence of blockchain solutions. Specific attention must be paid to the future extraction of data from the blockchain chosen in the case of migration or different directions.

2. Registering each parcel's ownership in the blockchain initially to ensure that there is a complete register of land ownership as developing a system by which only new transactions are registered in the blockchain could quickly cause a fractured system where some of the state's records are in electronic format and the other half in town vaults; this would place a large burden on those viewing or auditing both and likely affect marketability of title.

3. Individually recording all land instruments and assure that each local and state public agency has a recordkeeping process that intersects with the blockchain to ensure instruments (e.g. permits, liens, etc.) are registered appropriately.

4. Routinely auditing blockchains to ensure requirements are being met.

VIII. Conclusions

This goal of this white paper is to provide a foundation for the understanding of both the requirements for public recordkeeping in Vermont, with additional detail and background on the importance of land recording, as well as an understanding of what blockchain technology can offer. Blockchains are tools and like all tools, they can be constructed well just as they can be constructed poorly. They can also be used well or used poorly.

Blockchains do have potential for recordkeeping generally, but specific steps need to be taken to determine in what way blockchains will be suitable for public recordkeeping. Just as an information technology professional would not recommend a database for what could be accomplished by a spreadsheet, blockchains will not be the solution to every recordkeeping requirement. Ultimately, a blockchain can be used to do any number of tasks, but it may not be the ideal tool, and, as demonstrated, the cost of implementation and sustainability is potentially high.

References

Becker, Georg. (2018) *Merkle Signature Schemes, Merkle Trees and their Cryptanalysis*. Ruhr University Bochum.

Electronic Records Management Software Applications Design Criteria Standard, DoD 5015.02-STD. United States Department of Defense. (2007) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/501502std.pdf

ISO 15489-1:2016(en); Information and documentation — Records management — Part 1: Concepts and principles. https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en

Keller, Jared Robert. October 18th, 2018. *Challenges in using blockchains to build trust in digital archiving.* Retrieved from. https://theodi.org/article/challenges-in-using-blockchain-to-build-trust-in-digital-archiving/

Lemieux, Victoria L. (2017). A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation. *2017 IEEE International Conference on Big Data (Big Data).* DOI: 10.1109/BigData.2017.8258180

Lemieux, Victoria. (2016). Blockchain for Recordkeeping; Help or Hype? DOI:10.13140/RG.2.2.28447.56488.

Lemieux, Victoria (2018). Preserving the Archival Bond in Distributed Ledgers: A Data Model and Syntax. *WWW '17 Workshop on Linked Data and Distributed Ledgers.* DOI: 10.1145/3041021.3053896

InterPARES Project: http://www.interpares.org/book/index.htm

Nakamoto, Satoshi. (2008). Bitcoin: A peer-to-peer electronic cash system.

National Institute for Standards and Technology. (2018). *NISTIR 8202, Blockchain Technology Overview*, https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

Popper, Nathaniel. June 17, 2016. A Hacking of More Than $50 Million Dashes Hopes in the World of Digital Currency. *New York Times.*

Requirements for Assessing and Maintaining the Authenticity of Electronic Records http://www.interpares.org/book/interpares_book_k_app02.pdf

Uniform Real Property Recording Act http://www.uniformlaws.org/shared/docs/real%20property%20electronic%20recording/urpera_final_apr05.pdf

Vermont Data Processing Study, Committee to Study State Government, 1958.
https://www.sec.state.vt.us/media/839848/vt_dataprocessingstudy_1958.pdf

Vermont. Governor Phil Scott. Executive Order 06-17
https://governor.vermont.gov/sites/scott/files/documents/EO%206.IT%20REORG%20FINAL.pdf

Vermont. Secretary of State, Attorney General, Department of Financial Regulation. Blockchain Technology: Opportunities and Risks. (2016) https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf