BLOCKCHAIN TECHNOLOGY:

OPPORTUNITIES AND RISKS

A report of findings and recommendations concerning the potential opportunities and risks of creating a presumption of validity for electronic facts and records that employ blockchain technology and addressing any unresolved regulatory issues.

JAMES CONDOS, SECRETARY OF STATE
VERMONT SECRETARY OF STATE

WILLIAM H. SORRELL, ATTORNEY GENERAL
VERMONT OFFICE OF ATTORNEY GENERAL

SUSAN L. DONEGAN, COMMISSIONER
VERMONT DEPARTMENT OF FINANCIAL REGULATION

JANUARY 15, 2016

VERMONT

Table of Contents

Summary

- A valid blockchain is a reliable way of confirming the party submitting a record to the blockchain, the time and date of its submission, and the contents of the record at the time of submission.
- A blockchain is an electronic ledger (register) of digital records, events, or transactions that are represented in condensed form known as a hash (digital security feature), authenticated, and maintained through a "distributed" or "shared" network of participants using a group consensus protocol (multiple users).
- Blockchain technology is already in use in the private sector, though clearly in the early stages of adoption, the most prevalent example being virtual currency known as Bitcoin.
- At present, the costs and challenges associated with the use of blockchain technology for Vermont's public recordkeeping outweigh the identifiable benefits.
- Providing legal recognition of blockchain technology may create a "first mover" advantage with the potential to bring economic activity surrounding the development of blockchain technology to Vermont, but this potential is difficult to quantify and challenging to capture due to the nature of the technology.

Introduction

Pursuant to Section A.3 of Act 51 of 2015, an act relating to promoting economic development:

> On or before January 15, 2016, the Secretary of State, the Commissioner of Financial Regulation, and the Attorney General shall consult with one or more Vermont delegates to the National Conference of Commissioners on Uniform State Laws and with the Center for Legal Innovation at Vermont Law School, and together shall submit a report to the General Assembly their finding[s] and recommendations on the potential opportunities and risks of creating a presumption of validity for electronic facts and records that employ blockchain technology and addressing any unresolved regulatory issues.[1]

This report is compiled by the Office of the Vermont Secretary of State, the Department of Financial Regulation, and the Office of the Attorney General, in consultation with Oliver Goodenough of the Center for Legal Innovation at Vermont Law School, and Carl Lisman, a Vermont delegate to the Council of Commissioners on Uniform State Laws.

A blockchain is an electronic ledger of digital records, events, or transactions that are cryptographically hashed, authenticated, and maintained through a "distributed" or "shared" network of participants using a group consensus protocol. Much like a checkbook is a ledger of one's personal financial transactions, with each entry indicating the details of a particular transaction (withdrawal or deposit, recipient and sender, amount, date, etc.), the blockchain is a complete listing of all transactions, whether financial or otherwise.[2] However, unlike a checkbook, the blockchain is distributed among thousands of computers or "nodes" with a process for validating transactions that utilizes a group-consensus protocol. Making an addition to a blockchain ledger requires the approval of the network at large making retrospective changes essentially impossible.

Blockchain technology's most disruptive aspect is its ability to eliminate the need for third-party intermediaries in some transactions. The technology is, in the words of its creator, a "system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other

[1] Act 51 of 2015, § A.3.

[2] The theoretical and speculative applications for blockchain technology are too numerous to detail in this report, but a small sample of the types of uses for this technology includes: transfer of digital securities, digital identification verification, escrow services, and more.

without the need for a trusted third party."[3] Because many industries rely upon guarantors, authenticators, and "trusted third parties" (in fact, they are often industries themselves), blockchain technology is likely to be extremely disruptive.

This report provides a high-level summary of how blockchain technology works. It also discusses current applications of blockchain technology and possible future applications – in both the context of private transactions and public records. Finally, the report addresses some of the possible economic opportunities connected with blockchain technology as well as risks associated with both the technology and its uses.

While the study group evaluated blockchain technology generally, its impact will be affected most by its implementation. Evaluating the soundness of blockchain technology is akin to evaluating the efficacy of a lock. Just as the security of a lock is called into question if everyone in town has a copy of the key, the security of the blockchain is heavily dependent on its protocols– how it verifies transactions, what encryption algorithms are used, and more. Without proper implementation, as with any tool or technology, the efficacy of the blockchain will be compromised.

Section 1: Blockchain Technology Overview

This report does not attempt to provide an in-depth, academic study of the underlying technology of blockchain. Numerous scholars, entrepreneurs, and jurists have covered at length and with greater technological proficiency the details of blockchain technology.[4] Instead, the report explains the underlying building blocks that comprise blockchain's technological foundation. Though each implementation may vary, a few key elements are characteristic of blockchain:

- creation and maintenance of an electronic register of transactions,
- encryption of hashes (digests) of transactions,

[3] (Nakamoto, 2008)
[4] For a more thorough primer on blockchain technology, please see Appendix A for resources.

- validation or verification of those transactions; and
- timestamping those transactions.

The protocols which implement these elements in a particular blockchain influence the reliability of the information contained therein.

Electronic Register of Transactions

Any system that records data must have a format and location for storing it. A register of transactions or other records is simply a list of every transaction that has been recorded by the system. For example, a municipality's register of title and deed transfers and the aforementioned checkbook are registers. The blockchain is a continually-growing digital register of transactions. Each set of transactions (the number of which is prescribed by the protocol) is considered a block in the chain, and the register as a whole is the *blockchain.* This chain is stored and continually added to by a network of computers, each of which is known as a *node*. Each node has, at minimum, a copy of a certain number of the most recent blocks, and some might possess a copy of the entire blockchain. To add a block to a chain, parties broadcast to the network the details of the transaction, and nodes verify these transactions, as described below. Once a node has verified the prescribed number of transactions, and solves additional

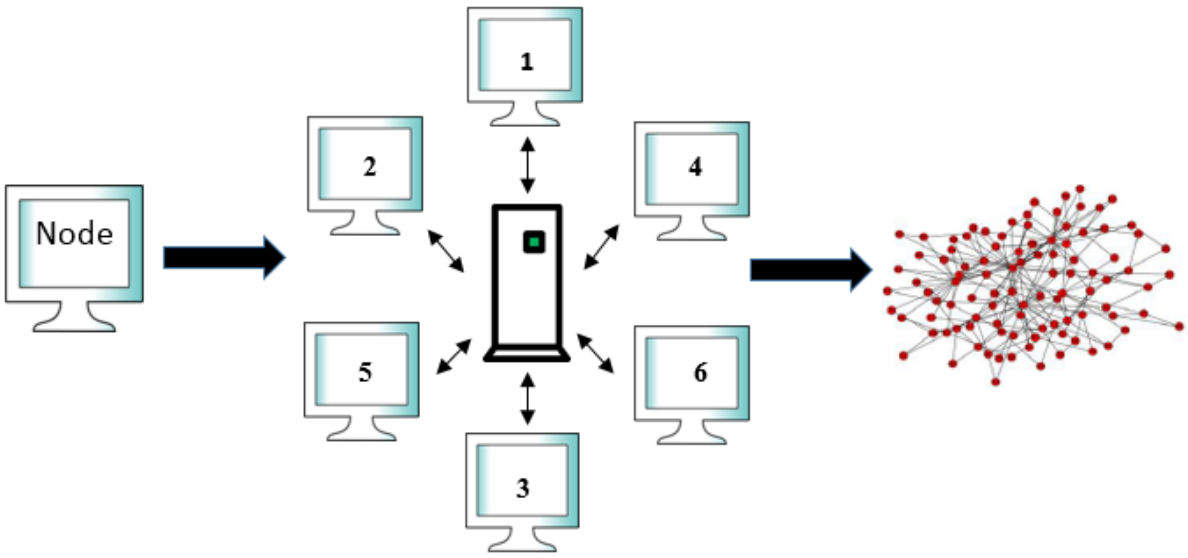

Figure 1: Nodes independently verify transactions before agreeing on those that are valid

computational problems dictated by the protocol, that block can be added to the chain (see Figure 1). Other nodes add it to their chain as well. In this way, the blockchain grows mostly identically at each of the individual nodes. The responsibility for storage of the transaction ledger is distributed to many individuals, adding redundancy with little risk of corruption or errors.

Encrypting Data

One of the fundamental pieces in digital security is the encryption of information; the translation of one piece of data into another using a mathematical algorithm so that the original data is obscured and can only be accessed by the intended recipient(s). Encryption pervades nearly every aspect of digital recordkeeping and the transaction of business of all kinds over the internet, in both public and private contexts. However, it is important to distinguish between two types of the same technique. First is what is typically called encryption, which is essentially a one-for-one translation from one set of data to another. If a document is encrypted using a mathematical formula, it can be decrypted to produce the original document.

Blockchain technology typically uses the encryption method known as cryptographic hashing. When a transaction is submitted, the contents of that transaction plus a few key pieces of *metadata* (including the timestamp and the parties involved) are encrypted using a mathematical algorithm. The output is known as a hash;[5] a short digest of the data. An electronic record run through the cryptographic hashing algorithm using a particular key (or set of keys) will always produce the same hash. Any change, however insignificant, in the document will cause the hash to be significantly different. Furthermore, since the hash is merely a short digest of the original, it is not possible to decrypt a *hash* maintained in the blockchain and produce the original document, but it is possible to use the *hash* to verify a copy of a transaction or document maintained outside of the blockchain. Blockchain technology uses cryptographic hashing to save space. It rapidly becomes impractical or impossible to maintain the entire ledger if every

[5] See Appendix A for examples of cryptographic hashes.

encrypted document is fully registered, and the computing costs to decrypt entire transactions would be very large.

Verification of Transactions

Each party to a transaction has two keys: a public key, which is known to the world, and a private key, which is kept secret. These keys are digital certificates stored on the user's computer systems that allow for the encryption and decryption of data. A sender uses his or her key to encrypt the transaction data. The recipients, in this case all nodes in the network, use the public key to decrypt information required by the blockchain's protocol to validate the transaction. Examples of required information include the digital signature of the sender, knowledge that the sender has not previously sent a conflicting update, and that nothing else in the update is invalid. This technology is nearly identical to that used in many existing digital signature or e-sign technologies; a sender generates a digital signature from his/her private key which can then be verified by anyone using his/her public key.[6] This technique is an essential and proven technique for securing communications over potentially insecure channels and has been in use in the public and private sector for decades.

A blockchain user or group of users will cryptographically hash the record of any transaction. This hash is then broadcast to the network as the evidence that a particular transaction has occurred or event has been logged. Individual network nodes receive this broadcast and begin the process of ensuring that it is valid in accordance with the protocol of that particular blockchain. Once a requisite number of nodes agree that a set of transactions is valid (i.e., reaching a consensus), those transactions can be added to the chain as a block, and future blocks can be built upon the information contained therein. This ensures continuity of transactions and an unbroken transaction history. (See Figure 2)

[6] See the work of Rivest, Shamier, and Adelman for a more in-depth analysis of public key cryptography.

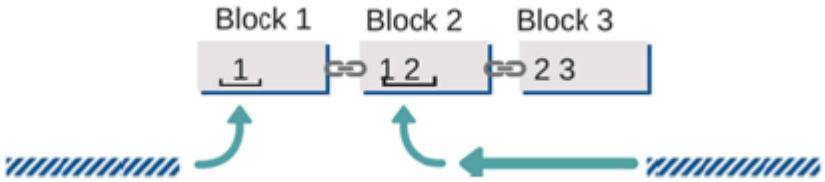

Figure 2: New blocks are added to the chain, and are linked to previous blocks

The advantage of the distributed network is the individual work done by each node. But verification involves significant computational work, so nodes are typically compensated for their contribution of computing power. Whether that compensation takes the form of monetary rewards, additional uses of the service, or another form depends on the protocol of the blockchain. The compensation of nodes ensures continued participation. Should participation cease, the chain effectively ends and becomes useless as a service (as few incentives would remain for storage or verification).

Timestamping

The link that ties individual blocks together is the timestamp. Recording the timing of the transaction is essential to the nature of the blockchain. The chain is only appended, never retrospectively edited. When a node verifies a transaction, it checks it against (among other things) timestamps of previous transactions. This is done to ensure that, for example, if an individual transacts 1 unit at 12:00 and that same unit at 12:01 and tries to record both, the network will come to the consensus that the second transaction is invalid. Similarly, this allows data stored in the blockchain to be placed in chronological order. This timestamp references the timestamp of the previous transaction as well, effectively making a "chain" of transactions. Individual timestamps are also encrypted and sourced from a trusted timestamp server, making the timestamps resistant to compromise.

Each block added to the chain is mathematically linked to the block before it, as well as to those blocks following it. This is done through a linking of the timestamp, the hash of the previous block, the

hash of the entire chain, *et cetera*, depending on the protocol. Because of the distributed, consensus-driven nature of the blockchain it is nearly impossible for an attack to compromise the entire system. The number of nodes (and attendant computing power) required to confirm an error or malicious attack would be impractical in a large blockchain like Bitcoin. Trying to forge a previously verified block would be akin to changing the shape of a brick in an ever growing stack – each subsequent brick would also need to be modified to fit with the previously one. The blockchain is resistant to compromise due to the nature of the linked blocks. However, as will be discussed, there are ways the use of this technology is vulnerable to compromise, but they are not fundamental vulnerabilities with the blockchain itself.

Section 2: Application of Blockchain Technology to Records

Record accuracy and trustworthiness, especially in the context of electronic records, is critical to the usefulness of the record. [7] A record that cannot be trusted effectively cannot be used. The measure of trustworthiness is primarily based on the reliability, accuracy, and authenticity of the record.

> Reliability is defined as the trustworthiness of a record as a statement of fact, based on the competence of its author, its completeness, and the controls on its creation; accuracy is defined as the correctness and precision of a record's content, based on the above and on the controls on the recording of content and its transmission; and authenticity is defined as the trustworthiness of a record as a record, meaning that the records is what it purports to be, free from tampering or corruption, based on the competence of its keeper(s) through time (i.e. creator and/or preserver) and on the reliability of the records system(s) in which it resides.[8]

Blockchain technology does not address the reliability or accuracy of a digital record. Instead, it can address a record's authenticity by confirming the party or parties submitting a record, the time and date of its submission, and the contents of the record at the time of submission.

Blockchain technology offers no assistance in terms of the reliability or accuracy of the records contained in the blockchain; if bad data is used as an input, as long as the correct protocols are utilized, it will be accepted by the network and added to the blockchain. If a document containing false information is hashed as part of a properly formatted transaction, the network will validate it. Furthermore, the

[7] (Gladney, 2009)
[8] (Duranti & Rogers, 2012, p. 525)

network is unable to distinguish between a transaction by an actual user and a malicious transaction by someone with unauthorized access to the user's private key. Furthermore, the network could obviously could not through its protocols determine whether a sender was reliable in terms of the veracity of their submitted information.

Where blockchain technology does provide an advantage is in its ability to evaluate the authenticity of records. As explained above, a transaction that has been verified and added to a valid blockchain is mathematically secure. The hash of a document existing outside the blockchain and the hash registered within the blockchain will be identical if the documents are identical. If the documents are different (due to forgery, corruption, error, or other problems) the hashes will not match. Thus, the blockchain can potentially provide an immutable registration of a record, to which future records can be compared for authenticity. Any presumption of validity around records registered in a blockchain must be limited to authenticity. The statutory language set forth in Appendix B reflects this distinction between *reliability/accuracy* and *authenticity*.

Section 3: Private Transactions and Existing Legal Structure

Information is essential to any individual or organization for a multitude of purposes: proof-of-fact, legal or regulatory compliance, efficiency of operations, accountability and transparency, and more.[9] Blockchain technology is a tool for the management of information, specifically the records of transactions. Whether the content of that transaction is the hash of a transfer of Bitcoin from one wallet to another, a contract agreed to by two parties, or a document registered for purposes of future verification, each of these instances represents the creation of an electronic record that is encrypted, distributed, verified, and eventually added to an ever-growing ledger of other transactions.

Private recordkeeping may benefit, through reduced costs, from utilizing blockchain technology to eliminate centralized recordkeeping or authenticity-verifying authority. Two issues complicate these

[9] (ARMA International, 2014)

possible advantages. First, the blockchain does not store documents, only hashes. Parties transacting business in a blockchain would need to preserve electronic documents themselves (which could be confirmed by comparison to the hashes in the blockchain). Private individuals and organizations are often not well-equipped for the long-term preservation of their electronic records.[10] Second, while a blockchain may reduce costs, there will likely still be some transaction fees related to verification, as described above.

The existing legal framework in Vermont for use and validity of electronic transactions and records is set forth in the Uniform Electronic Transactions Act ("UETA").[11] UETA provides a broadly-defined legal framework for parties who wish to conduct electronic transactions in Vermont. Most uses of blockchain technology, although not specifically identified, would fall within the recognition provided to electronic records, signatures, and contracts afforded by UETA.[12] However, UETA's recognition of electronic transactions is limited in some respects, including by the application of other statutory requirements.[13]

While UETA may cover many of the transactions for which people currently contemplate utilizing blockchain technology, it does not cover everything. A transaction under UETA is "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs."[14] Prospective uses for the blockchain are not limited to the transaction of business between two parties. In certain situations, a single party may wish to register some information in the blockchain; for example, a will or other document with long-term value. Such single-party registrations are not transactions within the meaning of UETA (although still constituting "transactions" in the blockchain sense), and thus might not be covered by UETA. Blockchain-specific legislation could account for such records.

---

[10] (Gladney, 2009)
[11] 9 V.S.A. ch. 20.
[12] *See* 9. V.S.A. § 276.
[13] *See, e.g.*, 9 V.S.A. §§ 275, 277.
[14] 9 V.S.A. § 271(17)

UETA is intended to be a broadly construed authorization with respect to electronic transactions, but creates no obligations for their use.[15] Under UETA, in litigation, electronic transactions and records are treated in the same manner as manual or paper records.[16] There is no indication that current law prohibits or in any way disfavors the use of blockchain for electronic transactions, but to the extent the legislature wishes to clarify this recognition, it should be done outside of the bounds of UETA. Modifying the uniform statute may undermine both its uniformity and its approach to broadly address dynamic and changing technologies. It may also trigger pre-emption of Vermont's version of UETA by the federal E*SIGN law.

Section 4: Public Implications of Blockchain Technology

Public records are essential to the state of Vermont both for the fulfilling its statutory responsibilities and for the public to inspect and monitor the actions of public servants. State law makes this clear: "Officers of government are trustees and servants of the people and it is in the public interest to enable any person to review and criticize their decisions even though such examination may cause inconvenience or embarrassment."[17] Ultimately, state government is accountable to the people, and the inspection of records provides one of the primary means for ensuring this accountability. Additionally, Vermont defines public records concisely:

> "public record" or "public document" means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of public agency business.[18]

Electronic data created or received by the state of Vermont in the course of business is a public record, and must be managed according to the requirements set forth in Title 1, Chapter 5, Subchapter 3. Therefore it is of the utmost importance for the State to use recordkeeping systems and implement records

[15] 9 V.S.A. § 274
[16] 9 V.S.A. § 282 ("I n a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.")
[17] 1 V.S.A. § 315(a)
[18] 1 V.S.A. § 317(b)

management policies that produce and preserve trustworthy electronic records and safeguard against the risks of loss of those records.

Public records are held in the custody of the state, whether that is an agency or an individual acting in his or her capacity as an officer of that agency. Although 1 V.S.A. § 318 outlines the responsibility of the custodian in specific circumstances, the custodian of a public record is charged with the responsibilities of preserving and providing access to the records.

> A public officer, by virtue of his or her office, is the legal custodian of all papers, books, and records pertaining to his or her office. It is the custodian's duty to preserve the public records, and to ensure that nobody alters or destroys them. The custodian is also responsible for delivery of such documents to his or her successor. The law presumes that a public officer will properly perform his or her duty as to the care, management, and control of records, and their preservation, and if a particular paper is not found in a public office where, if in existence, it ought to be, it will be presumed that it never existed.[19]

There ought to be an unbroken chain of custody from the point of creation or receipt of a record through its active and inactive life until its final disposition.[20] Inserting an existing public record into any system employing blockchain technology could violate legal expectations relating to the custody and control of public records.

At present blockchain technology adds little in terms of public recordkeeping. The records kept by the State are presumed reliable and accurate in terms of content. Moreover, effective records management policies and procedures by agencies should address the authenticity of records. The need to preserve copies of electronic records for long periods of time is already essential to state business and strategies and tools are in place to address these needs. Because blockchain technology would likely result only in the registration of hashes, the state would still need to preserve original documents long-term. In light of the very limited possible benefits and the likely significant costs for either entering into a private or public blockchain or setting up a state-operated blockchain, at this time, blockchain technology would be of limited value in conducting state business.

---

[19] 76 C.J.S. Records § 37 (2015)
[20] http://content.arma.org/IMM/Libraries/Sept-Oct_2011_PDFs/IMM_0911_RIM_fundamentals_records_life_cycle.sflb.ashx

Section 5: Digital Currency / Securities

Blockchain technology appears ideally suited to alter the way in which financial assets are currently transacted, affecting capital markets, clearing houses, and exchanges with broker-dealers and banks. Systems that currently rely on a trusted middleman to support and/or guarantee the authenticity of a transaction today could efficiently be conducted using the blockchain. The financial industry is beginning to accept the utility of blockchain technology and certain functions within the sector are already using blockchain-based technology for transferring ownership or custody of financial assets. The amount of money the financial industry is investing in this new technology is evidence of the potential utility of blockchain technology to complete such functions. A November 2015 article on CNN.com indicates that financial services firms have invested $1 billion in blockchain-related entities.[21]

Financial services companies cite many benefits of blockchain technology. These benefits include reducing operations staff currently required to transact services through the use of a secure, immutable, reliable digital ledger that is constantly updated, such as a blockchain. Similarly, financial services firms can minimize operational complexity with the use of the blockchain. Currently, securities clearing and trading operations take two to three days to settle a trade. This delay can lead to credit and liquidity risks. Blockchain-authenticated trading (current bitcoin based system) takes minutes. A standalone system could potentially authenticate transactions even faster. Faster transactions reduce the risk of purchaser default. For example, financial institutions that have custody over large financial assets are looking to the technology to help comply with the Dodd-Frank Wall Street Reform and Consumer Protection Act. The efficiency of transactions that blockchain technology can provide may help to reduce counterparty credit risk which may reduce an institution's balance sheet capital requirements under Dodd-

[21] http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested

Frank. Distributed ledgers virtually eliminate credit and liquidity risk by requiring pre-funding, in which the cash and collateral to be traded pre-exist prior to trading.[22]

A securities transaction system entirely based in the blockchain could essentially eliminate the illegal practice of "naked short-selling." Short selling allows a person to borrow securities they do not own and sell them for cash value. The short-seller bets against the market, anticipating the value of the borrowed stock is likely to decrease. Naked short-selling is the illegal practice of short-selling stocks that don't actually exist. This is accomplished by manipulating the time lapse of authenticating a transaction. A distributed blockchain system would essentially prevent such activity because virtually no delay would exist between accepting a trade and closing the transaction.

Vermont banking statutes already address and regulate certain virtual currency transactions, as "money services." Businesses that sell stored value Bitcoins in Vermont are engaged in money transmission, requiring a license.[23] [24]

Similarly, at the federal level, the Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") issued guidance on this subject on March 18, 2013.[25] While a user of Bitcoin (to purchase goods and services) is not under FinCEN's regulatory authority, an administrator or exchanger of Bitcoin is a Money Services Business ("MSB") or "Money Transmitter" and must comply with FinCEN's regulations including those relating to reporting and recordkeeping.[26] [27] The language set forth in Appendix B would not create or carry any presumption that the underlying activity supported by that record is legal. Thus, the applicability of existing civil and criminal laws and regulations governing Bitcoin or other blockchain activities related to securities and money transmission would remain unchanged.

---

[22] (McKinsey & Company, 2015)
[23] See In Re: PYC, Inc.; BLU-BIN, Inc., Docket No. 15-004-B, (March 11, 2015), found at http://www.dfr.vermont.gov/reg-bul-ord/pyc-inc-blu-bin-inc
[24] 8 VSA §2502 (a)
[25] https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf
[26] See FIN-2013-G001
[27] (Jacobsen & Pena, 2014)

Section 6: Blockchain Benefits and Risks

Benefits

Blockchain technology is developing and expanding at a rapid pace. During the drafting of this report, many new developments occurred, and the market for blockchain technology has had several new entrants. As is discussed further in Appendix C, banks, news organizations, and scholars recognize the potential of blockchain as a significant disruptive technology. Private parties will likely utilize blockchain technology for recording transactions and verifying records.

The study group does not doubt the potential economic impact of blockchain technology generally. Possible increases in economic activity could be direct or indirect. The potential direct economic benefits might arise from businesses and parties that utilize the blockchain choosing Vermont law for their contractual relationships. This may result in additional legal and accounting work in Vermont. Indirectly, Vermont's affirmative recognition of this technology may provide cachet that would attract businesses working in this area to locate here, but the study group has no concrete evidence of this. The group sees the greatest potential economic benefit as blockchain-related services (the nodes of networks, the storage of the originals of electronic documents) locating in Vermont, but the nature of the blockchain is opposed generally to the centralization of these services.

To the extent that Vermont can be part of a process of economic and technological innovation that is likely to go forward with or without any legislative recognition, early acceptance of this technology may result in some economic benefit to the State. It is not clear that legislation set forth in Appendix B would successfully lure such activity to Vermont.

Risks

The study group has identified only very limited risks to Vermont associated with express legal recognition of private records utilizing blockchain technology. The underlying principles that underpin this technology are well established, and recognizing it for confirming authenticity of a document seems

well-founded. There are, however, some risks associated not with the technology itself, but with its broader use.

Market Disruption

One effect of blockchain technology could be a massive disintermediation of the financial system. It could replace all of the current procedures that process, record, reconcile, and audit transactions with a system where participants trade directly. While the state may see some small gains in first-mover legal work and a potential blockchain tech startup, the true economic benefits of blockchain transactions are the potential reduction in transaction costs to the participants. The individual economic gain must be balanced by the inevitable losses in employment in those areas where people are no longer needed to perform all of the back-office work. Moreover, any attempt to regulate blockchain may actually make Vermont a less hospitable environment. Currently, blockchain is not subject to any unique regulation. Any regulation that results in additional costs may, in fact, dissuade companies from locating in Vermont.

Consumer Protection

There is no indication that blockchain technology itself creates new consumer protection concerns. When the technology serves as a platform for conducting commercial transactions, it will likely be utilized by some to engage in unfair and deceptive acts and practices in violation of the Vermont Consumer Protection Act.[28] These transactions would remain subject to consumer protection laws, enforceable by the State or by private individuals.

Because Bitcoin is currently the most commonly utilized and understood use of blockchain technology, it is worth noting general consumer risks associated with it. First, because Bitcoin is not backed by a single government or organization (but instead is decentralized) it is subject to significant volatility. Consumers holding Bitcoins risk experiencing wide swings in the value or purchasing power of the Bitcoin they hold. Additionally, because use of Bitcoin as a payment system is not subject to the regulatory scheme of more traditional payment systems, there may be additional risks related to returns

[28] 9 V.S.A. Ch. 63

and transaction reversals. The Federal Trade Commission has identified some of these general risks related to engaging in transactions using Bitcoin.[29] [30]

In addition to the fraudulent or illegal activities conducted using Bitcoin, there are limited consumer protection concerns related to the broader use of blockchain technology. Integral to the technology is the maintenance of private keys by participants. A private key is essentially an additional source of personally identifiable information (like credit card numbers, Social Security numbers, or bank account numbers). Based on current implementations of blockchain technology, if a private key is lost or stolen, an individual has no recourse. At best, a person who loses a private key will be required to obtain a new key to add to the blockchain. At worst, the loss or compromise of a private key is complete loss of control over one's blockchain transactions. The only way to identify someone online in some of these blockchain systems is through the use of a private key; a malicious party could masquerade convincingly as the user until a private key is deactivated. Essentially this creates an additional identity theft risk.

Also, as there are potentially significant rewards in the verification of transactions and the addition of blocks to the blockchain, especially in the case of Bitcoin, there is a great financial incentive to manipulate or otherwise steal computing power (typically in cloud computing environments). This type of criminal behavior has the potential to cause significant losses in the private sector if blockchain technology continues to expand.

Conclusions and Recommendations

Blockchain technology is a sophisticated, interesting, and emerging technology. It provides a reliable way of confirming the party submitting a record to the blockchain, the time and date of its submission, and the contents of the record at the time of submission, eliminating the need for third-party intermediaries in certain situations. However, it is important to consider that blockchain technology does

[29] *See* (Cohen, 2015)

[30] While not fundamental to blockchain technology, Bitcoin, the current implementation of this technology is commonly utilized by individuals to engage in illegal activity because of the anonymity associated with the transactions. http://www.bloombergview.com/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-

not verify or address the reliability or the accuracy of the contents, and additionally blockchain technology provides no storage for records, but instead the hashes thereof.

Regarding economic advantages to legal recognition of blockchain technology, Vermont is currently a hospitable environment for commerce related to blockchain technology even though the State has not recognized this technology in statute at this time. The study committee has not identified any specific legal or practical benefits from the legislation set forth in Appendix B. However, the group has also not identified any risk inherent in blockchain technology that would warrant withholding the recognition of validity set forth in the legislation. While the committee does not doubt that blockchain technology and the industry forming around it demonstrate significant economic activity and interest, it is unclear what steps Vermont could take to lure any of that activity to the state.

Blockchain technology is already in use in the private sector, though clearly in the early stages of adoption, the most prevalent example being virtual currency known as Bitcoin. Further study is required before considering it for the regular business of the State, and moreover, any application would certainly need to support rather than replace the existing records management infrastructure. It is the belief of the study committee that the benefits of adoption of blockchain technology by state agencies is, at this time, not outweighed by the costs and challenges of such implementation.

References

ARMA International. (2014). *Generally Accepted Recordkeeping Principles.* Retrieved from www.arma.org: http://www.arma.org/docs/sharepoint-roadshow/the-principles_executive-summaries_final.doc

Cohen, K. (2015, June 22). *Before paying with bitcoins.* Retrieved from FTC Consumer Information: http://www.consumer.ftc.gov/blog/paying-bitcoins

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654.

Duranti, L., & Rogers, C. (2012, October). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review*, 522-531.

Garay, J. A., Kiayias, A., & Leonardos, N. (2015). *The Bitcoin Backbone Protocol: Analysis and Applications.*

Gladney, H. (2009). Long-Term Preservation of Digital Records: Trustworthy Digital Objects. *The American Archivist*, 401-435.

Jacobsen, B., & Pena, F. (2014, Jul/Aug). What Every Lawyer Should Know About Bitcoins. *Utah Bar Journal, Vol. 27*(4), 40.

Lemieux, V. (2015). Trusting Records: Is Blockchain Technology the Answer?

McKinsey & Company. (2015). *McKinsey Working Papers on Corporate & Investment Banking / No 12; Beyond the Hype: Blockchains in Capital Markets.* McKinsey & Company.

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

Rabin, M. O. (1983). Randomized byzantine generals. *Foundations of Computer Science 1983*, 403-409.

Rivest, R. L., Shamir, A., & Adelman, L. (1978, February). A method for obtaining digital signatures and public-key cryptosystems. *ACM 21*(2), pp. 120-126.

Appendix A

A cryptographic hash (using the SHA-256 algorithm) of the text of this document:

acfa1ddcce49724dcf8c422fb52fe6510b30bedb32709cc699b5e0e7b8c91d0d

Even making a minor change in this document (for example, adding the aforementioned hash to the text) produces this result using the same algorithm:

9cff70c1351e000c8676432c5f1fa629b61da9ec01658a5dfd5f239313178eb1

There is no known way to reverse-engineer the original content from the cryptographic hash. Reversing the hash would be akin to asking: What numbers added together equal the number 238,284? Imagine a document consisting of a set of numbers: 05 14 23 46 71 90 Hashing a document is performing a mathematical operation to them. For example, the sum of the above numbers is 249. If given the sum, it is impossible to tell with any degree of accuracy what the original numbers are. Change one of the numbers, and the hash changes. Hashing an electronic document is like this, except the original input is thousands or millions of numbers, and the mathematical operation is hundreds of degrees more complicated than a simple summation (e.g. take the sum, divide by 20, take the square root, add 5, with 200 more steps).

An example of a block in the Bitcoin blockchain:

Block	#125552
BlockHash	00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
# of Transactions	4
Height	125552 (Mainchain)
Block Reward	50 BTC
Timestamp	May 21, 2011 1:26:31 PM
Merkle Root	2b12fcf1b09288fcaff797d71e950e71ae42b91e8bdb2304758dfcffc2b620e3
Previous Block	125551
Difficulty	244112.48777434
Bits	1a44b9f2
Size (bytes)	1496
Version	1
Nonce	2504433986
Next Block	125553

For more technical resources on blockchain technology, please see:

Garay, Juan, Aggelos Kiayias, and Nikos Leonardos. "The bitcoin backbone protocol: Analysis and applications." In *Advances in Cryptology-EUROCRYPT 2015*, pp. 281-310. Springer Berlin Heidelberg, 2015.

Decker, Christian, and Roger Wattenhofer. "Information propagation in the Bitcoin network." In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pp. 1-10. IEEE, 2013.

Bos, Joppe W., J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. "Elliptic curve cryptography in practice." In *Financial Cryptography and Data Security*, pp. 157-175. Springer Berlin Heidelberg, 2014.

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

Appendix B

Possible Statutory Language for Blockchain Recognition

The Committee is providing the following language as an example of what could be considered as an enactment for providing recognition of the validity of blockchain approaches for the purposes of establishing the authenticity of records. The Committee views this as a possible starting point for the normal processes of legislative drafting.

§11. BLOCKCHAIN ENABLING

(a) In this section, "blockchain technology" means a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via Internet interaction, peer-to-peer network, or otherwise.

(b) Presumptions and admissibility:

(1) Extrinsic evidence of authenticity as a condition precedent to admissibility in a Vermont court is not required for a record maintained by a valid application of blockchain technology.

(2) The following presumptions shall apply:

(A) a fact or record verified through a valid application of blockchain technology is authentic;

(B) the date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain; and

(C) the person established through such as blockchain as the person who made such recordation is the person who made the recordation.

A presumption does not extend to the truthfulness, validity or legal status of the contents of the fact or record. A person against whom the fact operates has the burden of producing evidence sufficient to support a finding that the presumed fact, record , time or identity is not authentic as set forth on the date added to the blockchain, but the presumption does not shift to a person the burden of persuading the trier of fact that the underlying fact or record is itself accurate in what it purports to represent.

(c) Without limitation, the presumption established in this section shall apply to a fact or record maintained by blockchain technology to determine:

(1) contractual parties, provisions, execution, effective dates, and status;

(2) the ownership, assignment, negotiation, and transfer of money, property, contracts, instruments, and other legal rights and duties;

(3) identity, participation, and status in the formation, management, record keeping, and governance of a business corporation, nonprofit corporation, partnership, limited partnership, limited liability company, general cooperative association, limited cooperative association, unincorporated nonprofit association, statutory trust, business trust, common-law business trust, estate, trust, association, joint venture, public corporation, government or governmental subdivision, agency, or instrumentality, or any other legal or commercial entity;

(4) identity, participation, and status for interactions in private transactions and with a government or governmental subdivision, agency, or instrumentality;

(5) the authenticity or integrity of a record, whether publicly or privately relevant; and

(6) the authenticity or integrity of records of communication.

(d) The provisions of this section shall not create or negate:

(1) an obligation or duty for any private party, government, or governmental subdivision, agency, or instrumentality to adopt or otherwise implement blockchain technology for any purpose authorized in this section; or

(2) the legality or authorization for any particular underlying activity whose practices or data are verified through the application of blockchain technology.

Appendix C

Opinion of and provided by Professor Oliver Goodenough, Vermont Law School.

There is widespread conviction that blockchain technology is likely to be a significant contributor to global economic activity in the near and extended future. There is also a perception, repeated by several of the reports on the blockchain, that a clearer institutional structure, including legal recognition, would help to liberate that activity. As the process of this Committee has gone forward, we have been contacted by a number of companies with interest in what Vermont is considering. What is more speculative is whether or not a move by Vermont to fill this legal void can result in the migration of blockchain-based economic activity to Vermont. This discussion will first review the economic potential of blockchain technology as a general matter, citing news reports, policy analysis treatments, and reports of investment activity in the field, and will then turn to the possibilities for economic development in Vermont.

General Economic Potential of the Application of Blockchain Technology

News Reports

In the last few months, there have been numerous in-depth evaluations of the blockchain in high-profile and respected news reports. Perhaps most prominent was the cover story in the October 31, 2015, issue of the Economist magazine. In both a lead and a feature article, the Economist enumerated the potential for the technology to transform any activity where valid, widely available, record-keeping is an essential element, and went on to note that this includes many, many aspects of our economy.

The Wall Street Journal has had a series of articles describing how companies from major banks to imaginative start-ups are making serious commitments to blockchain-based operations. In a July 15, 2015, blogpost, entitled "Blockchain in the Corporate Environment Has Big Potential, But Faces Implementation Challenges," the Journal describes initiatives such as an experiment by the NASDAQ to

use a blockchain approach in creating a limited marketplace for trading private securities. The implementation challenges noted in the article include some technological aspects, but a principal focus is the lack of a legal framework for blockchain based transactions:

> While it seems technically very likely that Smart Contracts can be programmed to execute the lifecycle events of a financial asset, and that those assets can be legally enshrined in computer code as a smart asset, how are they governed by law?

As noted above, the Vermont statutory initiative being considered here could provide a potential solution to a portion of that challenge. The Journal goes on to conclude "assuming these challenges can be overcome, blockchains present an enormous opportunity for the world's banks and financial institutions, which have moved quickly to make investments in it." Other Journal articles describe blockchain exploration and implementation by a number of financial institutions and technology companies.

The New York Times has also noted blockchain potential for driving the next wave of innovation in the financial field. The summation of the expectations about Blockchain set out in an August 28, 2015, article "Bitcoin Technology Piques Interest on Wall St." is worth quoting in moderate length:

> "Most people still think of Bitcoin as the virtual currency used by drug dealers and shadowy hackers looking to evade the authorities.
>
> But the innovations that helped turn Bitcoin into the most popular virtual currency are now being viewed as a potentially enormous disruptive force for several industries, including accounting, music and law.
>
> Nowhere, though, are more money and resources being spent on the technology than on Wall Street — the very industry that Bitcoin was created to circumvent.
>
> "There is so much pull and interest on this right now," said Derek White, the chief digital officer at Barclays, the British global bank, which has a team of employees working on about 20 experiments that explore how the technology underlying Bitcoin might change finance. "That comes from a recognition that, 'Wow, we can use this to change the fundamental model of how we operate to create our future.'"[31]

[31] http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0

In addition to these "mainstream" discussions, it is worth noting that there are several subject specific online news sites dedicated to the blockchain and its sub-topics of bitcoin and other online-currencies. A partial list includes:

- Blockchain - https://blog.blockchain.com/
- CoinDesk - http://www.coindesk.com/
- The CoinTelegraph - http://cointelegraph.com/
- Cryptocoins News - https://www.cryptocoinsnews.com

Policy and Economic Analysis

In addition to this recognition in the press, serious policy analysis has recognized the potential of blockchain. For instance, the Bank of England issued a report on blockchain approaches in its Quarterly Bulletin for the third quarter of 2014. The report joins the conclusion that the distributed ledger techniques of the blockchain are "a key technological innovation." The full report is available at http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

In the Untied States, McKinsey & Company, the widely recognized business consulting company, very recently published a working paper analysis of blockchain. The December, 2015 report was entitled "Beyond the Hype: Blockchains in Capital Markets." It joins with other analysis to predict that blockchain technology will have widespread, disruptive potential, although it sees the development of widespread implementation as a process that will stretch over several years. The report calls in several places for industry to work with regulators to create a strong legal framework for blockchain use. Again, a recognition statute like that under consideration could be an important element in providing such a framework. A copy of this working paper is available at http://www.the-blockchain.com/docs/McKinsey%20Blockchains%20in%20Capital%20Markets_2015.pdf

Serious practice resources such as Bloomberg BNA's Electronic Commerce & Law Report explore non-financial applications. Its article "Blockchain Technology Underpinning Bitcoin Used to

Authenticate Documents, Digital Art" notes that "the blockchain offers promising solutions for document authentication in legal disputes and for preventing digital art forgeries." The piece points out the need for a legal standard of admissibility, and the limitations of the current Federal rules to provide this. We note that the proposed Vermont legislation would help to provide just such a standard. The article is available at http://lawprofessors.typepad.com/files/blockchain-article.pdf.

Academic analyses are growing in number. A partial listing can be found at the Digital Currency Council's library page at http://www.digitalcurrencycouncil.com/library/

Investment activity

The commitment of money to a sector is a good read of its value and helps indicate the scale of activities that Vermont may be able to take a piece of. As is noted above, many large financial institutions are making bets of internal investment on blockchain approaches. In an "Emerging Theme Radar" note sent to its clients in early December 2015, Goldman Sachs underscored this spreading enthusiasm:

> "While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the Blockchain, can change... well everything.[32]
> The world of start-up and venture level investment has also been hot." .

The website CoinDesk reported on July 19, 2015:

> "With more than $800m so far invested in bitcoin and blockchain technology startups since 2012, it's safe to say that venture capitalists are certainly captivated.".[33]

By November, the website CoinTelegraph had upped the number with the headline "$1 Billion Invested So Far in Bitcoin & Blockchain Infrastructure".[34] Even discounting for customary financial world hyperbole, there is clear evidence that significant investment is being made in blockchain based businesses, and that the rate of investment is growing.

[32] http://www.businessinsider.com/goldman-sachs-the-blockchain-can-change-well-everything-2015-12?r=UK&IR=T
[33] http://www.coindesk.com/10-vc-firms-bullish-on-bitcoins-potential/.
[34] http://cointelegraph.com/news/115595/1-billion-invested-so-far-in-bitcoin-blockchain-infrastructure.

Potential Economic Benefits for Vermont

All of this global attention is interesting, but the key questions for this report are how Vermont could benefit economically from the blockchain, and how would the proposed legislation assist in that? The two possible tracks include: (i) the potential benefits from a direct adoption of blockchain technology for Vermont governmental functions and (ii) the potential benefits from a legal recognition of blockchain for private uses, such as the evidentiary recognition that forms the basis of the language considered here. As is explored in detail in a prior discussion in this report, there may be eventual benefits of the direct use of blockchain in governmental functions, but such uses are not currently of sufficient benefit to Vermont for any adoption to be mandated or recommended. By contrast, the potential for benefit from enabling private sector blockchain activity based on Vermont statutory recognition could be direct and immediate, although also speculative hard to quantify. The Committee believes that, the costs and risks of such an enabling approach should be limited. Weighing the speculative potential for growth against these limited concerns is a classic exercise of legislative determination.

Governmental Adoption of Blockchain technology

Much of the literature on blockchain application points to functions that are at least partly governmental, such as property, company and voter registries. The literature is particularly focused on the ability of blockchain to provide assurance of record authenticity, or, as the Economist put it, being a Trust Machine. This function is critical in areas of the world with high levels of systemic corruption; luckily Vermont is not such a location. As stated previously, this early and critical benefit from adopting a blockchain approach has relatively little immediate need in Vermont government and would be disruptive and problematic on many levels while the technology is at its current stage.

That said, as the technology develops, we can anticipate that it will have utility in our governmental functions, and as such, units such as the Secretary of State's office should keep tabs on its growth and its potential for ultimate deployment. We also note that there is already discussion around the

possible establishment of a blockchain network specifically devoted to governmental function, and Vermont could possibly be a participant.

Legal recognition for private uses, including evidentiary recognition, electronic transaction law extension

There is a significant, if hard to quantify, potential for economic development in Vermont from creating a legal infrastructure of recognition and regularization of blockchain activity. As noted in several of the articles discussed above, the lack of such explicit legal recognition is cited as an inhibiting factor on growth in this sector. The prominent development economist Paul Romer describes the relationship of rules and technology in growth:

> "Economic growth is driven by the coevolution of two sets of ideas, technologies and rules. Governments can increase the rate of growth—in ways that benefit all citizens—by creating systems of rules that are both encouraging of and responsive to new technologies.".

There are examples of how providing low cost legal pathways can work to a state's advantage. In Vermont, the often cited (but hard to replicate) example is captive insurance. New Hampshire has had similar success in laws that provided a better framework for trust company activity.[35] In perhaps the most prominent example from a century ago, Delaware's enabling corporation laws led to an activity with huge impact for its economy and state finances. Of course, there are many examples where such moves have not attracted commerce to a state. In the blockchain context, it is encouraging that the activity is predicted to be large, that its proponents are calling for legal recognition as part of creating a certain regulatory environment, and that, so far, no other state has seized the opportunity to create this recognition.

Vermont, therefore, has the potential to seize a first-mover advantage on those aspects of blockchain rules that can be fostered by state-level legal recognition. This potential can be envisioned in

[35] See, e.g., Joseph F. McDonald, III, Migrating Trusts to New Hampshire: The Why and the How, available at https://www.nhbar.org/uploads/pdf/bj-winter2010-vol51-no2-pg34.pdf

two principal ways: the direct benefits of making Vermont the elective legal location for blockchain commerce and the less direct benefits of creating an "attractor" for locating blockchain-based product and service development in Vermont and for tech-related business more generally.

Vermont as the elective legal situs for Blockchain commerce

So far, we are not aware that any governmental authority has given specific recognition to blockchain and its related consensus ledger techniques as a valid way for establishing the factual existence of the record, and the related data of its time of creation and the entities which created it. A change in Vermont law to give such recognition could, therefore, provide an incentive to make Vermont the legal situs of choice for blockchain-based activity. By "situs of choice" we mean that parties in a private arrangement that involves blockchain validation would elect to have at least that portion of their activity governed by, and adjudicated under, Vermont law. Such a directed election of law is often given effect in private transactions under customary Choice of Law rules, even when the transactions have only limited contact with the jurisdiction being elected.

The most immediate result of such elections would be an increase in work for the legal community in Vermont. The validity of a transaction under such an election would ultimately be a question that would need to be answered by a Vermont qualified attorney, who would be involved both at the stage of formation of the arrangement and in the context of disputes that rely on a Vermont court for adjudication. Contributing to the income of Vermont lawyers is good, clean work, particularly when the payments are coming from outside the state. The likelihood of such choice of law adoption would be increased by the development and promulgation of model choice of law and choice of litigation venue language. Such model language, best suggested by our State bar or by attorneys wishing to specialize in this field, would be available for adoption by blockchain services and transaction parties anticipating blockchain recordation of their contracts and other records. Publicizing this into the broader legal, technical, and financial communities working on blockchain applications would be a further helpful step.

And because the surety of the application of Vermont law grows with the depth of contact of the activity with Vermont, we also foresee the possibility that Vermont's financial sector would be able to bring portions of the clearing or other blockchain-based functions to Vermont, particularly if the virtuous circle of growing expertise creating growing activity and vice versa were to take hold. Ultimately, the legal choice alone could make Vermont an attractive location for many aspects of a blockchain business.

The election could lead to ancillary applications of Vermont law to other legal aspects of the arrangement. In addition to e-corporations, it could extend to various aspects of blockchain centered contracting. As blockchain activity expands, Vermont would have the potential to develop other aspects of its law that would make more and more of it an attractive election for other aspects of the contents of the transactions being recorded. For instance, Vermont's UETA law could become even more block-chain friendly and could be elected for financial transactions. Such a circle of reinforcement could include complementing and re-invigorating our existing e-corporation work.

Tax revenues could grow. While electing our state's law to govern all or a portion of a transaction does not in itself necessarily create a taxable nexus for Vermont, to the degree that the link to the underlying activity grows strong enough, such a nexus can develop. Those aspect of the business actually located in Vermont, including legal or technological services, would directly increase our tax base. The importance of Global Foundry (formerly IBM) shows what this looks like at the extreme end of the success of having technology business located in Vermont (although that original location decision was based on factors other than legal attractiveness).

Creating an attractor for locating Blockchain based product and service development in Vermont

Vermont already has significant recognition as a growing, if small, tech business center. For instance, in February 2015, Forbes magazine listed Burlington as one of the top 10 most innovative tech centers in the United States. See http://www.forbes.com/forbes/welcome/ While it did place ninth, it came in ahead of Boston as the highest ranked city east of the Mississippi River. Steps like blockchain recognition could only help support this, providing both direct jobs in blockchain related activities and

positive fallout from the buzz and perceived "coolness" of such legal responsiveness to technological advances.

We could also anticipate our colleges and universities, some of which are already leaders in such tech sectors as gaming and cybersecurity, adding courses and research projects on blockchain, which would in turn lead to an educated workforce, more startups, etc., etc.

All of this is particularly hard to predict with certainty; we do know, however, that Vermont, and in particular Burlington, has a start along this spiral of tech-related economic development, and that in other jurisdictions steps to create legal institutions friendly to that spiral have had positive effects. For instance, California's restrictions on non-competition clauses is often cited as a factor in the growth of the computer industry in Silicon Valley.[36] Given the low costs and risks we foresee for blockchain recognition in the private context, it appears that such legislation could be reasonably adopted as part of an overall policy of fostering business-driven economic growth.

[36] E.g., Natalie Kitroeff, Silicon Valley Is the World's Innovation Capital Because of a Technicality, *Bloomberg.com*, March 17, 2015, available at http://www.bloomberg.com/news/articles/2015-03-17/silicon-valley-is-the-world-s-innovation-capital-because-of-a-technicality