JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

BLOCK CHAIN TECHNOLOGY : OPPORTUNITIES AND RISKS

P.Kumari Deepika, Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan College of Engineering and Technology

A. Kandasamy, Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi Srinivasan College of Engineering and Technology

ABSTRACT;

Block chain 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 Bit coin. 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 recordsmanagement infrastructure Block chain technology is a sophisticated, interesting, and emerging technology. It provides a reliable way of confirming the party submitting a record to the block chain, 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. Regarding economic advantages to legal recognition of block chain technology, Vermont is currently a hospitable environment for commerce related to block chain technology even though the State has not recognized this technology in statute at this time.

1.INTRODUCTION;

A block chain 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 block chain is a complete listing of all transactions, whether financial or otherwise.However, unlike a checkbook, the block chain is distributed among thousands of computers or “nodes” with a process for validating transactions that utilizes a groupconsensus protocol. Making an addition to a block chain ledger requires the approval of the network at large making retrospective changes essentially impossible.

Block chain 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 without the need for a trusted third party.”Because many industries rely upon guarantors, authenticators, and “trusted third parties” (in fact, they are often

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

industries themselves), block chain technology is likely to be extremely disruptive. This paper provides a high-level summary of how block chain technology works. It also discusses current applications of block chain 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 block chain technology as well as risks associated with both the technology and its uses.

2. MATERIALS AND METHODOLOGY;

Numerous scholars, entrepreneurs, and jurists have covered at length and with greater technological proficiency the details of block chain technology.Instead, the report explains the underlying building blocks that comprise block chain's technological foundation. Though each implementation may vary, a few key elements are characteristic of block chain:

- creation and maintenance of an electronic register of transactions,
- encryption of hashes (digests) of transactions,
- validation or verification of those transactions
- timestamping those transactions.

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

2.1 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 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.

2.2 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).

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

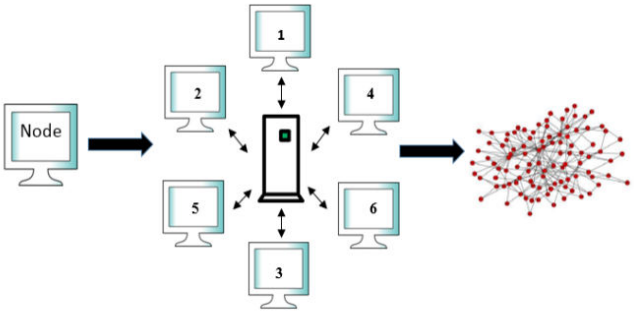

Figure 2.1 Nodes independently verify transactions before agreeing on those that are valid

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

2.3 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

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

over potentially insecure channels and has been in use in the public and private sector for decades.

2.4 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 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

3. RESULTS AND DISCUSSIONS;

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 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*.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

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"). 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.However, UETA's recognition of electronic transactions is limited in some respects, including by the application of other statutory requirements.UETA is intended to be a broadly construed authorization with respect to electronic transactions, but creates no obligations for their use. Under UETA, in litigation, electronic transactions and records are treated in the same manner as manual or paper records.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

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.

4. CONCLUSION AND FUTURE WORK;

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. 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 not verify or address the reliability or the accuracy of the contents, and

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

additionally blockchain technology provides no storage for records, but instead the hashes thereof.

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 fromwww.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

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

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.