ALTERNATE USES FOR BITCOIN-TECHNOLOGY IN LAW

by Ronald L. Chichester[i]

1. Introduction

Bitcoin is an open-source[ii] network for an alternative currency. The network is used as a payment system for digital assets. Someone under the alias "Satoshi Nakamoto" developed a cryptographic mailing list software application and released the source code for that application under an open-source license in 2009. According to Nakamoto, Bitcoin is a "purely peer-to-peer version of electronic cash" that "would allow online payments to be sent directly from one party to another without going through a financial institution."[iii] Digital cash is not new. However, in the past, there was always the need to engage a trusted third party which had to maintain a ledger of the transaction. In contrast, under Bitcoin, each transaction is verified by multiple nodes on the network which recorded the transaction on a public distributed ledger called a blockchain.[iv] The blockchain technology employed by Bitcoin eliminates the need for a third party to be involved in (or record) the transaction. In essence, the third-party verification process has been automated using the blockchain technology. The phenomenal rise of Bitcoin has been described in many papers,[v] books[vi] and even movies.[vii] However, this paper is not going to try to re-invent that wheel. Rather, this paper is going to identify uses of the blockchain technology for areas other than currency, but with legal ramifications. For example, blockchains would enable the automated recording of contract compliance[viii] in business law, real estate, software licensing, family law,[ix] voting,[x] and parole conditions in criminal law.

2. Blockchains Explained

Blockchains require multiple parties and a shared infrastructure. The first piece of infrastructure is a network. The Internet is a suitable network, although depending upon the application, something as small as a local area network is acceptable. The next piece of infrastructure requires three or more parties to each have a device that is connected to the network. Each of those devices must be running software derived from the aforementioned open source software application.[xi] Once the applications are running and can communicate with each other over the network, then transactions can take place and be recorded. It is the peer-to-peer character of the blockchain that distinguishes it from centralized ledgers used by financial organizations. The following two diagrams illustrate the distinction.

Figure 1 illustrates a traditional arrangement between two parties that, for business purposes, require some type of certification authority. In the scenario of Figure 1, a producer generates a product for a consumer. However, the consumer wishes to verify the authenticity or quality of the product, and this is accomplished through the use of a third party, namely the certifying agent.

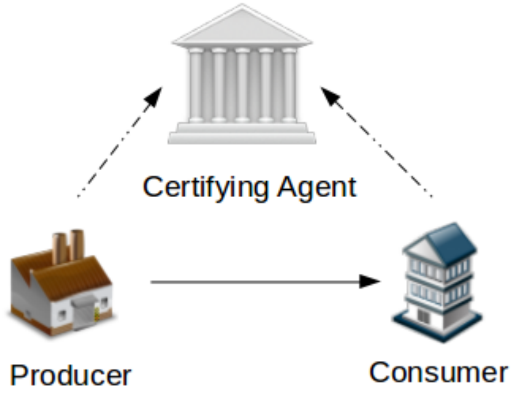

Figure 1: Traditional Middleman Arrangement

Figure 2 illustrates how the blockchain can substitute for the certification authority. In essence, a blockchain can be used to automate or decentralize the certification authority.

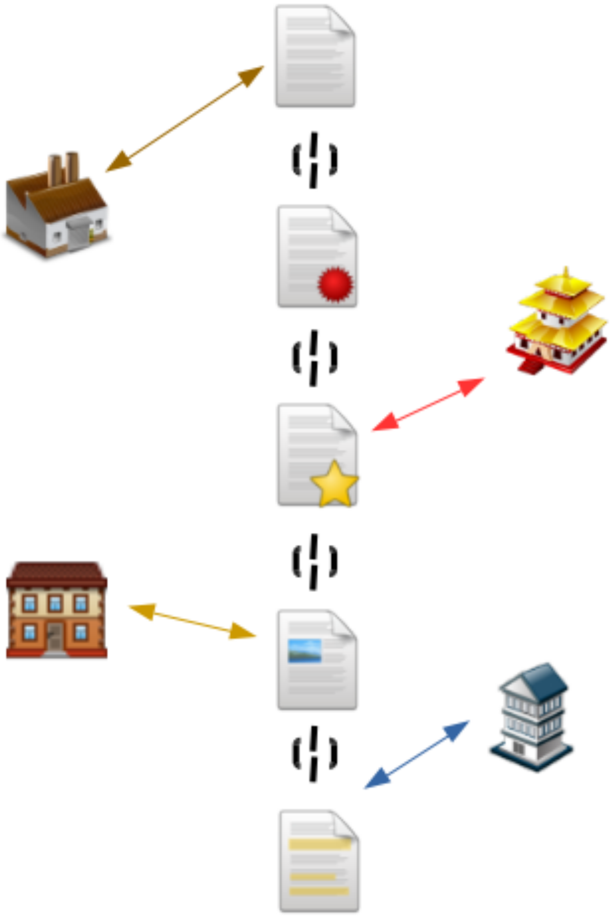

Figure 2: Blockchain

The process for adding something to a blockchain is illustrated in Figure 3 below. Referring to Figure 3, the process starts when a person or organization wishes to add a (signed) contract to a blockchain (step 1). The person puts a copy of the contract into the blockchain software, which in turn generates a "block" (step 2). The block is then placed onto the network (step 3) and its presence is broadcast to all of the devices that are connected to that network (step 4). The devices that are connected to the network then "approve" of the placement as "valid" (step 5). Once validated, the block is then added to the blockchain so that an indelible and transparent record of the block is available on the blockchain (step 6). Interested parties can then retrieve the block and verify its authenticity (step 7). Note, removal of one block from the chain breaks the chain, which accounts for the indelible nature of the blockchain.

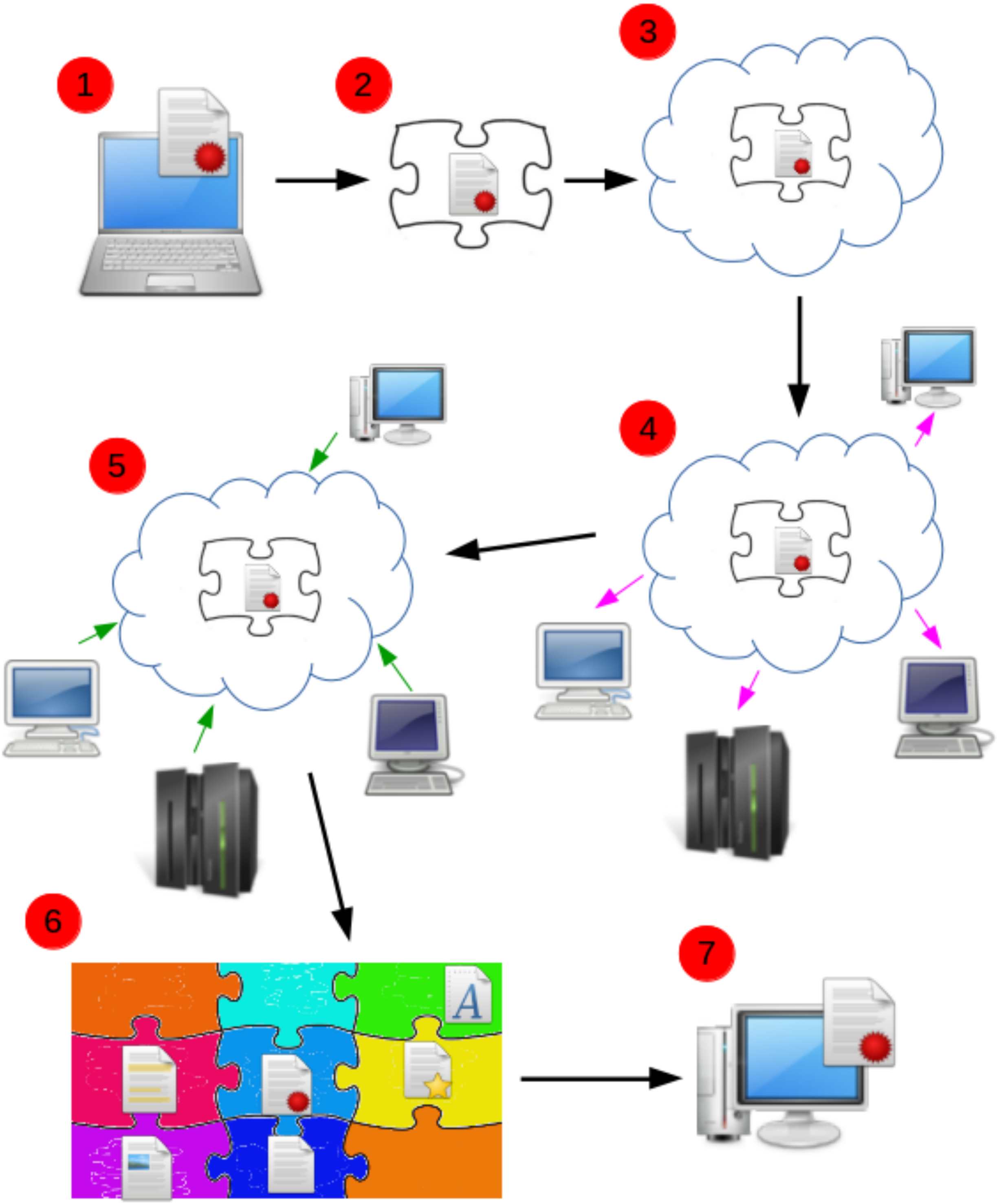

Figure 3: Blockchain Procedure

As illustrated above, the blockchain technology is very well suited for digital currency.

However, this same technology can be employed wherever two individuals (or organizations) wish to have a verified transaction of something of value.

3. Blockchains in Business and Law

Blockchains are an obvious choice for organizations that need to record transactions, but do so in an automated and inexpensive way. For example, consider the scenario where a software license is undertaken, but where the developer is a solo or small operation whose longevity is in question by a much larger customer (who depends upon that software for critical operations). In those cases, the customer often requires that the software developer deposit the current version of the code base to an escrow agent as updates are made available so that the customer can be assured of continued critical operations if the developer dies or otherwise discontinues developed or maintenance of the software. With blockchains, the software developer can avoid the expense and encumbrance of the software escrow agent, by providing an encrypted file of the source code of the application to the customer through the blockchain (in exactly the same manner that bitcoins are transferred). Similarly, if an escrow event is triggered, the cryptographic key for the software can be sent to the customer using the using the blockchain method.

In another example, a marriage was performed at Disney World in Orlando, Florida in 2014, wherein the nuptials were submitted to a blockchain. (The couple was legally married in a civil ceremony.) In this case, the marriage was "performed and registered without the involvement of any government or religious organization."[xii]

There is no reason to think that links within a blockchain could not be admissible in court. While an expert may be needed to opine on the authenticity of the particular blockchain and the specific transaction, there is nothing inherently different about blockchains than other software programs.[xiii] Moreover, the mere presence of the blockchain may obviate the need for litigation in the first place. Finally, there are also techniques (besides encryption) that can be employed to keep the contents of the agreement secret yet still enjoy the benefits of blockchains.

4. Conclusion

The blockchain model provides a public evidentiary mechanism for actions undertaken by parties. In other words, blockchains can be used as a public recordation of actions taken (or not taken) by a party in an agreement. Moreover, because the blockchain method is implemented in software, the transactions can be embedded into existing software systems, thereby leveraging existing automation. Further, records contained within a blockchain can be admissible in court. Thus, blockchains enable a reduction in costs and risks associated with the monitoring or existence of agreements between individuals and organizations. The blockchain method has already proven useful for more than just money.

[i] B.S. Aerospace Engineering, University of Michigan; M.S. Aerospace Engineering, University of Michigan; J.D. University of Houston. The author is a past Chair of the Computer & Technology and Business Law Sections of the State Bar of Texas. He is also a registered

patent attorney, a certified computer forensic examiner, an expert witness, and a certified information systems auditor.

[ii] Software is written in the form of instructions according to the syntax of a programming language. Those instructions are called source code. Source code is then compiled or interpreted into a language usable by a processor to perform the intended instructions (e.g., a software program). Open-source refers to the method of licensing copyrighted source code in a way that ensures its use and accessibility by all. According to the Open Source Initiative, "[t]he "open source" label was created at a strategy session held on February 3rd, 1998 in Palo Alto, California, shortly after the announcement of the release of the Netscape source code. The strategy session grew from a realization that the attention around the Netscape announcement had created an opportunity to educate and advocate for the superiority of an open development process." https://opensource.org/history *See also*, http://www.forbes.com/forbes/1998/0810/6203094a.html

[iii] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", p. 1 (Abstract). The paper is available at: https://bitcoin.org/bitcoin.pdf

[iv] Joshua Kopstein, "The Mission to Decentralize the Internet". The New Yorker (12 December 2013) which is available at: http://www.newyorker.com/tech/elements/the-mission-to-decentralize-the-internet. The article states that Bitcoin uses the "network's 'nodes'—users running the Bitcoin software on their computers—collectively check the integrity of other nodes to ensure that no one spends the same coins twice. All transactions are published on a shared public ledger, called the 'block chain,' and verified by 'miners,' [who are] users whose powerful computers solve difficult math problems in exchange for freshly minted bitcoins." *Id.*

[*v*] *See, e.g.*, https://en.wikipedia.org/wiki/Bitcoin, https://bitcoin.org/bitcoin.pdf,

[vi] See, e.g., "Mastering Bitcoin" which is available (for free) at https://github.com/bitcoinbook/bitcoinbook.

[*vii*] *See, e.g.*, "Bitcoin: The End of Money As We Know It" (2015). http://www.imdb.com/title/tt4654844/

[*viii*] *See, e.g.*, "Smart Contracts, Platofrms and Intermediaries" available at: https://medium.com/@heckerhut/smart-contracts-platforms-and-intermediaries-c3d30f5182a6#.un29012he

[*ix*] *See, e.g.,* "Couple Make History with World's First Bitcoin Wedding" (PanAmPost, October 7, 2014), available at https://panampost.com/belen-marty/2014/10/07/couple-make-history-with-worlds-first-bitcoin-wedding/ (where the wedding was recorded using a blockchain transaction).

[*x*] *See, e.g.*, "The First Bitcoin Voting Machine Is On Its Way" available at http://motherboard.vice.com/read/the-first-bitcoin-voting-machine-is-on-its-way

[xi] Installation of the software is quite easy. For those running Apple OS X, you simply bring up a Terminal (under the Utilities menu) and type:

```
sudo easy_install pip
sudo pip install blockchain
```

For Linux users, check your packages manager and see which blockchain client applications (such as Electrum) are available. If all else fails, you can use (on Debian):

```
sudo apt-get install python-pip
sudo pip install blockchain
```

For Windows machines, the Ethereum blockchain is now provided as a service on Microsoft Azure. In fact, you can get Ehtereum Blockchain as a Service (EBaaS) at the enterprise level. *See, e.g.,* https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/

[*xii*] *Supra*, note 9.

[*xiii*] *See, e.g.,* cases involving Rule 803(6) of the Federal Rules of Evidence and the Texas Rules of Evidence, both of which concern the heresay exception for records of "regularly conducted activity." Texas Rule of Evidence 803(6), which includes "[a] memorandum, report, record, or data compilation, in any form..." Importantly, Rule 803(7) allows the *absence* of an entry kept in accordance with the provisions of 803(6), which can be quite important in the blockchain method because a simple review of the blockchains would easily show entries that are *not* in the defendant's blockchain record but are present in both the plaintiff's and third party blockchain records.