Chicago-Kent Journal of Intellectual Property

Volume 16 | Issue 2 Article 9

6-21-2017

Blockchain Receipts: Patentability and Admissibility in Court

Angela Guo

BLOCKCHAIN RECEIPTS: PATENTABILITY AND ADMISSIBILITY IN COURT

ANGELA GUO*

I. INTRODUCTION

A. Digital Currency

Over recent years, the popularity of digital currency has grown tremendously in a number of different industries. This rise in popularity has been accompanied by heightened scrutiny of the ins and outs of these innovations; specifically, investors, law enforcement officials, and entrepreneurs alike have dedicated time and resources to understanding what lies at the heart of digital currency and what makes this technology transformative. Although the general public still considers the most colloquially popular of these virtual currencies—Bitcoin—to be a legally

* JD/MPP candidate, Class of 2018, Stanford Law School and the Harvard Kennedy School of Government. I would like to thank Assistant US Attorney Kathryn Haun for her guidance and for teaching a fascinating Digital Currency and Cybercrime class at Stanford Law School that piqued my interest in the topic. I would also like to extend my gratitude to members of the Chicago-Kent Journal of IP for providing helpful feedback throughout the editing process.

dubious entity "used by drug dealers and shadowy hackers looking to evade the authorities,"[1] investor interest in Bitcoin has focused on how Bitcoin technology has the potential to fundamentally change the way money is transferred.[2] Furthermore, the technology that enables virtual currencies to function the way they do has promising implications for other applications.[3]

Bitcoin is more than just a simple digital token with a relevant monetary value—it actually consists of the full network that accepts, stores, and organizes these tokens and transfers them from one consumer to another. A credit card charge and money in a bank account exist to most people only as entries tracked in a bank's electronic database; each unit of Bitcoin functions in much the same way—as "nothing more than an entry on a digital ledger."[4] Similar to currency speculation and the stock market, Bitcoin valuation is dependent on the open market and relies on various exchanges (i.e. Coinbase)[5] where people can create "wallets" and buy and sell their units.[6]

Significant differences exist between these virtual currencies and normal currencies, thus preventing conceptual redundancies. Although normal currencies are also electronic in large part, they are typically tracked and accounted for by banks that serve as "middlemen" between two parties in a transaction. Virtual currencies, on the other hand, such as Bitcoin are "kept on a ledger that is maintained and updated by any user of Bitcoin who wants to help."[7] This communal accountability functions in lieu of a central authority. As a result, no sole organization can disable accounts or request personal identifying information from virtual currency users— "anyone can open an account and spend whatever Bitcoins they have as long as they have the password—or secret key—for their account."[8]

During the early stages of Bitcoin's existence in 2009, the general public was initially incentivized to use the currency by the prospect of receiving free Bitcoin.[9] At the time, a bundle of fifty free Bitcoin was released every ten minutes to one of the computers that had subscribed to

1. Nathaniel Popper, *Bitcoin Technology Piques Interest on Wall St.*, NEW YORK TIMES (Aug. 28, 2015), http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0.

2. *Id*.

3. *Id*.

4. Nathaniel Popper, *Bitcoin Basics*, NEW YORK TIMES (Nov. 4, 2015), http://www.nytimes.com/2015/11/05/business/bitcoin-basics.html.

5. Popper, *supra* note 4.

6. BITCOIN, https://bitcoin.org/en/choose-your-wallet (last visited Apr. 14, 2017) (listing other examples of Bitcoin wallets).

7. *Id*.

8. *Id*.

9. *Id*.

help update, maintain, and verify the ledger.[10] These Bitcoin units, upon distribution, could be divided and transferred into any amount up to eight decimal points to any user who had a wallet on an exchange company. To access their wallets for withdrawals and transfers, Bitcoin users were given private keys that only the wallet-owner was privy to. Public wallet keys could also be given out to other Bitcoin users to allow them to deposit coins during transactions. However, public key access was limited *only* to deposits while users with private keys held exclusive access to the wallet.[11] The finite number of Bitcoin – set to be capped at 21 million and fully distributed by year 2140 – served as both a mechanism to curb inflation and as an added incentive to participate in the "giveaway."[12] Computers that became a part of this verifying network in an effort to "mine" free coins would also serve as additional support systems for the currency. As the network of computers grew, so did the reliability and integrity of the overall system.

B. The Blockchain

The communal ledger system that powered these virtual currencies was known as the "blockchain." Conceptually, the blockchain was similar to other publicly updated databases such as Wikipedia or "Google Docs," which rely deeply on general users to submit on content, provide verification, and update the information. To ensure that all transactions are recorded accurately and reliably, the Bitcoin network gives every computer or user a publicly shared "copy" of the ledger and updates these copies in real time through a synchronizing algorithm.[13] This record of transactions is most analogous to "just a big, publicly available spreadsheet," one that is distributed to every user and computer in the community.[14] Since every computer within the network has a copy of these transactions, inconsistences are easily resolved through the "consensus algorithm."[15] If, for example, a hacker were to tamper with the spreadsheets to reflect false transfers of Bitcoin into his personal wallet, the network would immediately correct the inconsistency as significantly more copies of the transaction sheet would not reflect that this amount had been transferred. Corrections are made in favor

10. *Id.*

11. *See Frequently Asked Questions*, BITCOIN PROJECT, http://bitcoin.org/en/faq#is-bitcoin-really-used-by-people. (Last Accessed June 6, 2017).

12. Popper, *supra* note 4.

13. Popper, *supra* note 1.

14. *Id.*

15. James Ching, *The Federalization of Bitcoins*, LAW JOURNAL NEWSLETTERS (June 2013). http://www.lawjournalnewsletters.com/issues/ljn_ecommerce/30_2/news/The-Federalization-of-Bitcoins-158235-1.html.

of the most agreed-upon version amongst all of the existing copies on the network. Given the decentralized nature of the spreadsheet, the lack of central database, and the absence of a master key, the only way to truly alter the master sheet requires controlling a dispositive majority of the entire Bitcoin network – an increasingly difficult feat at Bitcoin grows in popularity and more users join the network. Consequently, it is now virtually impossible to "hack" into Bitcoin databases and transfer assets maliciously.

This blockchain innovation has been the fundamental differentiating feature of virtual currencies. By crowdsourcing and instantly updating all records on the blockchain, digital currencies have eliminated the necessity for the middlemen (e.g. banks, PayPal, Venmo) that previously served as the controlling authority for financial transactions. Additionally, blockchain technology brings the Holy Grail of anonymity just a bit closer: users utilize the public key-private key system from anywhere in the world to send and receive Bitcoin; their actions are recorded on the network without utilizing any personal or identifying information. The resulting "untraceable," anonymous, instantaneous, and free currency system has become an appealing method for cross-national monetary transactions.

However, these same advantages that have contributed to Bitcoin's popularity surge have also turned digital currency into "an obvious choice" for criminal activity. The advent of online marketplaces for illicit goods and services[16] has largely depended on the rise of Bitcoin, often used as the primary method of financial transaction on these darknet and surface web pages. Thus far, law enforcement officials have had only limited success in tracking Bitcoin users by locating I.P. addresses or peering into the entire blockchain ledger, techniques that have proven to be "slow and relatively unsuccessful."[17]

Although digital currencies have been magnetic to those partaking in criminal activities, the blockchain innovation – and digital currencies themselves – are by no means illicit. Instead, the technology has made it possible to send and receive money instantly, reliably, and at no cost to and from anywhere in the world. Other industries, especially the financial sector, have grown increasingly interested in the blockchain ledger system as a way to make trading much cheaper and faster. The irony has not been lost on both the Bitcoin community and big banks, entities in direct contention with each other; although banks are hampered and threatened by the rise in popularity of digital currencies, they are still drawn to the highly efficient distributed ledger concept at the heart of these systems.

16. *E.g.*, Silk Road, Silk Road 2, etc.
17. Popper, *supra* note 4.

Given the claimed and perceived reliability of the distributed ledger, the blockchain model begs another purpose – one that would surely become central to its overall usefulness: admissibility as evidence in court. Since patentability of the blockchain concept and the "consensus algorithm" is in question (one that will be discussed in a later section), some have argued that the "key to a commercial receipting system's profitability does not lie in proprietary software systems but rather on the admissibility of the receipt in future litigation."[18] It is indisputable that the blockchain functions primarily as a verification system; in order to truly become a viable verification system, the veracity of blockchain receipts must be recognized by courts and law enforcement in relevant situations. Admissibility of blockchain data in court would enable transactions to be legally upheld and enforced, thereby giving them "real life" validity. However, the admissibility of these distributed ledger receipts has not been entirely settled. Answers to both this admissibility question and the technology's patentability are critical to the future of both the technology and digital currency at large. California Department of Justice Attorney James Ching opines that if blockchain receipts cannot function as evidence of a transaction for litigation purposes, "[they] are virtually useless."[19] ,

II. EVIDENTIARY ADMISSIBILITY – HEARSAY

Perhaps the most important question facing the admissibility of blockchain evidence is whether it qualifies as admissible hearsay under an existing exception in the Federal Rules of Evidence. Rules barring hearsay evidence stem from concerns about the unreliability of out-of-court evidence when the evidence is put forth to assert the truth of the matter.[20] Evidence introduced in the courtroom by eyewitnesses and experts is typically tested and protected by several courtroom tools, including: (1) the requirement that every witness swears under the oath; (2) the jury's ability to assess credibility through observation of a witness's demeanor; and (3) exposure to cross-examination by the opposing party.[21] A blockchain receipt, if introduced in court, would almost certainly be used as evidence to prove the truth of the transaction documented in the receipt. As a result, blockchain evidence, as an out-of-court "assertion" utilized to prove the truth of the matter, would

18. James Ching, *Is Blockchain Evidence Inadmissible Hearsay?* (Jan. 6, 2016). http://www.law.com/sites/jamesching/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/.

19. *Id.*

20. FED. R. EVID. 801.

21. FED. R. EVID. 802.

probably be subject to both hearsay scrutiny and possibly Confrontation Clause analysis.[22]

A. Computer and Technology Generated Information as Evidence

Courts have already begun to evaluate computer-generated information, albeit in a limited capacity. In *United States v. Lizarraga-Tirado*, the Ninth Circuit analyzed the use of a Google Maps entry of a crime scene in an immigration case. 789 F.3d 1107 (9th Cir. 2015). During the case, federal prosecutors introduced a Google Earth screenshot with a computer-generated GPS "thumbtack" stuck to the alleged scene of the defendant's apprehension within US borders.[23] Counsel for the defendant, an undocumented alien charged with illegal reentry, lodged hearsay objections to both the screenshot and the thumbtack.[24] The defendant had testified that he was still on the Mexico side of the border, insisting that "because he was arrested on a dark night in a remote location," the Border Control agents may have been mistaken during his arrest.[25] Since the defendant's defense was predicated on disputing the government's claim that he was in the United States at the time of his arrest, the Google Earth screenshot and thumbtack were highly probative and material to the outcome of the case.[26] In response, border patrol agents testified that they had recorded the defendant's coordinates from before and during the arrest on a handheld GPS device, proving his illegal entry.[27] Prosecutors presented the coordinators to the jury using Google Earth and Google Maps images with an automatically generated tack that clearly showed the arrest was within US borders.

The Ninth Circuit overruled and dismissed the first hearsay objection to the Google Earth satellite image on the basis that it was analogous to a photograph – Judge Kozinski opined that "because [the image], like a photograph, makes no assertion, it isn't hearsay," but rather a factual depiction of a particular scene at a particular time.[28] However, evaluating the legitimacy of the second inadmissible hearsay objection – the one against the digitally generated "tack" on the coordinates – was far trickier. The tack was treated like a labeled "marker," which asserts that that the "labeled item exists at the location of the marker." Since the agent had not personally

22. U.S. v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015).

23. This "thumbtack" was generated via Google Maps' "search" functions, which pinpoint specific addresses and coordinates when directed to do so by the program's user.

24. *Lizarraga-Tirado*, 789 F.3d at 1110.

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id*. at 1109.

generated the tack, she was unable to be cross-examined about its placement and accuracy.

After additional analysis, Judge Kozinski explained that the court "accurately and readily determined" under Fed. R. Evid. 201(b) that the tack was generated automatically; a quick Google Earth search of the coordinates on any computer would produce an identical image and tack. As a result, the Ninth Circuit concluded that such a tack – automatically placed and labeled by the program – was unimpeachable and not hearsay because "the relevant assertion isn't made by a person; it's made by the Google Earth program."[29] Additionally, the court found *United States v. Lamons* to be dispositive, adopting the court's holding that machine statements generally could not be considered hearsay. 532 F.3d 1251, 1263 (11th Cir. 2008). Inadmissible hearsay could only apply to out-of-court statements made by a person; an electronically-generated "assertion" placed without any human intervention could not fall under that category.

However, the Ninth Circuit does acknowledge that machine-generated evidence, although not necessarily hearsay – is not always reliable or perfect in an evidentiary context. Judge Kozinski points to machine malfunction, inconsistent results, and tampering as authentication concerns under Fed. R. Evid. 901.[30] Authentication broadly demands that the evidence put forth must show and be what the proponent of the evidence claims it is.[31] Separate from hearsay, proper authentication of evidence requires that the party introducing the evidence show that a machine is "reliable and correctly calibrated, and that the data put into the machine is accurate."[32] Although the defendant did not raise an authentication objection at trial, Judge Kozinski indicates that the burden of reliability and accuracy could be met "with testimony from a Google Earth programmer or a witness who frequently works with and relies on the program."[33] An alternative means of meeting the standard could be judicial notice of the fact.

B. Lizarraga-Tirado's Applicability to Blockchain Evidence

The Ninth Circuit's analysis of digitally-generated evidence is highly relevant and potentially influential to how courts may decide to rule on the admissibility of blockchain evidence in the future. Since humans do not actually generate the receipts on the blockchain, it is possible that courts will

29. *Id*. at 1110.
30. FED. R. EVID. 901.
31. FED. R. EVID. 901(a).
32. *Lizarraga-Tirado*, 789 F.3d at 1115.
33. *Id.*

recognize distributed ledger receipts as computer-generated evidence and therefore not hearsay. Although people certainly engage directly in transferring Bitcoin to each other, records of each transaction are generated without human influence, entered automatically through a constantly-updating algorithm on every computer in the blockchain network. A timestamped section of the ledger could be determined to function as a factual depiction of a particular scene at a particular time, much like a Google Earth or Google Maps image.

It is also possible that courts would find substantial distinction between a Google Earth satellite image and a blockchain, opining that the blockchain is closer to a man-made contention and not a picture. Since each transaction recorded in a distributed ledger is the direct result of human transaction – and is cryptographically signed by the "owner" of Bitcoin wallet with his private key – the amount of influence that a person has on such a machine-made assertion is arguably much larger than any possible impact someone could have on a digital photograph. In an attempt to circumvent these potentially thorny arguments, several distributed ledger companies, including Digital Assets, have started making ledgers that do not require permissions.

The "consensus algorithm" may be the key to meeting burdens of proof for both hearsay and authentication objections. As in *Lizarraga-Tirado*, the assertion made by the blockchain in each of the receipts could arguably be the direct result of the consensus algorithm, and not human influence or permission.[34] In much the same way that thumbtack is generated electronically even though a person types in the initial coordinates, blockchain receipts are the product of computers deciding the correct version. A single (or even mass) human attempt to tamper with the blockchain will almost certainly be unsuccessful because the machine-produced algorithm "answers" will override these inconsistences in pursuit of the truth.

If blockchain evidence is found not to be inadmissible hearsay, it will likely still incur scrutiny under authentication objections. However, a proponent of ledger receipts could once again point to the consensus algorithm and prove that a machine is "reliable and correctly calibrated."[35] The existence of a vast network of independent verifiers would likely be extremely compelling in proving authenticity and accuracy. Furthermore, expert testimony can also be brought in to meet the burden of authentication

34. *Id.*
35. *Id*.

under FRE 901; as Kozinski indicated in *Lizarraga-Tirado*, an exchange programmer,[36] an avid Bitcoin user, a programmer attempting to replicate the blockchain, a digital currency expert, or an investor could all be brought in at trial to explain the process, accuracy, and the exceptional reliability of blockchain receipts.

III. BLOCKCHAIN EVIDENCE UNDER THE BUSINESS RECORDS EXCEPTION

Finally, even if blockchain receipts were considered hearsay, the receipts would likely be admissible under the Business Records exception in Fed. R. Evid. 803(6). This business records exception specifically notes that evidence can be admissible as a "business record" if it met several requirements, including that it "was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling" and that "making the record was a regular practice of that activity."[37] In digital currency, blockchain receipts do not exist to function as ammunition in litigation activity. The blockchain receipts and the consensus algorithm are quintessential examples of record-keeping in the ordinary course of business. Although these receipts could certainly prove themselves to be useful in verifying document authorship, this record keeping feature stems from a desire to be accurate and to deter malicious users, a very different objective from use at litigation. Thus, blockchain receipts might even be admissible at face value in spite of hearsay concerns, as a business record can "bypass" the hearsay debate entirely.

IV. CLASSIFYING BITCOIN AS INTELLECTUAL PROPERTY

Though the blockchain's admissibility as a litigation tool in court remains murky, the technology's applications outside of court are anything but. These emergent applications have ranged far and wide; consumers and entrepreneurs alike have expressed confidence in the technology's ability to revolutionize everything from the finance industry to national security. A number of fintech startups have delved into using the blockchain to protect intellectual property, a natural leap given the decentralized record-keeping nature of the technology. But even though IP applications for the blockchain seem inevitable, its patentability might not be quite as simple.

It has become increasingly clear over the last few years that Bitcoin is likely not patentable in and of itself. To many judges and legal scholars, digital currencies are, at their core, currencies, and are no more patentable

36. *E.g.*, from an exchange like Coinbase.
37. FED. R. EVID. 803(6).

than the US dollar. However, modern-day digital currencies do possess many characteristics that differ from both the traditional currencies and early digital currencies from video games and the virtual world. This makes classification difficult. The qualities unique to digital currencies such as decentralization, intangibility, and functionality outside of a niche virtual domain have contributed to immense debate with respect to what kind of property Bitcoins are. Even within intellectual property, digital currencies do not fall neatly within any of the main categories of patents, copyrights, trade secrets, or trademarks.[38]

Some of these categories can be eliminated without much further discussion. According to attorneys Michael A. Berta and Willow W. Noonan at Arnold & Porter LLP, bitcoins do not fall under the purview of patentable inventions – "no matter how inventive the Bitcoin system as a whole may be, each individual bitcoin likely is not a separate patentable invention."[39] Additionally, the fundamental anonymity of the Bitcoin system disallows its classification as a trademark. Trademarks typically protect brand names and mechanisms used by producers to identify and distinguish its goods on the market. Since a bitcoin functions as a unit of currency that specifically cannot be traced to its possessor, it cannot constitute a trademark outside of the use of its name alone.

A bitcoin likely also cannot be protected by a copyright. Though case law in this area to date has been sparse, some have pointed to the "private key" in digital currencies as potentially copyrightable. This private key, which is instrumental in allowing the owner to anonymously access her money and transfer bitcoins from one wallet to another, consists of a lengthy and randomly generated string of letters and numbers. However, simple fixation of random numbers and letters alone does not meet the threshold for copyright protection – some semblance of originality and creativity must also be embedded in the copyrightable matter. In the case of private keys, random generation of the letters and numbers precludes any of the creativity found in traditionally copyrighted works. Additionally, the highly functional nature of the private key requires that "they conform to strict formatting requirements," further weakening the case for copyright protection.[40] In the same way that mathematical formulas cannot be copyrighted in part due to standardized notation, bitcoin keys are rigidly and formulaically calculated for the sole purpose of transferring and receiving bitcoins. And even if

38. Michael A. Berta and Willow W. Noonan, *The Property-Contract Duality of Bitcoin*, FINANCIER WORLDWIDE (June 2015), https://www.financierworldwide.com/the-property-contract-duality-of-bitcoin/#.WNpPRGTysb0.

39. *Id.*

40. *Id.*

bitcoin keys were borderline copyrightable, registering secret keys with the United States Copyright Office laughably undermines the purpose of an "anonymous" currency – if published, the secret keys would lose much of their power and functionality. It would be unwise at best to "compromise the secrecy of a bitcoin [private] key by registering it with the Copyright Office."[41]

As a result, trade secrets remain perhaps the most compelling classification category for bitcoins. Courts have often defined trade secrets as "information that derives economic value from not being generally known or readily ascertainable, and that [they are] the subject of reasonable efforts to maintain its secrecy."[42] At surface level, bitcoin private keys do appear to meet these standards. Private keys by their very nature are not generally known or readily ascertainable and the digital currency certainly derives significant economic value from this conscious secrecy. Bitcoin owners have every incentive to safeguard their private keys since hackers otherwise would pillage their wallets.

Yet classifying bitcoins as trade secrets still does not seem quite right perhaps due to the changing nature of the private keys upon transfer. Although bitcoins "at rest" appear to meet all the qualifications of a trade secret, bitcoin transactions are very different from the typical transfer of a trade secret product. When bitcoins have been transferred, "they are no longer secured by the same private key," moving from being protected by the sender's private key to the recipient's private key.[43] Unlike a Chick-fil-a sandwich, "the secret information representing the bitcoin (i.e., the private key) is completely different" and no longer remains covered by the same trade secret.[44] This complicating factor has made it very difficult for courts to evaluate bitcoins as trade secrets or any other category of intellectual property. Even Satoshi Nakamoto, the pseudonym of the anonymous founder (or founders) of the digital currency, has not yet come forth with an effort to designate Bitcoin itself as any specific form of intellectual property.

41. *Id.*
42. *Id.*
43. *Id.*
44. Michael A. Berta and Willow W. Noonan, *The Property-Contract Duality of Bitcoin*, FINANCIER WORLDWIDE (June 2015), https://www.financierworldwide.com/the-property-contract-duality-of-bitcoin/#.WNpPRGTysb0.

V. THE RUSH TO PATENT THE BLOCKCHAIN

While few entities seem to be rushing to classifying individual bitcoins as intellectual property, many more have jumped at attempts to patent the technology that drives digital currency. Although there is still some discussion as to whether trade secret or copyright protection should apply, patents have emerged as the primary mechanism thus far for those seeking to protect their claims and uses of the technology. According to Reuters, 63 blockchain-related patents were filed globally last year and 27 have been filed up until March of this year.[45] These filings have come from a host of enterprises – from Goldman Sachs to Coinbase – that seek to use the technology to circumvent financial middlemen and intermediaries.

The United States Patent Office has not yet granted any of these patents. Given the recent filings of most of these patent applications, the USPO likely has not yet truly begun to evaluate these applications. However, is still unclear whether such patents will even be deemed valid in the current legal landscape.

Blockchain patentees face several hurdles in their fight to use, protect, and claim the technology. First, Bitcoin creator Satoshi Nakamoto publicly published a paper about his invention in 2008, detailing the functionality, components, and creation of his invention. Since then, Nakamoto has vanished, but his publication meant that "the core of the technology is now part of the public domain and only important additions and variations could be patented."[46] This article – and the ensuing development of the bitcoin network afterwards – counts as *prior art* against any individual's newfound attempt to patent blockchain technology. Although several people have stepped forward claiming to be Mr. Nakamoto, none have conclusively or definitively proven this relationship. As a result, any patent application likely hinges on its "improvement" to the general existing idea of a blockchain system and increased computer or system functionality. However, even an improvement patent must still survive the *Alice* and *Mayo* challenges – to do so, any blockchain patentee must sufficiently include improvements that constitute "significantly more" to a "non-abstract idea" than what already exists of the open-source technology has been revealed to the general public

45. Byron Kaye and Jeremy Wagstaff, *Creator races to patent technology with gambling tycoon*, REUTERS INVESTIGATES (Mar. 2, 2017), http://www.reuters.com/investigates/special-report/bitcoin-wright-patents/.

46. *Who Owns the Blockchain?*, THE ECONOMIST (Jan. 12, 2017), http://www.economist.com/news/business/21714395-financial-firms-and-assorted-startups-are-rushing-patent-technology-underlies.

for some time.[47] But for now, only time will tell if such a revolutionary technology can be claimed as intellectual property – or be used in court.

47. Ira Schaefer and Ted Mlynar, *Is a Blockchain Patent Still Possible?*, COINDESK (Nov. 15, 2016), http://www.coindesk.com/blockchain-patent-still-possible/.