SMU | Dedman School of Law

SMU Law Review

Volume 72 | Issue 4 Article 18

2019

The Blockchain Paradox: Almost Always Reliable, Almost Never Admissible

J. Collin Spring
Southern Methodist University, Dedman School of Law, jspring@smu.edu

THE BLOCKCHAIN PARADOX: ALMOST ALWAYS RELIABLE, ALMOST NEVER ADMISSIBLE

*J. Collin Spring**

TABLE OF CONTENTS

* Candidate for Juris Doctor, SMU Dedman School of Law (May 2020). The author would like to dedicate this comment to LaJeanne Spring, his grandmother, for the unending support she has provided. Special thanks to W. Keith Robinson, Altshuler Distinguisher Teaching Professor and Co-Director of the Tsai Center for Law, Science, and Innovation, SMU Dedman School of Law, for his input on Part II of this comment.

I. INTRODUCTION

BITCOIN—to some people, it is "gold for nerds."[1] "A techno tour de force."[2] To others, it's "rat poison."[3] However any given person might feel about cryptocurrencies, though, the underlying technology—blockchain technology—is a technological breakthrough that is reshaping industry after industry. While cryptocurrencies are the most well-known application of blockchain, this technology is currently being used in a variety of sectors, including supply chain management,[4] government services,[5] healthcare,[6] food safety,[7] identification,[8] and cybersecurity.[9] Naturally, as the use of blockchain continues to grow, litigation involving blockchain grows with it. Blockchain litigation was practically nonexistent before 2017. However, blockchain litigation began to increase sharply when, notably, the price of Bitcoin reached its all-time high of nearly $20,000 before crashing.[10] This trend seems poised to continue. Accordingly, trial lawyers and judges across the country are likely to soon find themselves grappling with the interplay of blockchain reports and evidentiary law for the first time.

A careful study of this interplay between blockchain technology and existing evidence law reveals two themes: (1) in most cases, blockchain

---

1. Daniel Mark Harrison, *'Gold for Nerds': The True Story of Blockchain*, COINSPEAKER (Dec. 21, 2014), https://www.coinspeaker.com/gold-for-nerds-the-true-story-of-bitcoin/ [https://perma.cc/58B7-SN84].

2. *FOX Business* (FOX television broadcast May 6, 2013), https://video.foxbusiness.com/v/2359385547001/?#sp=show-clips [https://perma.cc/D4HQ-MNBN] (statement of Bill Gates).

3. *Id.* (statement of Charlie Munger).

4. Bernard Marr, *How Blockchain Will Transform the Supply Chain and Logistics Industry*, FORBES (Mar. 23, 2018), https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#207423a5fecd [https://perma.cc/77FS-BE2P].

5. Amr Refaat, *How the UAE Is Empowering Its Citizens Through Blockchain*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Oct. 30, 2018), https://www.ibm.com/blogs/blockchain/2018/10/how-the-uae-is-empowering-its-citizens-through-blockchain [https://perma.cc/K2S2-MER7].

6. Quora, *What Are the Use Cases for Blockchain Tech in Healthcare?*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Dec. 17, 2018), https://www.ibm.com/blogs/blockchain/2018/12/what-are-the-use-cases-for-blockchain-tech-in-healthcare [https://perma.cc/G25Q-S4W5].

7. Roger Aitken, *IBM Forges Blockchain Collaboration with Nestlé & Walmart in Global Food Safety*, FORBES (Aug. 22, 2017), https://www.forbes.com/sites/rogeraitken/2017/08/22/ibm-forges-blockchain-collaboration-with-nestle-walmart-for-global-food-safety/#4364efaf3d36 [https://perma.cc/6NHQ-3BLR].

8. Simon Chandler, *Blockchain-Based Digital ID Systems are Increasingly Finding Real-World Use*, COINTELEGRAPH (Feb. 7, 2019), https://cointelegraph.com/news/blockchain-based-digital-id-systems-are-increasingly-finding-real-world-use [https://perma.cc/FA3P-YU94].

9. Rachel Wolfson, *How a Leading Cyber Security Company Uses Blockchain to Prevent Data Tampering*, FORBES (July 3, 2018), https://www.forbes.com/sites/rachelwolfson/2018/07/03/how-a-leading-cyber-security-company-uses-blockchain-technology-to-prevent-data-tampering/#307dc8f14529 [https://perma.cc/LDY9-CYW7].

10. Stan Higgins, *From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited*, COINDESK (Dec. 29, 2017), https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited [https://perma.cc/LAU8-9GYR].

evidence is patently inadmissible; and (2) considering the purposes of the Federal Rules of Evidence (FRE), in most cases, blockchain evidence should be admissible.

Part II of this comment aims to provide a layman's overview of how blockchain works and what its vulnerabilities are. Part III explores the applicable principles of the law of evidence and concludes that, as it currently stands, blockchain reports are only admissible in federal court in limited circumstances through the residual exception to hearsay enshrined in FRE 809. Part IV begins by detailing the relatively sparse existing law addressing blockchain evidence and then responds to the existing scholarship on the matter. Part V proposes an amendment to the FRE that accounts for the vulnerabilities in blockchain without placing undue burden on litigants needing to introduce blockchain evidence.[11]

II. BLOCKCHAIN BASICS (AND NOT-SO-BASICS)

A. Blockchain—What It Is, and How It Works

Blockchain is a "peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power."[12] While there is no phrase in English that means exactly the same thing, the closest translation is roughly "a publicly shared ledger that is difficult to change."

Blockchains are records that are shared across a group of computers, called a "network."[13] Each computer, called a "node," stores a copy of the blockchain record.[14] The network updates this record approximately every ten minutes to see if there is new data that needs to be added to the blockchain.[15] Blockchain networks come in two principle types: public and private.[16] The distinction is essentially who can set up a computer to serve as a node. In a public blockchain, anyone can download a copy of the blockchain ledger and set up a new node on the network.[17] Private

11. Blockchain evidence is a large topic and necessarily cannot be covered in one comment. A myriad of issues will not be treated in depth here but still warrant some discussion. First, litigants should be aware that, in most jurisdictions, expert testimony will be needed to lay a foundation sufficient to admit blockchain evidence. Second, beyond a brief discussion of Vermont's statute, this comment does not endeavor to explore how blockchain fits into state-level evidence law. While these two issues are far from the only topics which cannot be explored here, they are sufficiently important such that trial attorneys should bear them in mind when preparing a case involving blockchain evidence.

12. Satoshi Nakamodo, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin 8, https://bitcoin.org/bitcoin.pdf [https://perma.cc/S2SY-ZF6Y] (last visited Sept. 1, 2019).

13. Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers*, 25 Rich. J.L. & Tech. 2, 29 (2018).

14. *Id*.

15. *Id.* at 43.

16. *Id.* at 77, 79.

17. Praveen Jayachandran, *The Difference Between Public and Private Blockchain*, Blockchain Pulse: IBM Blockchain Blog (May 31, 2017), https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ [https://perma.cc/CYF3-7CK3].

blockchains, however, are permissioned—new nodes can only be established by people who have been invited to join the network.[18] As discussed below, this distinction is not currently addressed in the evidentiary standards used for blockchain records but should be accorded heavy weight when deciding admissibility.[19]

A blockchain transaction begins with users inputting data.[20] Using cryptocurrency as an example, a user will tell the network that she wants to transmit a certain amount of currency to another user.[21] This is a "transaction."[22] The transaction is stored in a "block."[23] A block is like a page in a physical ledger, it stores the information inputted by the users.[24] A single block can contain an immense amount of data—for example, on average, a block on the Bitcoin blockchain stores more than 500 transactions.[25]

New blocks are added to the chain by mining nodes (miners), powerful computers that "group outstanding transactions into blocks and add them to the blockchain . . . [b]y solving a complex mathematical puzzle . . . and including the answer in the block."[26] These puzzles are essentially solved by "guessing at random."[27] The hash encryption "makes it impossible to predict what the output will be."[28] The miner that finally solves the crypto puzzle announces the solution to the network.[29]

After a miner announces the new block to the network, the last step before a block is added is achieving "consensus."[30] While there are a variety of different consensus mechanisms,[31] they all share the same common function. To decide whether a block should be added to the blockchain, the nodes on the network follow a protocol to collectively determine if the proposed block is legitimate.[32] If it is, it is accepted by the network, and the block becomes part of the chain; if it is not, then it does not.[33] When consensus is reached, the miners begin working to solve a new

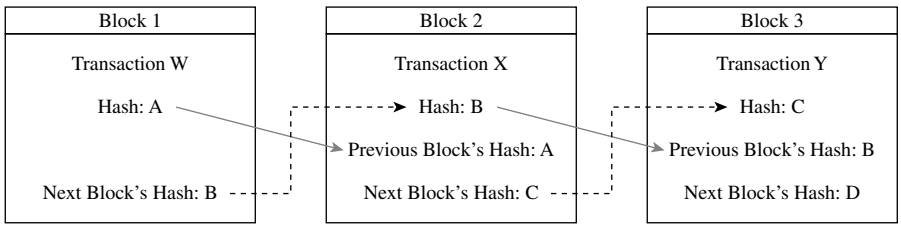
18. *Id.*
19. *See infra* Part V.
20. Nakamodo, *supra* note 12, at 2.
21. *Id.*
22. *See id.*
23. *Id.*
24. *Id.*
25. *See Average Block Size*, BLOCKCHAIN, https://www.blockchain.com/charts/avg-block-size [https://perma.cc/NHT5-XGUR] (last visited Sept. 1, 2019).
26. Noelle Acheson, *How Bitcoin Mining Works*, COINDESK, https://www.coindesk.com/information/how-bitcoin-mining-works [https://perma.cc/3GFS-JB4G] (last updated Jan. 29, 2018).
27. *Id.*
28. *Id.*
29. *Id.*
30. *See* Amy Castor, *A (Short) Guide to Blockchain Consensus Protocols*, COINDESK (Mar. 4, 2017), https://www.coindesk.com/short-guide-blockchain-consensus-protocols [https://perma.cc/L74G-5RC6].
31. *See id.*
32. *What Is a Blockchain Consensus Algorithm?* BINANCE ACAD., https://binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm [https://perma.cc/D4HQ-MNBN] (last visited Sept. 1, 2019).
33. Nakamodo, *supra* note 12, at 3.

crypto puzzle and find a new block.[34] In theory, consensus is what gives the blockchain its reliability; disinterested third parties (nodes) are responsible for adding new information to the ledger.[35] As explored below, however, there is some risk of decentralization which undermines the reliability of the blockchain.[36]

Blocks are chained together by "hashes," encrypted codes which are made from the contents of the block and that identifies the block.[37] Each block contains its own hash, the hash of the previous block on the chain, and the hash of the next block on the chain.[38] These hashes chain together to give blockchain its immutable quality.[39] Because each block's hash is developed from the contents of the block itself, changing any information in the block changes the block's hash.[40] This, in turn, is reflected in the hash of the following blocks.[41]

Figures 1 and 2, below, and the accompanying text illustrate this pivotal element of blockchain technology.

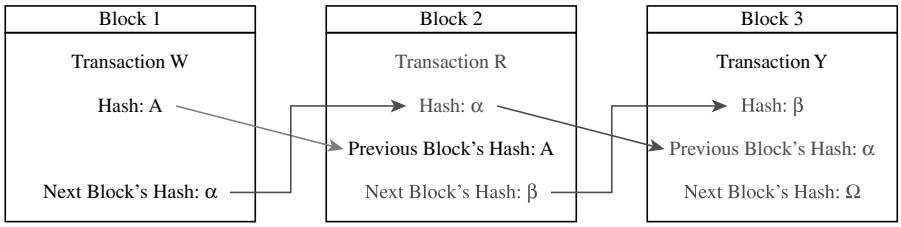
Figure 1



Imagine that Block 1 contains transaction W, which gives it a hash value of A. Block 2, with transaction X and hash A (from the preceding block), receives a hash value of B. Block 3, with transaction Y and preceding hash B returns a hash value of C, and so on. If one were to look at Block 3, it would show hash values of B (preceding block's hash), C (its own hash), and D (succeeding block's hash).

34. *Id.*
35. *See* Mike Orcutt, *How Secure Is Blockchain Really?*, MIT TECH. REV. (Apr. 25, 2018), https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/ [https://perma.cc/7XC2-PGN9].
36. *See infra* Part II.B.
37. Bacon et al., *supra* note 13, at 12–13.
38. *Id.* at 16.
39. *Id.* at 13.
40. *Id.* at 14.
41. *Id.* at 16.

Figure 2



Imagine, then, that changes were made to the transactions stored in Block 2. Because the hash value of Block 2 is based on it containing content X, when changes are made to the contents, that changes the hash value of Block 2. Because the hash value of Block 2 is recorded in Blocks 1 and 3, when it is altered, the change can be seen in every subsequent block in the chain. The network then rejects the change.[42]

Because one of the animating concerns of evidentiary law is reliability,[43] the user-side verification protocols of blockchain require some discussion. Verification protocols ensure that the user inputting the data into the blockchain is who he claims to be.[44] While these vary from blockchain to blockchain, the most common form of verification protocol uses a "public key" and a "private key."[45] While the analogy is not technologically precise,[46] for our purposes, it will suffice to think of a public key as a username and a private key as a password. A user inputs his private key before making a transaction, which (theoretically)[47] validates his identity.

Finally, we turn to "smart contracts." A smart contract is a "self-enforcing agreement" created digitally over a blockchain.[48] While traditional contracts rely on courts for enforcement, smart contracts cut out the middleman and allow the contract to enforce itself.[49] For example, parties could create a smart contract where, after a party transmits a predetermined amount of cryptocurrency, it automatically receives a document. As soon as the cryptocurrency is paid, the network sends the document to the recipient. Notably, a smart contract is *not* a contract in the legal sense—it does not need to meet the same requirements that a court

42. *See* Nakamodo, *supra* note 12, at 8.
43. *See* KENNETH S. BROUN ET AL., MCCORMICK ON EVIDENCE § 245 (7th ed. 2014).
44. *See* Nolan Bauerle, *How Does Blockchain Technology Work?*, COINDESK, https://www.coindesk.com/information/how-does-blockchain-technology-work [https://perma.cc/P4SP-A3W6] (last visited Sept. 1, 2019).
45. *Id.*
46. The technical differences between public keys and usernames and between private keys and passwords have little relevance for the discussion of evidentiary principles. Accordingly, they are omitted for brevity and clarity. For an in-depth discussion of the technological aspects of public and private keys, see Bisade Asolo, *Blockchain Public Key & Private Key: A Detailed Guide*, MYCRYPTOPEDIA (Mar. 28, 2019), https://www.mycryptopedia.com/public-key-private-key-explained/ [https://perma.cc/635P-2JAN].
47. *See infra* Part II.B.
48. Shermin Voshmgir, *Smart Contracts*, BLOCKCHAINHUB BERLIN, https://blockchainhub.net/smart-contracts [https://perma.cc/RD3S-NDX5] (last updated July 2019).
49. *Id.*

would hold a contract to before enforcing it.[50] Accordingly, when discussing smart contracts, it is important to bear in mind that they are smart "contracts."

To establish a smart contract, parties create computer code that captures the agreement between them.[51] These agreements then automatically enforce themselves, and when the first party performs the first end of the contract, the second party's performance automatically occurs.[52]

To summarize the above discussion of relevant principles of blockchain technology, blockchains can be public or private. Copies of the blockchain record are stored on nodes across a network. This record is constantly updating itself. Users input data. Miners solve crypto puzzles to combine these transactions into a block. Blocks are added to the chain through consensus. These blocks are chained together by a series of hashes which ensure that if anything in the record is changed, the network detects the alteration. Some blockchain interactions include smart contracts which allow users to make self-enforcing agreements that cut out the need to use third parties.

Now for the complex part.

B. Blockchain's Vulnerabilities

To develop a useful standard for admissibility of blockchain evidence, it is not enough to merely evaluate blockchain's strengths. To ensure reliability, a standard for admissibility must consider and account for blockchain's weaknesses, as the weaknesses may call the reliability of blockchain evidence into question.

Recall that blockchain's reliability flows from the fact that a network of independent and disinterested third-party nodes decides through consensus whether to add a new block to the chain, and that the chain's immutability comes from that same network of third parties detecting and rejecting alterations. Both of these qualities, then, rely upon a common assumption: that the network is truly disinterested (decentralized, in blockchain parlance).[53] Even in the original definition given by Satoshi Nakamodo for blockchain, the assumption of disinterest is made: blockchain is "peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change *if honest nodes control a majority of CPU power*."[54] When we challenge the assumption that the nodes are honest, both the reliability and the immutability of the blockchain disappear.

The network can become centralized in a variety of ways. The traditional approach, called a "51% attack," was long thought to be infeasible (at least on large, public blockchains like Bitcoin) because of the sheer

50. *See id.*
51. *Id.*
52. *Id.*
53. Nakamodo, *supra* note 12, at 4.
54. *Id.* at 8 (emphasis added).

amount of computing power required.[55] However, new methods are being pioneered that allow for the centralization of the blockchain. For example, Ittay Eyal and Emin Sirer of Cornell University have developed a method called "selfish mining" that would require far less computing power and, therefore, poses a serious threat.[56] We must also bear in mind that blockchain is a developing technology, and new vulnerabilities can (and surely will) be found.

51% attacks are fairly straightforward. They are the product of "the ability of someone controlling a majority of network hash rate to revise transaction history and prevent new transactions from confirming."[57] Essentially, when a party or group of parties controls a majority of the network, they control the consensus mechanism.[58] Accordingly, they can then decide which new blocks will be accepted by the network and can accept changes to existing blocks that honest networks would detect and reject.[59] While this was a largely theoretical concern for much of blockchain's history, 51% attacks have become a real problem for blockchain in recent years.[60] Researchers have projected that 51% attacks are poised to increase in the future.[61]

With a 51% attack providing the ability to deny the addition of legitimate blocks, allow the falsification of new blocks, and alter the contents of existing blocks, serious evidentiary concerns are posed. Discussed in more depth in Part V below, the possibility of such an attack undermines one of the primary goals of evidence law—ensuring that evidence is reliable.[62]

The issue presented to would-be attackers is that 51% attacks can require a truly massive amount of computing power.[63] This threat is most real in the context of small, public blockchains.[64] Because public blockchains are not permissioned, and anyone can join, it becomes simple for assailants to achieve the hashing power necessary to centralize and falsify the blockchain. Private blockchains pose a threat of a different

55. Alyssa Hertig, *Blockchain's Once-Feared 51% Attack Is Now Becoming Regular*, CoinDesk (June 8, 2018), https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular [https://perma.cc/X42X-85UW].

56. *See* Ittay Eyal & Emin Gün Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable* (Nov. 15, 2013) (unpublished manuscript) (on file with Cornell University), https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf [https://perma.cc/V4BU-VMV5].

57. *51% Attack, Majority Hash Rate Attack*, Bitcoin, https://bitcoin.org/en/glossary/51-percent-attack [https://perma.cc/SEC8-36J5] (last visited Sept. 1, 2019).

58. *See 51% Attack*, Learn Cryptography, https://learncryptography.com/cryptocurrency/51-attack [https://perma.cc/X2FG-X489] (last visited Sept. 1, 2019).

59. *Id.*

60. *See* Hertig, *supra* note 55 (Monacoin, Bitcoin Gold, Zencash, Verge, and Litecoin Cash were all subjected to 51% attacks in the month period between May 8 and June 8, 2018).

61. *See* Olga Neroda, *51% and the Future of POW*, Hacker Noon (Oct. 14, 2019), https://hackernoon.com/51-attacks-and-the-future-of-pow-402266905bfa [https://perma.cc/3QJC-DFM2].

62. *See infra* Part V.

63. *See* Hertig, *supra* note 55.

64. *Id.*

type. Here, because entry onto the network as a node is permissioned, the administrator of the blockchain can control who has access to hashing power. When new nodes are carefully screened, this could preclude 51% attacks altogether by ensuring that dishonest actors cannot join the network. However, it also allows the administrator of the blockchain to only grant permission to new nodes that align with his interests. An administrator could, in fact, specifically choose to permission only those nodes that would cooperate with him to falsify the record.

For large, public blockchains, one could be forgiven for thinking that this is a matter of purely academic concern. Consider, for example, the Bitcoin blockchain. As of the time of this writing, the Bitcoin blockchain has a hash rate of 47,117,891 terahashes (equal to one trillion hashes) per second.[65] As such, a would-be assailant would need the raw computing power necessary to perform over 23,448,946 trillion hashes per second to be able to perform such an attack. However, while that may sound remote, consider that a group of bitcoin miners has twice nearly achieved such control.[66] In January of 2014, Ghash.io, a pool of bitcoin miners, obtained 42% of the hashing power on the Bitcoin blockchain.[67] In June of 2014, the same group reached 50%, only a single percentage point away from the level necessary to decentralize the blockchain through traditional means.[68] Even on large, public blockchains such as Bitcoin, the chance of centralization is a real threat and should be considered when discussing the evidentiary standards that should apply to this type of technology.

The obvious drawback for would-be assailants is that a 51% attack requires 51% of the network power. Even though it is possible for a coordinated group to achieve such power, it may not always be feasible. This was thought, for most of blockchain's history, to insulate it from attack.[69] Then along came selfish mining.[70]

Selfish mining is a technique pioneered by Ittay Eyal and Emin Gün Sirer of Cornell University that allows for a group controlling much less than 51% of the network power to take control of the network.[71] In fact, Eyal and Sirer posit that "a group of *any* size can compromise the system."[72] Recall that when an honest miner solves a crypto puzzle, it announces the resulting new block to the chain, and miners start looking for

65. *Hash Rate*, BLOCKCHAIN.COM, https://www.blockchain.com/en/charts/hash-rate [https://perma.cc/ACA3-JJQF] (last visited Sept. 1, 2019).

66. *See* Daniel Cawrey, *Are 51% Attacks a Real Threat to Bitcoin?*, COINDESK (June 20, 2014), https://www.coindesk.com/51-attacks-real-threat-bitcoin [https://perma.cc/Q9G6-NCSA].

67. *Id.*

68. *Id.*

69. *See* Eyal & Sirer, *supra* note 56.

70. *Id.*

71. *Id.*

72. *Id.* (emphasis added).

the next block to solve.[73] Selfish miners, conversely, do not.[74] Instead, selfish miners:

> keep [their] discovered blocks private, thereby intentionally forking the chain. The honest nodes continue to mine on the public chain, while the pool [of selfish miners] mines on its own private branch. If the pool discovers more blocks, it develops a longer lead on the public chain, and continues to keep these new blocks private. When the public branch approaches the pool's private branch in length, the selfish miners reveal blocks from their private chain to the public.[75]

This technique advantages selfish miners by forcing the honest miners to devote their resources to solving crypto puzzles that have no value.[76] This in turn incentivizes honest miners to join the pool of selfish miners.[77] There is some debate on what percentage of total miners behaving selfishly begins to post a threat of decentralization.[78] However, it is clear that it is much less than the traditionally assumed 51%.[79] Ettal and Sirer pose that "the threshold is close to zero. . . . [I]f less than 100% of the miners are honest, the system may not be incentive compatible."[80] Even the highest possible threshold is fairly low—"mining protocol will never be safe against attacks by a selfish mining pool that commands more than 1/3 of the total mining power of the network."[81]

Finally, blockchain is vulnerable to many of the traditional weaknesses associated with the digital storage of information. Recall that some blockchains use password-like private keys to authenticate the identity of users requesting a transaction.[82] Like traditional passwords, private keys can be lost, forgotten, or stolen. If a malicious actor gains access to a user's public and private keys, they can easily create fraudulent transactions with the legitimate user's identity. In the cryptocurrency context, this typically means currency would be stolen. In other use cases, it allows for fraudulent information to be placed into and "verified by" the blockchain.

It should be noted that these are just a few of the types of attacks to which blockchain is vulnerable, and new methods of undermining blockchain are still being discovered.[83] Further, blockchain technology can be adapted to defend against different kinds of attacks.[84] For example, the pioneers of selfish mining have proposed a protocol that would

---

73. *See supra* Part II.B.
74. Eyal & Sirer, *supra* note 56.
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *See supra* Part II.A.
83. *See generally* Joseph Bonneau, *Hostile Blockchain Takeovers*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 92–100 (Aviv Zohar et al. eds., 2018).
84. Eyal & Sirer, *supra* note 56.

lower the risk of successful selfish mining attacks.[85] However, not all blockchains have implemented this protocol.[86] Because protocols can vary, determining the reliability of any given blockchain record requires examining the protocols not of blockchain generally, but of the specific blockchain in question. Accordingly, when considering what the rule of decision pertaining to blockchain admissibility *should* be, as the author endeavors to do in Part V below, it is important to develop a standard that is sufficiently flexible to account for the variance in protocols.

III. BLOCKCHAIN AS HEARSAY UNDER THE FEDERAL RULES OF EVIDENCE

We now move from the foreign and unwelcoming shores of computer engineering back to the relative familiarity of legal analysis. Applying well-established evidentiary principles to what has been discussed above, it becomes clear that blockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios. However, as will be explored *infra*, this state of affairs contradicts the very purpose of hearsay doctrine.

Blockchain's most powerful opponent is the rule against hearsay, enshrined in FRE 802.[87] The underlying purpose of the rule against hearsay is to ensure the reliability of evidence introduced at trial.[88] Consider, then, the discussion above about the reliability of blockchain evidence.[89] In the absence of a 51% attack, selfish mining, or other exploitation of blockchain's vulnerabilities, blockchain technology produces records that are *extraordinarily* reliable.[90] This should be borne in mind, as it shows that the current FRE, which preclude almost entirely the admission of blockchain evidence, must be amended.

FRE 802 simply provides that hearsay is not admissible unless explicitly made admissible.[91] The threshold inquiry, then, is whether blockchain evidence can properly be called hearsay. FRE 801 explains that hearsay is an out-of-court statement of a person offered for "the truth of the matter asserted."[92] Consider first who is the relevant declarant of statements contained in a blockchain record. It is well-established that a machine cannot make a statement.[93] Ergo, if the relevant declarant is the blockchain network itself, there is no statement and no hearsay issue.

85. *Id.*
86. *See id.*
87. FED. R. EVID. 802.
88. BROUN ET AL., *supra* note 43, § 245 ("The factors upon which the value of testimony depends are the perception, memory, narration, and sincerity of the witness[.] . . . The rule against hearsay is designed to ensure compliance with these ideal conditions, and when one of them is absent, the hearsay objection becomes pertinent.").
89. *See supra* Part II.
90. Nakamodo, *supra* note 12.
91. FED. R. EVID. 802.
92. *Id.* at 801.
93. *See* United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007); City of Webster Groves v. Quick, 323 S.W.2d 386, 390 (Mo. Ct. App. 1959).

However, correctly viewed, the declarant is not the blockchain itself but the person inputting data into the blockchain. The blockchain merely stores information that is input by users.[94] The types of machines that courts have held cannot create statements are those that produce data independent of human input, such as vehicle speed detection devices.[95] Accordingly, properly considered, the declarant is not the blockchain ledger, but the user inputting data into the ledger.

A "statement" requires expressive intent[96]—a requirement that blockchain satisfies easily. The only purpose of putting information into a blockchain is to create a record of it. Therefore, the act of placing information on a blockchain per se establishes a statement sufficient to meet this element. It is equally clear that blockchain records are out of court. They are not made at trial and are not made under oath. Blockchain evidence, then, is clearly hearsay when it is offered for the truth of the matter asserted.

It is difficult to imagine for what else blockchain evidence could be asserted. Typical non-truth-of-the-matter-asserted rationales for introducing what would otherwise be hearsay include showing notice, impeachment of a witness, or effect on the listener.[97] Unless a witness has falsely testified at trial about the contents of a blockchain record, such records have no impeachment value. The "listener" of statements included on the blockchain record is the network. There is no probative value in showing the effect of a statement on the network because there is no effect on the network. However, even if a non-truth purpose could be found, using such a purpose limits how lawyers can argue the evidence presented—evidence admitted for a specific purpose can only be used to argue that purpose.[98] This needlessly constrains an advocate's ability to argue on the basis of reliable blockchain evidence. Further, the ability to use a non-truth purpose to admit blockchain evidence will inevitably be fact specific—there may be no non-truth purpose for which such evidence is relevant. Because blockchain evidence is generally reliable, its admissibility should not require the fortuitous happenstance that a given case has facts that make the evidence amenable to admission for non-truth purposes. This again makes clear that blockchain evidence will almost always, if not literally always, fall within the definition of hearsay.

One theory that has been advanced by some commentators is that blockchain evidence should be considered non-hearsay because it is computer-generated.[99] This argument proceeds by analogy, based on the

94. Bacon et al., *supra* note 13, at 2.
95. *Quick*, 323 S.W.2d at 390.
96. *See id.*
97. BROUN ET AL., *supra* note 43, § 249.
98. *Id.* § 59.
99. Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 CHI. KENT J. INTELL. PROP. 440, 446–47 (2017); James Ching, *Is Blockchain Evidence Inadmissible Hearsay?*, LAW.COM (Jan. 7, 2016), https://www.law.com/sites/jamesching/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/?slreturn=20190914194232 [https://perma.cc/9VPZ-5WRV].

Ninth Circuit's decision in *United States v. Lizarraga-Tirado*.[100] In *Lizarraga-Tirado*, the court held that Google Earth satellite imagery that had a labeling tack automatically placed on it by the Google Earth program was not hearsay because it was not a statement made by a person.[101] Because the "relevant assertion [wasn't] made by a person[, but rather] by the Google Earth program," there was no statement and, therefore, no hearsay.[102] Angela Guo argued in her article *Blockchain Receipts: Patentability and Admissibility in Court* that, "[s]ince humans do not actually generate the receipts on the blockchain, it is possible that courts will recognize distributed ledger receipts as computer-generated evidence and therefore not hearsay."[103]

However, *Lizarraga-Tirado* is uninstructive because blockchain evidence is not meaningfully comparable to Google Earth satellite images. Google Earth is a self-contained system: once it has been established, it does not require any human input to produce data. The satellite automatically takes photos, which it automatically marks with GPS information and then automatically uploads to the internet. Blockchain, conversely, requires human interaction. The beginning of any blockchain transaction is a user inputting data. That data is then *processed* automatically to generate the blockchain record, but the provision of the data originally comes from a human source. Accordingly, while it was proper for the *Lizarraga-Tirado* court to find that there was no declarant (and therefore no hearsay) of a statement by a totally self-contained and autonomous process, it does not follow that the logic of that case should be extended to a process, like blockchain, that begins with humans inputting information. In processes such as those, the proper view is that the user beginning the process by inputting the information is a declarant who is making a hearsay statement.

A. Hearsay Exclusions Generally Will Not Apply to Blockchain Evidence

As any trial lawyer could tell you, the possibility that evidence is admissible is not foreclosed simply because it meets the standard definition of hearsay.[104] The FRE create a variety of exceptions and exclusions from hearsay.[105] However, whether blockchain evidence can meet an exclusion will be extremely fact-dependent, and blockchain evidence will typically only satisfy the weakest of the exceptions.

100. Guo, *supra* note 99, at 445.
101. United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109–10 (9th Cir. 2015).
102. *Id.* at 1110.
103. Guo, *supra* note 99, 446–47.
104. *See* Broun et al., *supra* note 43, §245.
105. *See* Fed. R. Evid. 801, 803–04, 807. Note that the hearsay *exclusions*, listed at FRE 801, differ from exceptions at least in the taxonomical sense. An exception to hearsay acknowledges that a statement is hearsay but provides for admissibility nonetheless. *See id.* 803–04. An exclusion, conversely, transforms a statement that meets the definition of hearsay and categorizes it as non-hearsay. *See id.* 801(d).

We turn first to the exclusions from hearsay, established at FRE 801(d).[106] FRE 801(d) creates two general categories of exclusions from hearsay.[107] The first category pertains to previous statements given by a witness testifying at trial.[108] This exclusion does not warrant extensive discussion. It requires that the prior statement be subject to cross-examination, which blockchain entries are not.[109] Accordingly, this exclusion will never be met in the blockchain context.

The second category of exclusions from hearsay concerns statements against an opposing party.[110] Here, the facts of the case will dictate whether a party can avail themselves of this exclusion. If a statement was made by the party against whom it is offered, then it is not hearsay.[111] This would allow for the admission of blockchain evidence where the adverse party had entered the data onto the blockchain. However, cabining blockchain's admissibility so tightly is undesirable for a variety of reasons. Foremost among these is that it does not enable litigants to introduce their own blockchain records that help their case. Under this formulation, blockchain evidence is only a sword, never a shield. Suppose, for example, that a case is brought for breach of contract. The plaintiff claims that the defendant never paid for the services that the plaintiff provided. The defendant's claim is simple: he claims he did. He has a blockchain record showing that the correct amount of cryptocurrency funds was transferred from the defendant to the plaintiff. However, he is unable to introduce this evidence on an 801(d) theory as only the plaintiff may avail himself of FRE 801(d)(2). The defendant's meritorious defense may now be unprovable.

B. Hearsay Exceptions Generally Will Not Apply to Blockchain Evidence

Having determined that blockchain evidence will generally be hearsay that meets no exclusion, we must examine what exceptions, if any, would save blockchain from inadmissibility. The exclusions to the rule against hearsay are found in three places in the FRE: 803, 804, and 807.[112] The exceptions of FRE 803 are available regardless of whether the declarant is available to testify.[113] Conversely, FRE 804 exceptions require that the declarant is unavailable.[114] Finally, FRE 807 contains the residual excep-

106. *Id.*
107. *Id.*
108. *Id.* 801(d)(1).
109. *See id.*
110. *Id.* 801(d)(2).
111. *Id.* Note that a variety of types of statements by individuals related to the party-opponent, such as employees, co-conspirators, agents, spokesmen, and joint ventures are deemed to be the statements of a party-opponent for purposes of FRE 801(d)(2). *Id.* 801(d)(2)(A)–(E). This broadens the number of factual scenarios in which litigants may use this exception. It is not necessary that the named party himself input the data into the blockchain, if such an associated party did.
112. Fed. R. Evid. 803, 804, 807.
113. *Id.* 803.
114. *Id.* 804.

tion to hearsay, a catch-all provision to allow for the admission of hearsay that meets no recognized exception but, nonetheless, "has equivalent circumstantial guarantees of trustworthiness."[115] Considering blockchain evidence through each of these lenses in turn, it becomes clear that blockchain evidence is only generally admissible through the residual exception and that it may be difficult to admit even then.

FRE 803 provides for a litany of exceptions,[116] many of which do not merit discussion here. Two exceptions require attention, however. First, the public records exception of FRE 803(8) merits discussion, as more and more governments are turning to blockchain technology for the provision of governmental services.[117] Second, the business records exception of FRE 803(6) should be discussed because some scholars have proposed that it provides for the admission of blockchain evidence over a hearsay objection.[118] These arguments are not meritorious but deserve response.

1. The Public Records Exception for Blockchain in the Public Sector

Blockchain technology is seeing more and more application in government services.[119] Although no American government agency has yet widely adopted blockchain technology, the use of blockchain in foreign governments has bearing on the discussion of American evidentiary law. It is far from unthinkable that courts could be confronted with the need to examine the records of foreign governments to resolve issues of fact in multijurisdictional cases. Further, it is possible that the U.S. government will begin to employ blockchain technology in the future. In either case, the most relevant hearsay exception for this type of record is the public records exception.

FRE 803(8) provides an exception to hearsay when a record of a public office is introduced which "(A) . . . sets out: (i) the office's activities; (ii) a matter observed while under a legal duty to report . . . ; or (iii) . . . factual findings from a legally authorized investigation; and (B) the opponent does not show that the source of information or other circumstances indicate a lack of trustworthiness."[120]

Blockchain's typical use cases in government may fall within this exception. For example, blockchain has been employed to "digitize the process of issuing business licenses" in Dubai.[121] A blockchain record produced by a public office detailing which business licenses had been issued would fall within the ambit of FRE 803(8) because it would be a record that "sets out the office's activities."[122] Another proposed use case

115. *Id.* 807.
116. *Id.* 803.
117. *See, e.g.*, Refaat, *supra* note 5.
118. Guo, *supra* note 99, at 448; Ching, *supra* note 99.
119. *See, e.g.*, Refaat, *supra* note 5.
120. FED. R. EVID. 803(8).
121. Refaat, *supra* note 5.
122. FED. R. EVID. 803(8).

involves using blockchain to streamline the recordkeeping process for vehicle registration and property ownership.[123] Here, too, these would likely fall within the publication records exception. However, not all government use cases for blockchain would be admissible under public records. Take, for example, one commonly proposed use case—blockchain for election management.[124] The blockchain, it is proposed, could track the election and ensure its legitimacy.[125] The voting records of such an election, however, would not fall within FRE 803(8). It would not set out the actions of a public office, but rather the actions of private citizens making voting decisions.[126] It would not be a matter observed while under a legal duty to report; in fact, because who voters choose to vote for is secret, it would be a matter observed while under a legal duty *not* to report. It would further not be the findings of a legally authorized investigation. In short, this government use case, and many others like it, would not be, as a general proposition, admissible in federal court. As we have seen again and again, where blockchain evidence has any potential for admission under the current FRE standards, it requires a very specific set of facts.

2. The Business Records Exception

The business records exception of FRE 803(6) provides an exception to hearsay when a record is introduced and:

> (A) the record was made at or near the time by . . . someone with knowledge;
>
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling . . . ;
>
> (C) making the record was a regular practice of that activity;
>
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification . . . ; and
>
> (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.[127]

The history of the business records exception may seem to suggest that blockchain, at least in the cryptocurrency context, is a textbook example of a business record. In fact, the historical roots of the business records exception lie in seventeenth century England, where tradesmen were allowed to introduce their ledgers into evidence.[128] Blockchains are, essen-

123. John Palfreyman, *Blockchain for Government: Building Trust, Demolishing Bureaucracy*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Feb. 1, 2017), https://www.ibm.com/blogs/blockchain/2017/02/blockchain-government-building-trust-demolishing-bureaucracy/ [https://perma.cc/XN7Z-ULXB].

124. Jane Susskind, Comment, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 806 (2017).

125. *Id.* at 806–07.

126. *Id.* at 806.

127. FED. R. EVID. 803(6).

128. BROUN ET AL., *supra* note 43, § 285.

tially, digital ledgers.[129] However, the rationale behind allowing physical ledgers into evidence was that "[t]he regularity and continuity of the records [were] calculated to train the recordkeeper in habits of precision," which ensured the reliability of the data contained in the ledger.[130] This breaks the similarity between physical ledgers and blockchain. Blockchain ledgers have not yet obtained the ubiquity of use that the ledgers of the tradesmen in early England had. There is nothing to suggest that there is sufficient regularity of keeping blockchain records to have trained blockchain users to be precise.

Some commentators have advanced the argument that, nonetheless, FRE 803(6) provides for the admission of blockchain evidence.[131] Although the scholarship on the subject is exceedingly sparse, the consensus amongst those few commentators who have weighed in seems to be in favor of that proposition. First proposed by James Ching, the argument focuses on the reliability of the blockchain algorithm and whether blockchain receipts are "records."[132] While Ching correctly notes that the drafters of FRE 803(6) intended for "records" to be interpreted broadly,[133] he fails to discuss one of the key elements of the business records exception:[134] that the record be kept "in the course of *a regularly conducted activity* of a *business, organization, occupation, or calling*."[135] Taking into account this missing element of the business records analysis, it becomes clear that blockchain records will rarely be admissible as business records and that Ching's argument fails.

At the onset, we must determine *whose* regularly conducted activity is at issue—the user inputting the data or the blockchain network itself? In incentive-based mining systems, such as the Bitcoin and Ethereum blockchains, miners can and do make a profession of providing mining services to the blockchain in exchange for compensation.[136] A facially nonfrivolous argument could be made that the miner's constant devotion of resources (a regularly conducted activity) in exchange for compensation (a business or occupation) is sufficient to bring blockchain records within the ambit of the business records exception. However, this view is specious. Recall the classic analogy of blockchain to a physical ledger. The blockchain user is akin to the person writing in a traditional ledger; the blockchain is akin to the physical ledger itself. Applying the business records exception to a physical ledger, there is no question whether we are concerned with the activity of the ledger or the person writing in it. The physical ledger has no cognizable occupation or calling; the inquiry focuses on the person inputting information into the ledger. The same

129. *See* Nakamodo, *supra* note 12, at 3.
130. BROUN ET AL., *supra* note 43, § 286.
131. Guo, *supra* note 99, at 448; Ching, *supra* note 99.
132. Ching, *supra* note 99.
133. *Id.*
134. *Id.*
135. FED. R. EVID. 803(6) (emphasis added).
136. Castor, *supra* note 30.

should hold true in the blockchain context, and the argument that the network's own business, occupation, or calling could allow for the business records exception to apply to blockchain records must fail.

Application of the business records exception turns, then, on whether the record was made in the course of the *user's* regularly conducted activity in the course of business. In determining whether this exception is applicable, courts consider whether the record was "made for something other than a regular business purpose."[137] If it was, then the record falls outside the scope of the business records exception.[138] Currently, very few individuals and organizations regularly conduct business via blockchain technology. Accordingly, most, if not all, current applications of blockchain technology would fall outside the scope of the business records exception.

Assuming that a court held that a given blockchain record was created for regular business purposes, the difficulty of admitting blockchain evidence through FRE 803(6) is compounded by the question of who may serve as a sponsoring witness. The exception requires the testimony or certification of a custodian of record or another qualified witness.[139] A custodian can be defined as the person who is "responsible for securing and controlling access to evidence and maintaining the evidence in exactly the condition it was in when received."[140] In the blockchain context, there is no one human custodian of record, but rather, it is the network as a whole that maintains the record. Therefore, "another qualified witness" would need to sponsor the testimony.[141]

Courts have held that "[a] qualified witness is simply one who can explain and be cross-examined concerning the manner in which the records are made and kept."[142] In the context of blockchain, however, this is no simple task. To be "qualified" under that standard, a potential witness would need to be competent not only to testify to the manner in which the data entered into the blockchain was gathered by the user, but also to the specifics of how the specific blockchain at issue processed that data to produce the record. In many instances, identifying such a uniquely competent witness will prove impossible. Considering the above, the business records exception provides little value to litigants looking to admit blockchain evidence.

3. The Residual Exception—Blockchain's Last, Best Hope for Admissibility

Finally, we turn to the residual exception of FRE 807.[143] FRE 807 cre-

137. United States v. Kim, 595 F.2d 755, 761 (D.C. Cir. 1979).
138. *Id.*
139. FED. R. EVID. 803(6).
140. *Custodian,* BLACK'S LAW DICTIONARY (11th ed. 2019).
141. FED. R. EVID. 803(6).
142. Wallace Motor Sales, Inc. v. Am. Motor Sales Corp., 780 F.2d 1049, 1061 (1st Cir. 1985).
143. FED. R. EVID. 807.

ates a catch-all exception for evidence constituting hearsay that does not fall within a specifically recognized exception to the rule against hearsay.[144] Evidence qualifies for a residual exception when it (1) "has equivalent circumstantial guarantees of trustworthiness" to established hearsay exceptions; (2) is offered to prove a material fact; (3) is the most probative evidence on point that can reasonably be obtained; and (4) "admitting it will best serve the purposes of [the FRE] and the interests of justice."[145] Note that FRE 807 also requires that the opposing party be given reasonable notice of the intention of the evidence's proponent to offer hearsay under this exception.[146] This requirement is designed to provide the opponent a fair opportunity to respond to the hearsay exception argument.[147] This requirement is instructive in tailoring an ideal legal standard for the admission of blockchain evidence, as detailed in Part V below.[148]

Blockchain evidence makes a strong case for admission under the residual exception. Where a litigant introduces evidence from a blockchain and shows that the blockchain was not compromised, the guarantees of trustworthiness are in fact higher than most established hearsay exceptions. However, the legislative history of the residual exception militates against its long-term use to admit blockchain evidence. As McCormick explains, the Senate Advisory Committee proposed the residual exception to

> provide for treating new and presently unanticipated situations which demonstrate a trustworthiness within the spirit of the specifically stated exceptions. The House Judiciary Committee deleted the provisions entirely, believing they injected too much uncertainty into the law and arguing that *additional hearsay exceptions should be created by amending the rules*. . . . In arguing to restore these exceptions[,] . . . the Senate Judiciary Committee stated that it intended that the residual exception should be used "very rarely, and only in exceptional circumstances."[149]

Although the residual exception has seen a good deal of use over the years,[150] it has never been used in the long term as a repeated backdoor for an entire class of evidence. The preceding history of the residual exception makes clear that it would be inappropriate to use it in such a manner to admit blockchain long term.

---

144. *Id.*

145. *Id.*

146. *Id.*

147. *See* Jonathan E. Grant, *The Pre-Trial Notice Requirement of Federal Rule of Evidence 803(24)*, 36 DRAKE L. REV. 91, 97–98 (1986).

148. *See infra* Part V.

149. BROUN ET AL., *supra* note 43, § 324 (footnote and internal quotations omitted) (emphasis added) (quoting S. REP. NO. 1277, at 18–20 (1974), *as reprinted in* 1974 U.S.C.C.A.N. 7051, 7066).

150. *See, e.g.*, G. Michael Fenner, *The Residual Exception to the Hearsay Rule: The Complete Treatment*, 33 CREIGHTON L. REV. 265, 303–04 (2000).

Further, in cases that are not clear-cut, trial court judges may struggle to decide whether blockchain evidence has the necessary guarantees of trustworthiness. Determining whether a blockchain record is trustworthy is a technically complex endeavor, requiring exploration of the distribution of mining power to detect decentralization through exploits such as 51% attacks and selfish mining.[151] Necessarily, making the determination of whether a blockchain record is trustworthy will require the testimony of experts. This will doubtlessly lead to a battle of the experts, requiring heavy expenditure of both time and resources for the court and the litigants. Judges would be placed in the difficult position of making determinations about highly technical testimony without the manageable judicial standards that could be provided by an enumerated exception. Instead, they must parse through complex, technical issues to decide whether there are "equivalent circumstantial guarantees of trustworthiness."[152] This incredibly vague standard further complicates an already difficult judicial task. It becomes clear that, while the residual exception is currently the best method to admit blockchain evidence, on policy grounds, it is not a particularly good one.

The blockchain paradox, then, has presented itself in full. The animating concern of the rule against hearsay is ensuring the reliability of evidence.[153] Except in limited circumstances (when the blockchain has been centralized by bad actors), blockchain is exceedingly reliable. Except in limited circumstances (when the facts of a given case allow for a narrow exception or exclusion as detailed above), blockchain is patently inadmissible unless under an exception that is not intended to serve as a long-term route to admissibility for entire categories of evidence.[154] Under the FRE as currently written, blockchain is almost always reliable and almost never admissible. The question then becomes how the law should adapt to admit reliable blockchain evidence and exclude unreliable blockchain evidence.

IV. CURRENTLY IMPLEMENTED SOLUTIONS TO THE BLOCKCHAIN PARADOX

Very few countries, including the United States, have meaningfully addressed the problems presented by blockchain evidence. Unique among U.S. states is Vermont, where the state's Blockchain Enabling Act (the Act) creates a statutory scheme whereby, subject to certain conditions, blockchain evidence is presumptively authentic and admissible.[155] However, considering the discussion in Parts II.A and II.B above (especially regarding selfish mining) the conditions placed on admissibility by the legislature are inadequate. The Vermont approach represents a good first

151. *See* Eyal & Sirer, *supra* note 56.
152. FED. R. EVID. 807.
153. BROUN ET AL., *supra* note 43, § 324.
154. *Id.* (quoting S. REP. NO. 1277, at 18–20).
155. VT. STAT. ANN. tit. 12, § 1913 (2018).

effort but fails to take into account blockchain's vulnerabilities. The result is an overinclusive standard whereby unreliable blockchain evidence is admissible. The legislative history concerning the Act shows that these issues were not considered by the Vermont legislature.[156] In the international context, the Supreme People's Court of China has recently held that blockchain evidence is per se admissible.[157] Beyond these two examples, explored in more depth below, few jurisdictions have squarely addressed the admissibility of blockchain evidence.

First, we consider Vermont's Blockchain Enabling Act. The Act provides that blockchain records are self-authenticating and admissible when they are "accompanied by a written declaration of a qualified person, made under oath," and the declaration states (1) the qualifications of the affiant; (2) "the date and time the record entered the blockchain;" (3) the date and time it was pulled from the blockchain; (4) that the record's entry in the blockchain was part of "a regular conducted activity; and" (5) "the record was made by the regularly conducted activity as a regular practice."[158] These requirements closely mirror the business records exception to hearsay.[159] After having satisfied the requirements of the Act, the proponent of blockchain evidence need only show that (1) the record was made by someone with knowledge; and (2) the record was made at or near the time of the event recorded.[160] This creates a strong presumption—too strong of a presumption—in favor of the admissibility of blockchain evidence, even when the blockchain has become centralized.

The Act attempts to weaken this presumption by providing that the Act does not apply when "the source of information or the method or circumstances of preparation indicate lack of trustworthiness."[161] This language is imported part and parcel from a previous version of FRE 803(6).[162] This language implicitly places the burden on the opponent of the evidence to show that the blockchain evidence is unreliable.[163] Further, the Act does not distinguish between public and private blockchains, applying the same evidentiary standard to both.[164] While the Act provides a good starting point for a manageable evidentiary standard for blockchain records, these two flaws require correction.

---

156. Joanna Diane Caytas, *Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere*, COLUM. SCI. & TECH. L. REV. (May 30, 2017), http://stlr.org/2017/05/30/blockchain-in-the-u-s-regulatory-setting-evidentiary-use-in-vermont-delaware-and-elsewhere/ [https://perma.cc/NJE9-K7CK].

157. Zuìgao Renmin Fayuan Guanyu Hulianwang Fayuàn Shenli Anjian Ruogan Wenti De Guidìng [Interpretation of the Supreme People's Court on Certain Issues in Internet Court Trial Cases] (promulgated by the Sup. People's Ct. Sept. 6, 2018, effective Sept. 7, 2018), CLI.3.321342 (Lawinfochina) [hereinafter Supreme People's Court Interpretation No. 16].

158. Tit. 12, § 1913.

159. *Compare* tit. 12, § 1913, *with* FED. R. EVID. 803(6).

160. Tit. 12, § 1913.

161. *Id.* § 1913(b)(2).

162. *Compare* FED. R. EVID. 803(6), *with* tit. 12, § 1913.

163. Tit. 12, § 1913(b)(2).

164. *Id.* § 1913(c)(5).

The Supreme People's Court of China recently issued an interpretation of law holding that blockchain evidence is admissible per se.[165] This arises against the backdrop of recent changes in the Chinese court system. In 2017, China created the nation's first internet court in Hangzhou.[166] Two more internet courts opened in the cities of Beijing and Guangzhou in 2018.[167] These specialized courts have jurisdiction over suits arising out of online shopping disputes, internet service contracts, online copyright issues, domain names, and similar matters.[168] As part of an ongoing judicial reform for the Chinese courts, the Chinese Supreme People's Court determined that evidence stored on blockchain is admissible in cases before the three internet courts.[169]

In light of the foregoing discussion, it should be evident that a rule of per se admissibility is ill-advised. While blockchain is almost always reliable, it is not always reliable.[170] Accordingly, a per se rule fails to allow for the nuanced level of reliability that a sophisticated system of justice demands.

V. THE NEED FOR AN AMENDMENT TO THE FEDERAL RULES OF EVIDENCE ESTABLISHING STANDARDS OF ADMISSIBILITY FOR BLOCKCHAIN EVIDENCE

What is the solution to the blockchain paradox? A variety of approaches could be followed. The legislature could do nothing and wait for courts to address the problem. Interpretations of existing hearsay exceptions could be promulgated, broadening them to reach blockchain evidence. Courts could abuse the residual exception to hearsay in perpetuity to allow for blockchain evidence. The proper approach, however, is to formally amend the Federal Rules of Evidence creating an enumerated exception that creates manageable, blockchain-specific standards for admission.

First, this comment addresses why an amendment is the proper route by which to develop this law. An amendment promotes two major policy goals: uniformity and *ex ante* clarity. Finally, this comment concludes by articulating a proposed amendment which establishes manageable evidentiary standards that balance the need for blockchain evidence against the interest in keeping out unreliable evidence.

---

165. Supreme People's Court Interpretation No. 16, *supra* note 157.

166. Victoria Hudgins, *Could China's Internet Courts Work in the US?*, LAW.COM (Dec. 3, 2018), https://www.law.com/legaltechnews/2018/12/03/could-chinas-internet-courts-work-in-the-u-s/ [https://perma.cc/MG48-LXLR].

167. *Id.*

168. *Id.*

169. *Id.*

170. Nolan Bauerle, *What Are Blockchain's Issues and Limitations?*, COINDESK, https://www.coindesk.com/information/blockchains-issues-limitations [https://perma.cc/7N4M-72U5] (last visited Sept. 1, 2019).

A. Why an Amendment is the Proper Method to Change the Law Concerning Blockchain Evidence

Congress has recognized from time to time that the law of evidence must adapt to keep pace with changes in technology. For example, FRE 101 was amended on December 1, 2011, providing, *inter alia*, for the introduction of FRE 101(b)(6).[171] FRE 101(b)(6), for the first time, established that "a reference to any kind of written material or any other medium includes electronically stored information."[172] This is but one example of Congress's recognition that evidence law must change with the changing times. The purpose of the FRE was to "allow 'expansion (of the Federal Rules of Evidence) by analogy to cover new or unanticipated situations.'"[173] However, this analogy has its limits. Because the reliability of blockchain evidence depends on nuanced factors that cannot adequately be captured by analogy, to serve the overarching policy goal of ensuring the reliability of evidence, blockchain deserves a specially tailored standard.

Blockchain is "the biggest thing since the Internet."[174] While the technology is still developing, it has already begun to cause major overhauls in a variety of industries.[175] Before blockchain litigation becomes commonplace in the courts, Congress should take the opportunity to amend the FRE to create a uniform, predictable standard.

An amendment is the sole mechanism available for the development of the law on this issue that will provide such a uniform, predictable result. Uniformity of the law is of paramount importance, as it ensures that like parties will be treated alike, regardless of whether they bring suit in Alaska or Alabama.[176] If the law is developed through an ex post facto approach, it will inevitably become fractured as different judges take different approaches and arrive at different decisions. This in turn leads to disparate treatment under the law based on what jurisdiction a litigant happens to appear in (and in the early blockchain cases, possibly even based on what particular judge is assigned to a given case). Additionally, such an approach encourages forum shopping. If a plaintiff knows that this certain class of evidence is or is not admissible under the law of a certain jurisdiction, they can opt to bring suit in the forum most favorable

171. Fed. R. Evid. 101(b)(6).

172. *Id.*

173. United States v. Bibbs, 564 F.2d 1165, 1169 n.2 (5th Cir. 1977) (quoting *Hearings on Proposed Rules of Evidence Before the Subcomm. on Criminal Justice of the H. Comm. on the Judiciary*, 93d Cong. 4 (1973) (statement of Professor Cleary, Reporter for the Advisory Comm.)).

174. Bitcoin Magazine, *Why the Bitcoin Blockchain is the Biggest Thing Since the Internet*, Nasdaq (Apr. 19, 2016), https://www.nasdaq.com/article/why-the-bitcoin-blockchain-is-the-biggest-thing-since-the-internet-cm608228 [https://perma.cc/989B-QRGC].

175. *See* Aitken, *supra* note 7 (blockchain in healthcare); Quora, *supra* note 6 (blockchain in healthcare); Refaat, *supra* note 5 (blockchain in government).

176. *See* J. Collin Spring, *Pilots out of Uniform: How the Sixth Circuit's* Etihad *Decision Undermines the Purpose of the Montreal Convention*, 84 J. Air L. & Com. 153, 160–61 (2019).

to them. It need not stretch the imagination to believe that a cunning plaintiff's attorney, knowing that the opposition needs to adduce blockchain evidence to state their defense, might choose to bring suit in the jurisdiction with the most restrictive standards to introduce blockchain evidence. Conversely, where the evidence is beneficial to plaintiffs, they will doubtlessly bring suit in the forum where the developed standard is most lenient. An amendment to the FRE explicitly detailing the standard to which blockchain evidence should be held would abate this risk.

Further, an amendment alone provides clarity and predictability for the parties seeking to introduce blockchain evidence. At the core of the principle of legality is foreseeability.[177] Litigants in early blockchain cases should be provided with foreseeability and should not be forced to guess if a potentially crucial piece of evidence will be allowed in. Because, especially when a case revolves around the potential breach of a smart contract that doubles as a legal contract, there may be no other source to provide dispositive information, it is essential that litigants be given *ex ante* clarity on the standards of blockchain admissibility so as to avoid prejudicing their ability to present their claims and defenses.

Inaction would be particularly perilous. As discussed above, the current best approach to admit blockchain evidence is the residual exception to hearsay.[178] However, the residual exception provides an extremely ambiguous standard—"equivalent circumstantial guarantees of trustworthiness."[179] This approach gives judges little guidance on how to resolve crucial evidentiary questions and will likely lead to disparate and arbitrary results. Further, this exception was intended by its drafters to be used in extraordinary circumstances. If applied in the long term as a method to introduce blockchain evidence, it will cease to perform the exceptional function that it was intended to perform.

It is clear, then, that something must be done—and the best thing to do is amend the FRE today in anticipation of the litigatory issues of tomorrow.

B. Resolving the Paradox: A Proposed Standard of Admissibility

Considering the above discussion, the following amendment to the FRE is proposed to be inserted at FRE 803(24):[180,181]

177. Alan Nissel, *Continuing Crimes in the Rome Statute*, 25 Mich. J. Int'l L. 653, 674 n.112 (2004).

178. See *supra* Part III.B.3.

179. Fed. R. Evid. 807.

180. Recall from Part III that FRE 803 contains those exceptions to hearsay which do not require the unavailability of the declarant. The proposed blockchain exception is properly housed here because the availability of the declarant is immaterial to the reliability of the evidence when the other conditions placed upon admissibility by the proposed exception are met.

181. The currently existing FRE 803(24) would be restyled FRE 803(25).

(24) *Records stored on a blockchain ledger.* A record stored on a blockchain system if:

(a) the record is:

(i) from a public blockchain or from a private blockchain administered by the opposing party, and the opposing party does not show that the blockchain technology generating the record was compromised in such a manner that indicates the record's lack of trustworthiness;

(ii) pulled from a private blockchain which is administered by someone other than the opposing party, and the proponent of the evidence shows that the blockchain technology generating the record was not compromised in such a manner that indicates the record's lack of trustworthiness;

(b) the record was made at or near the time of the event;

(c) if the record did not execute a smart contract, then the record was made by someone with knowledge; and

(d) all these conditions are shown by the testimony of a qualified witness, or by certification.

(e) as used in this section:

(i) "Blockchain" means a cryptographically secured, chronological, and decentralized consensus ledger or consensus database maintained via the internet, peer-to-peer network, or other interaction.

(ii) "Blockchain technology" means computer software or hardware or collections of computer software or hardware, or both, that utilize or enable a blockchain.[182]

(iii) "Public blockchain" means a blockchain utilizing a network which can be freely joined by anyone.

(iv) "Private blockchain" means a blockchain utilizing a permissioned network, which can only be joined by those invited by the network administrator.

(v) A party "administers" a blockchain when it has the right and ability to permit or deny new nodes from joining the blockchain network.

(vi) If a blockchain does not meet either definition given it shall be treated as a private blockchain administered by someone other than the opposing party.

Under the proposed amendment, the burden to show the reliability or unreliability shifts based on the nature of the blockchain at issue. This protects both the reliability of the evidence and provides for judicial efficiency. When dealing with records pulled from a public blockchain, especially a large public blockchain, the chance of centralization attacks is lowered and centralization is harder to prove. As a result, showing unreli-

182. Note that the first and second definitions provided by the proposed amendment mirror the definitions provided in Vermont's Blockchain Enabling Act. VT. STAT. ANN. tit. 12, § 1913 (2018).

ability will necessarily require a large expenditure of time and resources both from the parties and the court. Accordingly, the burden is properly placed on the opponent of the evidence to show that the blockchain record is not reliable. In many instances, this will obviate the need to adduce evidence of reliability at all; if the parties agree that the blockchain was not compromised, no foundation need be laid to show the same.

Conversely, in private blockchains, the chance of centralization is heightened, and ensuring reliability requires that, if the proponent of the evidence is the administrator of the blockchain, he carries the burden to show the reliability of the records sought to be admitted. Because a proponent-administrator of a blockchain record could selectively control those persons invited to join the network, such that he controls the consensus mechanism (and could therefore create false entries), courts should require a greater showing of reliability. Parties should not be allowed to centralize their private blockchain, create false evidence, and then admit it in court simply because it came from a blockchain.

These concerns apply primarily to litigants seeking to introduce evidence from blockchains which they themselves administer. Where a litigant seeks to introduce evidence from a private blockchain administered by the opposing party, no such concerns exist. The opposing party should be given the chance, at least in theory, to show that their own blockchain was compromised, but the policies for the heightened standard do not apply. Therefore, these instances should be governed by the same logic that applies to public blockchain records.

Note further that the knowledge requirement is removed when the evidence sought to be admitted pertains to a smart contract transaction. Because smart contracts are self-executing,[183] no showing of personal knowledge is necessary if the technology is reliable. The record itself has sufficient knowledge of its contents when smart contracts are at issue.

Where smart contracts are not at issue, however, personal knowledge should be required of the declarant. Blockchain, generally, can verify that the information placed in it has not been changed. It cannot, however (absent verification protocols or a self-executing smart contract), verify the data that is input. Accordingly, the declarant's personal knowledge is important to show the level of reliability that justifies a hearsay exception.

This proposal represents a balanced approach to the admissibility of blockchain evidence that accounts for its vulnerabilities without placing undue burdens on litigants. In doing so, it solves the blockchain paradox: it transforms blockchain evidence from being almost always reliable and almost never admissible to being almost always reliable and admissible when it is. Congress should amend the FRE to adopt such a standard.

183. *See supra* Part II.A.

VI. CONCLUSION

In summation, considering the discussion of blockchain technology in Part III above, blockchain evidence is *extraordinarily* reliable, except in the exceptional circumstance. The current approaches that jurisdictions have taken to the admissibility of blockchain evidence leave much to be desire. Vermont and China have both created schemes which are overinclusive—they permit for both the admission of reliable and unreliable blockchain evidence. The FRE, which have yet to be amended to address squarely the issue of blockchain evidence, are underinclusive—they would preclude as hearsay evidence that is profoundly reliable (and reliability is the animating concern of the rule against hearsay). Accordingly, an amendment to the FRE is necessary. This amendment should be sensitive and narrowly tailored. The author urges Congress to consider adopting the amendment in Part V, above.