BLOCKCHAIN EVIDENCE: HOW SMART LITIGATORS CAN KEEP IT OUT AT TRIAL

*Alexandra Sahara**

INTRODUCTION

A blockchain is a peer-to-peer decentralized ledger that records transactions by creating a secure, time-stamped chain of information.[1] A network of nodes—computers that use a consensus mechanism[2] and cryptography—stores this information, creating a long and permanent history of verified transactions—in other words, blocks on the blockchain.[3]

* J.D. Candidate, 2024, Fordham University School of Law; B.S., 2016, New York University. I want to thank Professor Donna Redel for inspiring this piece through her Blockchain Law course. I also want to thank the *Fordham Law Review* editors, specifically Matthew Sandor and Lexi Meyer, for their guidance and support. Lastly, I am forever grateful to my wife, Saloni, without whom I would have given up before even applying to law school.

1. Sylvia Polydor, *Blockchain Evidence in Court Proceedings in China—A Comparative Study of Admissible Evidence in the Digital Age (As of June 4, 2019)*, 3 STAN. J. BLOCKCHAIN L. & POL'Y 96, 96 (2020).

2. Jake Frankenfield, *What Are Consensus Mechanisms in Blockchain and Cryptocurrency?*, INVESTOPEDIA (Feb. 17, 2023), https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp [https://perma.cc/FR4Y-J84K].

3. For more details on how a blockchain works and the function of a node, which are beyond the scope of this Essay, see *What Is Blockchain Technology?*, IBM,

Blockchain records provide valuable, verifiable documentation of facts that can be used in litigation; this renders blockchain a more attractive archival option compared to standard electronic archives, which can be altered.[4]

As more blockchains emerge, litigators will need to verify their authenticity and reliability because valuable and sensitive evidence may only be accessible via blockchain.[5] While the United States has not federally recognized the utility of blockchain evidence, multiple states have enacted legislation to tackle the unique reliability and authenticity challenges of blockchain.[6]

Vermont, for example, passed a statute that makes blockchain records admissible over hearsay objections if the records are accompanied by a written declaration of a qualified person who can testify to the details of the blockchain transaction.[7] It states that "a digital record electronically registered in a blockchain shall be self-authenticating" and that a "fact or record verified through . . . blockchain technology is authentic."[8] In 2018, Ohio modified the definitions of "electronic record" and "electronic signature" in its Uniform Electronic Transactions Act[9] to include records and signatures secured through blockchain.[10] Arizona also made changes to its electronic transaction law, establishing that signatures obtained through blockchain technology are valid and binding.[11]

Other nations have similarly enacted blockchain reliability and authentication legislation. For example, China's Supreme People's Court ruled in 2018 that, if the technology is proven legitimate, "internet courts . . . shall recognize the legality of blockchain as a method for storing and authenticating digital evidence."[12] That same year, the United Kingdom began experimenting with a pilot program that uses blockchain to secure evidence introduced in courts.[13]

---

https://www.ibm.com/topics/blockchain [https://perma.cc/PA4W-GCQ7] (last visited Apr. 25, 2024).

4. *See* Polydor, *supra* note 1, at 96.

5. *See* MORRISON COHEN LLP, CRYPTOCURRENCY LITIGATION AND REGULATION TRACKER (2023), https://www.morrisoncohen.com/siteFiles/News/TheMorrisonCohen CryptocurrencyLitigationTracker1.pdf [https://perma.cc/B6RL-4NQF].

6. Alex Ashrafi, Comment, *Blockchain as Evidence: How Will It Get into Court?*, WM. & MARY CTR. FOR LEGAL & CT. TECH., Oct. 2019, at 6.

7. *Id.* at 4–5.

8. VT. STAT. ANN. tit. 12, § 1913(b)(1), (b)(3)(A) (West 2018).

9. OHIO REV. CODE ANN. § 1306 (West 2018).

10. *Id.* § 1306.01(G)–(H) .

11. ARIZ. REV. STAT. ANN. § 44-7061 (2017).

12. Wolfie Zhao, *China's Supreme Court Recognizes Blockchain Evidence as Legally Binding*, COINDESK (Sept. 13, 2021, 4:21 AM), https://www.coindesk.com/markets/2018/09/07/chinas-supreme-court-recognizes-blockchain-evidence-as-legally-binding/ [https://perma.cc/PJ63-BZH5].

13. Muyao Shen, *UK Government Pilots Blockchain in Bid to Secure Digital Evidence*, COINDESK (Sept. 13, 2021, 4:18 AM), https://www.coindesk.com/markets/2018/08/23/uk-government-pilots-blockchain-in-bid-to-secure-digital-evidence/ [https://perma.cc/RT3A-V5Z8].

Yet, even if blockchain evidence is presumed authentic, courts must still determine its reliability. For example, a public, fully decentralized[14] blockchain, like Bitcoin or Ethereum, allows anyone to join a network and see a copy of the transactions made.[15] But a private, partially decentralized blockchain, like Hyperledger, Enterprise Ethereum, R3 Corda, or Ripple, will have only a single authority with control over the network.[16] While some blockchains, like private blockchains, may present attractive business options due to higher transaction speeds, lower costs, and increased efficiency, they may sacrifice key safety characteristics that public blockchains offer—like decentralized security.[17] This is because there are fewer validators or fewer intrinsic incentive layers in their rigid architecture.[18] These practices can degrade network integrity, making the blockchain data open to tampering or to security threats.[19]

Specifically, common blockchain practices like forking and chain reorganization[20] create opportunities for exploitation; this is because nodes looking to add new transactions to the chain are forced to decide which of several chains to follow so that the blockchain can keep operating.[21] This can increase the vulnerability of decentralized finance transactions and security threats, like 51 percent attacks,[22] which puts data at risk for tampering or other inaccuracies.[23]

This Essay addresses how forked blockchains are, in fact, not immutable. More importantly, it addresses how future litigators can convince judges that questionable data on unreliable blockchains should not be admitted in court. It proceeds in three sections. Part I outlines how blockchains are not always immutable, with an emphasis on forking, which undermines blockchains' reliability as evidence. Part II explains how courts have previously addressed

---

14. Decentralization is "the transfer of control and decision-making" from a central entity (either an individual or organization) to a distributed network. *What is Decentralization in Blockchain?*, AMAZON WEB SERVS., https://aws.amazon.com/blockchain/decentralization-in-blockchain/ [https://perma.cc/F7SH-AZN8]. The goal is to reduce the "level of trust that participants must place in one another, and deter their ability to exert authority or control over one another." *Id.*

15. Gwyneth Iredale, *The Rise of Private Blockchain Technologies*, 101 BLOCKCHAINS (Feb. 15, 2021), https://101blockchains.com/private-blockchain/ [https://perma.cc/44QV-UDCN].

16. *Id.*

17. Ian Scarffe, *Private Blockchains Are on the Rise in 2023*, LINKEDIN (Apr. 8, 2023), https://www.linkedin.com/pulse/private-blockchains-rise-2023-ian-scarffe/ [https://perma.cc/9FVC-WVUA].

18. *Id.*

19. *The Importance of Blockchain Security*, CHAINALYSIS (Oct. 5, 2023), https://www.chainalysis.com/blog/blockchain-security/ [https://perma.cc/Y6A9-NKCU].

20. For a discussion of forking and chain reorganization, see *infra* Part I.B.

21. Onkar Singh, *What is Chain Reorganization in Blockchain Technology?*, COINTELEGRAPH (May 29, 2022), https://cointelegraph.com/explained/what-is-chain-reorganization-in-blockchain-technology [https://perma.cc/QB4S-76EU].

22. A 51 percent attack is where a group acquires more than 50 percent of the hashing power of a cryptocurrency network. Murtuza Merchant, *What Is a 51% Attack and How to Detect It?*, COINTELEGRAPH (Nov. 12, 2022), https://cointelegraph.com/news/what-is-a-51-attack-and-how-to-detect-it [https://perma.cc/UUP5-5PUL].

23. Singh, *supra* note 21.

unreliable electronic evidence. Part III poses two litigation hypotheticals in which judges might deny the admission of blockchain evidence due to the unreliability of the blockchain.

I. THE FANTASY OF FORKING AND IMMUTABILITY

While forks are a useful and necessary blockchain management tool that can update software, add new functionality, or reverse transactions, they may also sacrifice blockchain security and reliability.[24] With each new fork comes an opportunity for the information stored on a blockchain to be revised, tampered with, subject to attack, or to otherwise reflect inaccuracies in transactions. Indeed, this assumes that the community can even agree as to which blockchain fork should be continued and maintained at all. Consequently, rather than accepting blockchain evidence as inevitably admissible, litigators should look closely at the quality of the blockchain records at issue and challenge them if the blockchain is subject to the security risks inherent to forking.

A. How Consensus Mechanisms Navigate the Blockchain Trilemma

A common expectation, and later misunderstanding, about blockchain is that the information recorded is permanent and immutable. But, while a ledger on a peer-to-peer network is generally difficult to change, Coin Sciences founder and CEO Gideon Greenspan has stated that "there is no such thing as perfect immutability."[25]

Blockchain consensus mechanisms—the standardized ways that a blockchain's nodes reach agreement on which blocks to validate—form the basis of this theoretical immutability.[26] These consensus mechanisms play a primary role in how a blockchain navigates the blockchain trilemma, which refers to the three main challenges that a blockchain must balance: scalability, security, and decentralization.[27] Prioritizing one of these factors may compromise the others.[28]

Consider Ethereum, which forked in 2022 to switch from a Proof of Work consensus mechanism to a Proof of Stake consensus mechanism.[29] Proof of Stake blockchains work because validators (i.e., nodes) are determined based

24. A blockchain fork occurs when a blockchain splits into two or more competing paths. For a discussion of forking and chain reorganization, see *infra* Part I.B.

25. *See* Venky Pai, *Which Features of Blockchain Create Immutability?*, BITCOIN EU (Sept. 5, 2018), https://bitcoin.eu/which-features-of-blockchain-create-immutability/ [https://perma.cc/7QBU-39JV]; Gideon Greenspan, *The Blockchain Immutability Myth*, LINKEDIN (May 4, 2017), https://www.linkedin.com/pulse/blockchain-immutability-muth-gideon-greenspan/ [https://perma.cc/G653-FDHL].

26. *What Is the Blockchain Trilemma?*, OPENSEA (June 28, 2023), https://opensea.io/learn/blockchain/the-blockchain-trilemma [https://perma.cc/SG8S-H8D7].

27. *Id.*

28. *Id.*

29. A comparison of consensus mechanisms is outside of the scope of this Essay. For more on this topic, see *Proof-of-Work vs. Proof-of-Stake: Why Did Ethereum Switch to Proof-of-Stake?*, BAKE (Sept. 18, 2023), https://blog.bake.io/why-did-ethereum-switch-to-proof-of-stake/ [https://perma.cc/XC8Z-LDV6].

on the size of their cryptocurrency stake in the blockchain. In contrast, a Proof of Work consensus mechanism like Bitcoin determines validators based on their computing power.[30] Because validators are chosen based on their stake in a Proof of Stake mechanism, the blockchain can increase its processing speed, as more transactions can be processed simultaneously.[31] Prioritizing speed and scalability, however, may sacrifice security and decentralization; for example, bad actors staking large amounts of cryptocurrency make the network susceptible to control by a central body and may increase the risk of double spending[32] during blockchain reorganization.[33]

B. Impossible Immutability and Forking

Blockchains, regardless of their consensus mechanism, often practice hard forking and chain reorganization, which contribute to the myth of immutability.[34] Public and private blockchains, including popular ones like Bitcoin or Ethereum and smaller ones like Solana, have experienced numerous forks.[35] Generally, a fork begins with a proposal of new code presented to the community with the goal of improving the blockchain's function or design.[36] However, if a majority of users or miners cannot agree on whether or how to execute the new code, or if they cannot agree on new rules to define a valid block on the chain, the blockchain splits (i.e., forks). In that case, one chain follows the new code and the other chain continues running the older code.[37]

---

30. *What Is the Blockchain Trilemma?*, *supra* note 26.

31. *Id.*

32. Double-spending happens when modified blocks enter the blockchain, allowing a person to reclaim already spent coins, a practice comparable to counterfeiting currency. Jake Frankenfield, *Understanding Double-Spending and How to Prevent Attacks*, INVESTOPEDIA (Aug. 16, 2023), https://www.investopedia.com/terms/d/doublespending.asp [https://perma.cc/7S7U-HWQK].

33. A reorganization occurs when a block is removed to make room for a longer chain. *Chain Reorganization in Blockchain Technology*, LCX (Sept. 7, 2023), https://www.lcx.com/chain-reorganization-in-blockchain-technology [https://perma.cc/D5XB-ZTZZ]; *What Is the Blockchain Trilemma?*, *supra* note 26. Additionally, blockchains that use other consensus mechanisms, like VeChain or Steem, may face a similar problem by exchanging security for scalability. For more on this topic, see Anders Bylund, *What Is Proof of Authority (PoA)?*, MOTLEY FOOL (Nov. 30, 2023, 10:00 AM), https://www.fool.com/terms/p/proof-of-authority [https://perma.cc/9LHQ-4MPK]; Frankenfield, *supra* note 32.

34. *Hard Forks*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/cryptocurrency/hard-fork/ [https://perma.cc/BC27-6MQW] (last visited Apr. 25, 2024). Note that this Essay will only cover hard forking (which results in multiple blockchains) and not soft forking (which only updates a single chain).

35. Jake Frankenfield, *Hard Fork: What It Is in Blockchain, How It Works, Why It Happens*, INVESTOPEDIA (May 25, 2022), https://www.investopedia.com/terms/h/hard-fork.asp [https://perma.cc/EU63-8D4N].

36. *Hard Forks*, *supra* note 34.

37. *Id.*; Frankenfield, *supra* note 35.

These forks have created a wide variety of sister cryptocurrencies, such as Bitcoin Cash, Bitcoin Gold, Segregated Witness, or SegWit2xin, all of which developed from the Bitcoin blockchain.[38] A hard fork is a radical and often necessary change to protocol; it can introduce critical security upgrades, add new functionality or, importantly, reverse transactions by making previously valid blocks invalid, or vice versa.[39] For instance, Ethereum has undergone a number of hard forks, including one in 2016 to reverse fraudulent transactions after hackers breached the first Decentralized Autonomous Organization (DAO).[40] In September 2022, Ethereum forked again as it transitioned from a Proof of Work model to a Proof of Stake model, reducing energy consumption by 99.9 percent.[41]

As a result, a hard fork will usually require all users to upgrade to the latest version of the software.[42] Otherwise, users will remain on the nondominant chain, even though that chain may become rapidly outdated and lose so many validators that the integrity of the chain itself cannot be adequately maintained.[43]

The recent Polygon hard fork demonstrates how a "block conflict" can also cause forks.[44] A block conflict, which is a common issue in busy blockchains like Ethereum, occurs when two blocks are produced simultaneously, resulting in a small blockchain fork.[45] The "Longest Chain Rule," which is traditionally used to resolve this conflict, treats the longest chain as the valid chain.[46] As a result, transactions on the invalid chain are delayed and restructured into new blocks, leading to chain reorganization.[47] To ensure that all nodes maintain an updated copy of the ledger, one block is ultimately deleted from the chain to make room for the longer chain.[48]

C. The Risks and Vulnerabilities of Forking

The more reorganizations and hard forks that occur, the easier it is for a malicious actor to take advantage of a blockchain because the cost of mining on multiple chains is low and miners can double spend[49] at no cost.[50] This

38. Katelyn Peters, *A History of Bitcoin Hard Forks*, INVESTOPEDIA (June 2, 2023), https://www.investopedia.com/tech/history-bitcoin-hard-forks/ [https://perma.cc/L6YL-97B8].

39. *Hard Forks*, *supra* note 34.

40. Frankenfield, *supra* note 35.

41. *What Are Blockchain Forks?*, OPENSEA (Sept. 20, 2023), https://opensea.io/learn/what-are-blockchain-forks#toc-3 [https://perma.cc/5XVP-XGY].

42. Frankenfield, *supra* note 35.

43. *Id.*

44. *See* Singh, *supra* note 21; Jamie Redman, *Polygon Announces Upcoming Hard Fork to Address Gas Spikes and Chain Reorganizations*, BITCOIN.COM NEWS (Jan. 14, 2023), https://news.bitcoin.com/polygon-announces-upcoming-hard-fork-to-address-gas-spikes-and-chain-reorganizations/ [https://perma.cc/73BS-SVA2].

45. Singh, *supra* note 21.

46. *Id.*

47. *Id.*

48. *Id.*

49. Frankenfield, *supra* note 32.

50. Singh, *supra* note 21.

creates a possibility of a 51 percent attack, in which malicious actors amass a majority of the hashrate (i.e., computational power) of a cryptocurrency.[51] With ownership of more than 50 percent of all the nodes that perform the blockchain-validating functions, those actors could introduce a different version of the blockchain—with different data or reversed transactions entirely—or execute a distributed denial-of-service (DDOS) attack.[52] For example, in 2018, Bitcoin Gold experienced a 51 percent attack, resulting in the theft of $18 million worth of Bitcoin Gold.[53]

Imagine a similar scenario in which a bad actor wants to undermine the immutability of a blockchain to spend cryptocurrency that they do not own and make fraudulent purchases. Gideon Greenspan describes this exact hypothetical:

> First, [the bad actor] would install more mining capacity than the rest of the network put together, creating a so-called "51% attack." Second, instead of openly participating in the mining process, they would mine their own "secret branch," containing whichever transactions they approve and censoring the rest. Finally, when the desired amount of time had passed, they would anonymously broadcast their secret branch to the network. Since the attacker has more mining power than the rest of the network, their branch will contain more proof-of-work than the public one. Every bitcoin node will therefore switch over, since the rules of bitcoin state that the more difficult branch wins. Any previously confirmed transactions not in the secret branch will be reversed, and the bitcoin they spent could be sent elsewhere.[54]

Satoshi Nakamoto—the pseudonym for the presumed creator of Bitcoin—assumed that acquiring more than 50 percent of Bitcoin's hashrate would be impossible.[55] He did not consider, however, the incentives behind a similar attack using altcoins—a rapidly developing market of nonmainstream blockchains in the post-Bitcoin world.[56] Greenspan further explains how a 51 percent attack targeting a mainstream or altcoin blockchain may be more than just a paranoid conspiracy:

> Think about the reports that bitcoin is being used by Chinese citizens to circumvent their country's capital controls. And consider further that the Chinese government's tax revenues are approximately $3 trillion per year. Would a non-democratic country's government spend 0.04% of its budget to shut down a popular method for illegally taking money out of that

51. Merchant, *supra* note 22.

52. *Id.*

53. Billy Bambrough, *Bitcoin Rival Suffers Devastating Attack*, FORBES (Jan. 28, 2020, 3:48 PM), https://www.forbes.com/sites/billybambrough/2020/01/28/bitcoin-rival-suffers-devastating-attack/ [https://perma.cc/4QMU-UHLZ].

54. Greenspan, *supra* note 25.

55. *51% Attacks*, MIT DIGIT. CURRENCY INITIATIVE, https://dci.mit.edu/51-attacks [https://perma.cc/7VE9-VS87].

56. Altcoins are generally defined as all cryptocurrencies other than Bitcoin. Jake Frankenfield, *Altcoin Explained: Pros and Cons, Types, and Future*, INVESTOPEDIA (Dec. 31, 2023), https://www.investopedia.com/terms/a/altcoin.asp [https://perma.cc/U4ED-6EZW]; *51% Attacks*, *supra* note 55.

> country? I wouldn't claim that the answer is necessarily yes. But if you think the answer is definitely no, you're being more than a little naive. Especially considering that China reportedly employs 2 million people to police Internet content, which totals $10 billion/year if we assume a low wage of $5,000. That puts the $1.2 billion cost of reversing a year of bitcoin transactions in perspective.[57]

Smaller blockchains are more vulnerable to 51 percent attacks because it takes a significantly smaller number of miners to accumulate more than 50 percent of the blockchain's hashrate, and mining rental services have made it cheaper to acquire the necessary hardware for executing such attacks.[58] In fact, many altcoins have their network hashrate available to rent, leading to a number of high-value attacks.[59] Furthermore, "51% attacks are transient events meaning that unless they are observed at the time of attack, it is not possible to detect them later."[60]

D. Solana: An Example of Forking and Unreliability

Solana, a competitor of Ethereum and a mixed Proof of Stake and Proof of History blockchain,[61] is a perfect example of a heavily forked blockchain with significant outages that faced the dual threat of double transactions and unreliability.[62] Solana's smart contract platform has garnered immense popularity for its speed and performance, but its construction is vulnerable to centralization and security risks because there are relatively few blockchain validators.[63] In August 2022, Solana had only 3,400 unique validators compared to Ethereum's 426,000 validators, raising questions about the scale at which Solana could maintain such rapid transactions.[64] "With such a large concentration of on-chain wealth being held by a small number of addresses, this prompts potential issues with governance, limits the number of individuals that could become validators, and reduces overall network security. . . . Solana has been overloaded by transactions that have led to outages and a degraded network."[65]

---

57. Greenspan, *supra* note 25.
58. *51% Attacks*, *supra* note 55.
59. *Id.*
60. *Id.*
61. Martin Young, *Solana Records 1 Outage in First Half of 2023, 100% Uptime in Q2*, COINTELEGRAPH (July 21, 2023), https://cointelegraph.com/news/solana-uptime-improves-with-one-outage-this-year [https://perma.cc/8ESE-35GT].
62. *See* Rob Behnke, *Solana Security Overview*, HALBORN (Feb. 13, 2023), https://www.halborn.com/blog/post/solana-security-overview [https://perma.cc/ZZ4V-4JGM].
63. Sasha Shilina, *What is Solana, and How Does It Work?*, COINTELEGRAPH (Mar. 6, 2022), https://cointelegraph.com/news/what-is-solana-and-how-does-it-work [https://perma.cc/4D45-EWQV]; Zachary Lorance, *Solana Core Report*, CRYPTOEQ (Jan. 5, 2024), https://www.cryptoeq.io/corereports/solana-abridged [https://perma.cc/9554-2UG5].
64. Seth Rowden, *What Are the Problems with Solana? What Is the Biggest Drawback of Solana?*, BITKAN (June 20, 2023), https://bitkan.com/news/what-are-the-problems-with-solana-what-is-the-biggest-drawback-of-solana-16522 [https://perma.cc/VS6U-S99Y].
65. Lorance, *supra* note 63.

Of course, Solana was not the only blockchain facing outage issues. Others had problems when trying to scale their platforms. In late 2023, the Aptos blockchain shut down for over four hours, leading major exchanges like Upbit and OKX to suspend Aptos deposits and token withdrawals, all of which raised concerns about the blockchain's robustness and reliability.[66]

Ultimately, the very consensus mechanisms that allow blockchains to operate on such a large scale are the same mechanisms that require maintenance through practices like chain reorganization and forking. Indeed, though blockchains are often hailed as immutable, discounting the ways that blockchains can be altered and, therefore, made unreliable—whether by the community's intentional, democratic decisions or by malicious actors—would do courts a disservice.

II. ELECTRONIC UNRELIABILITY IN THE COURTS

As may be expected, patently unreliable evidence, including from an expert or specialist, is generally not admissible in a trial.[67] The introduction of evidence in federal courts, as governed by the Federal Rules of Evidence (FRE), requires evidence to be relevant, authentic, and reliable.[68] If evidence does not rise to that level, it is not admissible.[69]

FRE 901, which covers authentication requirements, establishes a baseline standard to test the reliability of evidence: "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[70] However, "[b]ecause it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the 'final' or legally operative

66. Qadir AK, *Aptos Blockchain Shuts Down for 4+ Hours, Sparks Concern Among Users*, COINPEDIA (Oct. 19, 2023), https://coinpedia.org/news/aptos-blockchain-goes-offline-for-over-four-hours-upbit-and-okx-suspend-operations/ [https://perma.cc/2M5U-ABSX].

67. FED. R. EVID. 702 advisory committee's note to 2023 amendment ("Rule 702(d) has also been amended to emphasize that each expert opinion must stay within the bounds of what can be concluded from a reliable application of the expert's basis and methodology. Judicial gatekeeping is essential because just as jurors may be unable, due to lack of specialized knowledge, to evaluate meaningfully the reliability of scientific and other methods underlying expert opinion, jurors may also lack the specialized knowledge to determine whether the conclusions of an expert go beyond what the expert's basis and methodology may reliably support.").

68. Polydor, *supra* note 1, at 104; *see also* FED. R. EVID. 402 (prohibiting the inclusion of "irrelevant" evidence); FED. R. EVID. 702 (addressing expert evidence reliability); FED. R. EVID. 702 advisory committee's note to 2000 amendment (stating that "the [Supreme] Court charged trial judges with the responsibility of acting as gatekeepers to exclude unreliable expert testimony, and the Court . . . clarified that this gatekeeper function applies to all expert testimony, not just testimony based in science. . . . [T]he Rule as amended provides that all types of expert testimony present questions of admissibility for the trial court in deciding whether the evidence is reliable and helpful"); FED. R. EVID. 901 (establishing the requirements of evidence authenticity).

69. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (noting that electronically stored information must, among other things, satisfy the evidence rules of relevance under FRE 401, authenticity under FRE 901, and hearsay under FRE 801).

70. FED. R. EVID. 901(a).

version."[71] FRE 901(b)(4) provides a nonexhaustive list of evidence that satisfies the requirements, including distinctive characteristics of the evidence in question.[72] The hash values associated with blocks in the blockchain, which are inserted at inception, are distinctive characteristics that can allow for authentication under FRE 901(b)(4) for those documents and transactions.[73]

As of 2017, the amended FRE 902 allows for certain evidence to self-authenticate when a certified record is generated by an electronic process or system.[74] Importantly, the advisory notes to FRE 902 seem to reference by implication how blockchain records can be offered as evidence,[75] stating that "identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that [they] checked the hash value of the proffered item and that it was identical to the original."[76]

Indeed, in most states, any form of computerized data, including blockchain evidence, raises unique questions about reliability (i.e., whether the data is accurate) and authenticity (i.e., whether the data is likely free from tampering). Any electronic program that is susceptible to programming errors, hacking, and power outages may hinder reliability.[77] Consequently, given blockchain's special characteristics, judges should consider the accuracy and reliability of computerized evidence when ruling on the admissibility of blockchain evidence.[78]

Recent case law may provide insight into how and why blockchain evidence may be admitted, particularly where machine statements might function as unreliable hearsay.[79] Some courts may demand that the moving party independently demonstrate the accuracy of computer-generated records, even if they are not considered hearsay.[80] A Missouri appellate court, for example, held on plain error review that a trial court did not err in admitting a trace report—a computer generated report of telephone call data by a telephone company's computer—over the defendant's hearsay objection.[81] The court adopted the position found in Professor Charles T. McCormick's treatise on evidence that "records of this type are not the

71. *Lorraine*, 241 F.R.D. at 547 (citing FED. R. EVID. 901(b)(4)).

72. FED. R. EVID. 901(b)(4).

73. *See id.*; Emily Knight, Note, *Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility Under the Federal Rules*, 48 HOFSTRA L. REV. 519, 550 (2019) ("Within this Rule, are two subsets of accurate data relating to blockchain: FRE 901(b)(4)—distinctive characteristics, and 901(b)(9)—evidence about a system or process.").

74. FED. R. EVID. 902; Polydor, *supra* note 1, at 104.

75. Polydor, *supra* note 1, at 104.

76. FED. R. EVID. 902 advisory committee's note to 2017 amendment.

77. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 557 (D. Md. 2007).

78. 1 DAVID F. HERR, ANNOTATED MANUAL FOR COMPLEX LITIGATION § 11.446 (4th ed. 2023); *Lorraine*, 241 F.R.D. at 557–59; Polydor, *supra* note 1, at 104.

79. *Expert Q&A on Developing Issues in Blockchain Litigation*, THOMSON REUTERS (July 29, 2019), https://uk.practicallaw.thomsonreuters.com/w-021-4555 [https://perma.cc/8QDR-JMUY].

80. *See generally* State v. Dunn, 7 S.W.3d 427 (Mo. Ct. App. 1999).

81. *Id.* at 431.

counterpart of a statement by a human declarant."[82] Instead, "they should not be treated as hearsay, but rather their admissibility should be determined on the basis of the reliability and accuracy of the process involved."[83]

In *United States v. Lizarraga-Tirado*,[84] the Ninth Circuit considered the admission of Google Earth evidence.[85] It found that self-authenticated data made by a program and not by a person may be offered to the court; where there are authenticity or malfunction claims, a party may establish reliability and accuracy through the testimony of an expert or witness who frequently works with the program.[86] The court specifically ruled that a Google Earth image showing a pinpoint of the defendant's location was admissible over the defense's objection that the satellite image and the digitally added pinpoint labeled with GPS coordinates were impermissible hearsay.[87] The court reasoned that the satellite image evidence was not hearsay because the data merely showed a scene as it existed at a specific time, rather than making an assertion.[88] Furthermore, the court noted that concerns about machine tampering, malfunction, or inconsistency should be addressed by authentication rules and not by hearsay rules.[89] The court also noted that proponents of evidence should address authentication objections through expert testimony.[90]

The Tennessee Supreme Court in *State v. Hall*[91] also held that a party must prove the reliability of evidence generated by a computer system through someone with knowledge about the operation of that computer system.[92] This is because "the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy."[93]

Under FRE 201(b), if certain technology is widely considered reliable and not subject to reasonable dispute, courts may take judicial notice of that fact because it is "generally known" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned."[94] Judges can apply this rule to any matter of public record, but not to disputed facts

82. *Id.* at 432 (quoting KENNETH S. BROUN, GEORGE E. DIX, MICHAEL H. GRAHAM, D.H. KAYE, ROBERT P. MOSTELLER & E.F. ROBERTS, MCCORMICK ON EVIDENCE § 294 (John W. Strong ed., 48th ed. 1992)).

83. *Id.*

84. 789 F.3d 1107 (9th Cir. 2015).

85. *See generally id.;* Polydor, *supra* note 1, at 104.

86. *Lizarraga-Tirado*, 789 F.3d at 1109–10.

87. *Id.* at 1108.

88. *Id.* at 1109.

89. *Id.* at 1110.

90. *Id.*; *see also* United States v. Espinal-Almeida, 699 F.3d 588, 612 (1st Cir. 2012) (evaluating whether "marked-up maps generated by Google Earth" were properly authenticated and concluding that they were).

91. 976 S.W.2d 121 (Tenn. 1998).

92. *Id.* at 147.

93. *Id.* (quoting State v. Meeks, 867 S.W.2d 361, 376 (Tenn. Crim. App. 1993)); *see also* United States v. Rollins, No. ACM34515, 2004 WL 26780, at *9–10 (A.F. Ct. Crim. App. Dec. 24, 2003), *aff'd in part*, *rev'd in part and remanded*, 61 M.J. 338 (C.A.A.F. 2005).

94. FED. R. EVID. 201(b).

contained in public records.[95] If a fact can be reasonably disputed, especially because a system may be found unreliable, then courts may not take judicial notice of facts that are favorable to the moving party.[96] In cases where both parties debate the reliability of evidence, courts can decide whether to admit the evidence and allow the jury to determine its weight or to deny the admission of that evidence entirely.[97]

The court's decision is critical in the early stages of litigation—for example, if a judge must rule on a motion to dismiss under Federal Rule of Civil Procedure (FRCP) 12(b)(6). In *Hunichen v. Atonomi*,[98] Hunichen alleged that Atonomi violated the Securities Act of Washington,[99] Atonomi countersued, and Hunichen moved to dismiss the counterclaim under FRCP 12(b)(6).[100] Hunichen's motion to dismiss relied on materials outside of the pleadings, including blockchain transaction records, which they argued were publicly available, unalterable, and undisputable as public records.[101] Hunichen also argued that the blockchain evidence was incorporated by reference because Atonomi necessarily accessed it to describe a select number of transactions in the pleadings.[102]

Citing *Khoja v. Orexigen Therapeutics*,[103] the court agreed with Atonomi and found that, given the disputes over the content of the evidence, including the transactions, it could not take judicial notice of the blockchain records.[104] In *Khoja*, the Ninth Circuit held that the district court improperly took judicial notice of an agency report and a transcript submitted with SEC filings because the substance of those materials was "'subject to varying interpretations' and there was reasonable dispute as to what facts were established."[105] The *Hunichen* court also found that Hunichen failed to show that the blockchain evidence was complete and that its content was not

95. Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988, 998 (9th Cir. 2018) (quoting Lee v. City of Los Angeles, 250 F.3d 668, 688 (9th Cir. 2001)).

96. United States v. Corinthian Colls., 655 F.3d 984, 999 (9th Cir. 2011) (citing Lee v. City of Los Angeles, 250 F.3d 668, 689–90 (9th Cir. 2001)).

97. FED. R. EVID. 702 advisory committee's note to 2000 amendment ("The trial judge in all cases of proffered expert testimony must find that it is properly grounded, well-reasoned, and not speculative before it can be admitted.").

98. No. C19-0615, 2020 WL 6875558, at *1 (W.D. Wash. Oct. 6, 2020), *report and recommendation adopted*, No. C19-0615, 2020 WL 6874889 (W.D. Wash. Nov. 23, 2020).

99. WASH. REV. CODE § 21.20.

100. *See generally* Motion to Dismiss Counterclaim and Third Party Claims, Hunichen v. Atonomi LLC, No. C19-0615, 2020 WL 6875558 (W.D. Wash. July 20, 2020), 2020 WL 7395844.

101. *Hunichen*, 2020 WL 6875558, at *5–6; *see also generally* Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190, 1204 (N.D. Cal. 2014) (stating that courts can take judicial notice of "publically [sic] accessible websites"); United States v. Gratkowski, 964 F.3d 307, 309 n.2 (5th Cir. 2020) (defining blockchain as "a technological advancement that permits members in a shared network to 'record a history of transactions on an immutable ledger'" (quoting Ashley N. Longman, Note, *The Future of Blockchain: As Technology Spreads, It May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 118 (2019))).

102. *Hunichen*, 2020 WL 6875558, at *1.

103. 899 F.3d 988 (9th Cir. 2018).

104. *See Hunichen*, 2020 WL 6875558, at *5–6.

105. *Khoja*, 899 F.3d at 1000.

subject to dispute or varying interpretation.[106] As a result, the court denied the motion.[107]

In most cases, the reliability of blockchain evidence offered through an expert can be challenged in two ways. First, litigators can challenge it because it may implicate hearsay issues.[108] The data on the blockchain is often an assertion that is offered to prove the truth of the matter—in other words, to prove that a certain transaction did happen between two parties or wallets.[109] Second, litigators may challenge the reliability of the expert evidence itself, arguing either that (1) the tools used to come to conclusions or analyze data are flawed, or (2) the methodology used does not rise to the standards established by the scientific community.

Daubert v. Merrell Dow Pharmaceuticals[110] established the courts' role as gatekeepers of expert evidence and the considerations for its admission.[111] The court must ensure that speculative, unreliable expert testimony does not reach the jury.[112] When determining whether an expert's testimony is reliable, the "trial judge must assess 'whether the reasoning or methodology underlying the testimony is scientifically valid and . . . whether that reasoning or methodology properly can be applied to the facts in issue.'"[113] Specifically, the court must examine, among other things, "(1) whether the expert's theory can be and has been tested; (2) whether the theory has been subjected to peer review and publication; (3) the known or potential rate of error of the particular scientific technique; and (4) whether the technique is generally accepted in the scientific community."[114]

For example, one court decided to strike an expert report that "lack[ed] . . . any identifiable 'methodology' to which the Court [could] apply the *Daubert* factors."[115] Another court similarly struck an expert report that was "not based on any methodology that [was] readily apparent from the record."[116]

In deciding the reliability of evidence and expert testimony, trial judges have considerable discretion. For example, judges may consider whether an expert's methodology "has been contrived to reach a particular result."[117] In

106. *Hunichen*, 2020 WL 6875558, at *6.
107. *Id.* at *6–7.
108. Polydor, *supra* note 1, at 104.
109. *Id.*
110. 509 U.S. 579 (1993).
111. *See generally id.*
112. *See* McCorvey v. Baxter Healthcare Corp., 298 F.3d 1253, 1256 (11th Cir. 2002); Kleiman v. Wright, No. 18-CV-80176, 2020 WL 6729362, at *4 (S.D. Fla. Nov. 16, 2020).
113. United States v. Frazier, 387 F.3d 1244, 1261–62 (11th Cir. 2004) (quoting *Daubert*, 509 U.S. at 592–93).
114. *Id.* at 1261–62 (quoting Quiet Tech. DC–8, Inc. v. Hurel–Dubois UK Ltd., 326 F.3d 1333, 1341 (11th Cir. 2003)).
115. Am. Gen. Life & Accident Ins. Co. v. Ward, 530 F. Supp. 2d 1306, 1314 (N.D. Ga. 2008).
116. Agri-AFC, LLC v. Everidge, No. 16-CV-00224, 2019 WL 385421, at *15 (M.D. Ga. Jan. 30, 2019).
117. *Kleiman*, 2020 WL 6729362, at *18 (quoting Rink v. Cheminova, Inc., 400 F.3d 1286, 1293 n.7 (11th Cir. 2005)).

Kleiman v. Wright,[118] the U.S. District Court for the Southern District of Florida reviewed the relationship between reliability and *Daubert* in expert testimony regarding blockchain transactions.[119] There, the defendant challenged a section of an expert report because it relied on documents from an anonymous source that could not be authenticated and included hearsay messages attacking the defendant's character.[120] The court held that the report and testimony could not be used as a conduit to present inadmissible evidence purely to attack the defendant's character for truthfulness.[121] The court found that the plaintiffs failed to satisfy FRE 803(6)—the business records exception to the rule against hearsay[122]—because they did not demonstrate that one of the messages at issue was kept in the course of "a regularly conducted activity of a business."[123] Further, the court found that certain bitcoin messages, including one about the defendant's character for truthfulness, were inadmissible hearsay and not otherwise admissible through an expert because their probative value did not substantially outweigh their prejudicial effect.[124]

Ultimately, these cases show that courts will generally not admit evidence that is unreliable, inauthentic, or irrelevant. If evidence—offered through an expert or otherwise—does not rise to that level, it is not admissible. However, future cases involving forked blockchains may require courts to wrestle with their discomfort about unreliable evidence.

III. HYPOTHETICAL CASES USING EVIDENCE FROM UNRELIABLY FORKED BLOCKCHAINS

Few public cases, if any, grapple with the possibility of unreliable blockchains and activities that might facilitate such unreliability (e.g., forking). Future cases, however, will have to determine when blockchain evidence is unreliable and at what point that evidence should be excluded at trial. Judges will have to scrutinize any evidence stored on unreliable blockchains. Consider two possible, and arguably likely, future scenarios in which a litigator should argue for the exclusion of blockchain evidence: (1) where a community cannot decide on which fork to follow, and (2) where a fork is unreliably managed by too small a community.

A. The Undecided Fork

Some might assume that hard forks happen overnight. On the contrary, hard forks often require a full proposal for a change in code.[125] The

118. No. 18-CV-80176, 2020 WL 6729362 (S.D. Fla. Nov. 16, 2020).
119. *Id.* at *31.
120. *Id.* at *27.
121. *Id.* at *30.
122. *See* FED. R. EVID. 803(6)(B).
123. *Kleiman*, 2020 WL 6729362, at *30 (quoting FED. R. EVID. 803(6)(B)).
124. *Id.*
125. Team Nas Academy, *What the Fork? What Are Blockchain Forks and How Do They Work?*, NAS EDUC., https://nasacademy.com/blog/article/what-is-blockchain-fork [https://perma.cc/Z2EL-UYHS] (last visited Apr. 25, 2024).

community then takes time to decide whether to implement that fork.[126] Meanwhile, if the community keeps debating which fork is legitimate, both forks will exist simultaneously because they have not decided which chain to follow.[127]

Consider the Ethereum DAO hack in 2016.[128] There, hackers found a vulnerability in Ethereum's smart contracts codebase and stole 3.6 million Ether raised from the DAO—the equivalent of about $50 million.[129] Consequently, on June 17, 2016, the Ethereum community proposed a hard fork to reverse the transactions and overwrite the blockchain history so that the original investors could regain their Ether.[130] Most of the community at the time supported the fork to reverse the transactions; however, a significant number of community members believed that reversing the transactions violated the key attraction of blockchain—immutability.[131] As a result of this heated debate, one portion of the community forked Ethereum's blockchain to create Ethereum Classic.[132] It was not until a month later, on July 20, 2016, that the hard fork was actually completed.[133] Even now, two versions of Ethereum coexist—one with a record of reversed transactions and one that was actually immutable.[134]

Now consider this hypothetical. In 2033, a similar hack of the DAO operating on a heavily forked blockchain, Z, has occurred, resulting in the theft of millions of dollars. Consequently, the community proposes another fork, but only half of the community is in favor of reversing the transactions. The other half fervently wants to continue the blockchain as is to preserve immutability. Locked in a head-to-head battle, this fork remains unresolved for months, with no signs of resolution. Because the code does not immediately adopt changes, two coexisting forks are now growing with every transaction, but with key information that is conflicting—one chain reflecting that a major hack occurred, while the other chain is operating as if nothing happened.

Meanwhile, there is an ongoing litigation and blockchain Z—specifically, the transactions dealing with the hack—is at the heart of that litigation. A prosecutor requires data from blockchain Z to convict a hacker of conspiracy and fraud, alleging that money was improperly moved from a legitimate user's wallet to the hacker's wallet. The defense will argue that one chain—the chain that has removed the evidence of the hacking transactions—is the proper chain to consider. The prosecutor, however, will argue that the other

126. *Id.*
127. *Id.*
128. DELOITTE, THE DAO: CHRONOLOGY OF A DARING HEIST AND ITS RESOLUTION 2 (2016), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte_Blockchain_Institute_Whitepaper_The_DAO.pdf [https://perma.cc/5EYW-2BZC].
129. *Id.* at 3.
130. *Hard Forks*, *supra* note 34; DELOITTE, *supra* note 128, at 6.
131. OPENSEA, *supra* note 41.
132. *Id.*
133. DELOITTE, *supra* note 128, at 5.
134. *Id.* at 8 ("[In] evaluating the hard fork . . . it is interesting to look at the unexpected consequence of this decision: the coexistence of two currencies.").

chain—the chain that did not remove the transactions—is proper because it contains evidence of the hack.

Without the Z community affirmatively adopting one chain or the other, a court could consider two options. First, they could admit evidence of both forks, assuming more data is more probative than prejudicial to the defendant. Second, if the court determines that no reasonable jury could find a disputed fact as to which chain is valid, it could deny the admission of either fork in favor of the other. A defendant could then make a hearsay objection to the chain—the one suggesting criminal liability—arguing that it would be used to prove the truth of the fact that the defendant made the illicit transaction.[135] It is unlikely that the prosecution could, with certainty, advocate for the admissibility of this evidence in a jurisdiction that has not established authentication of blockchain evidence or where blockchain evidence is not considered a business record.

Consequently, any chain experiencing a live dispute between forks would raise a question of reliability as to which fork is the proper record of transactions for a court to follow. In that case, a litigator could argue that the evidence has not been validated, authenticated, or generally accepted by the community that maintains those records and, thus, should not be admitted.[136]

B. The Dead Chains

Many assume that an existing blockchain has enough members to properly maintain the chain. For example, Bitcoin XT, a fork of Bitcoin, was initially successful with "between 30,000 to over 40,000 nodes running its software in the late summer of 2015."[137] But within just a few months, users lost interest in the project and it was essentially abandoned (Bitcoin XT is now no longer available).[138] Similarly, in 2016, Bitcoin Classic had a spike in initial interest, rising from 27,000 nodes to nearly 200,000 nodes over a period of several months.[139] Although that blockchain still exists, most of the community has moved on to other blockchains.[140] A lack of proper management of the blockchain (through a lack of nodes) makes the blockchain vulnerable to tampering or technical errors.

For blockchains with fewer nodes managing the chain and for blockchains following a Proof of Work consensus algorithm, 51 percent attacks are an inherent risk.[141] This is because, particularly in a Proof of Work blockchain, the creator of the subsequent block in the chain is selected through a majority vote, where votes are counted by hash power.[142] In cases where only a few

135. FED. R. EVID. 801.
136. *See generally* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993).
137. Peters, *supra* note 38.
138. *Id.*
139. *Id.*
140. *Id.*
141. Rob Behnke, *5 Common Types of Blockchain Hacks*, HALBORN (Apr. 30, 2021), https://www.halborn.com/blog/post/5-common-types-of-blockchain-hacks [https://perma.cc/FB7P-LMQV].
142. *Id.*

actors control more than 50 percent of the votes, those actors "can build a version of the blockchain faster than the rest of the network put together."[143] Once they have complete control over the chain's contents, they can tamper with the records on the chain.[144] The smaller the blockchain, the easier it is for a 51 percent attack to occur "because the cost of [amassing] a majority of the hashpower is so low."[145]

Consider the following hypothetical. A company, FTX2, creates a private blockchain. For years, only a few members have managed the heavily forked blockchain. Now, the government is accusing the company of committing wire fraud, money laundering, and conspiracy. Consequently, records on the nondominant side of the fork are necessary to indict several managers because the prosecution must state with particularity which transactions comprised the fraud.[146]

The defense can argue, however, that because only a few nodes have managed the chain over time, the chain was vulnerable to attacks. For instance, a 51 percent attack (which cannot be detected after the fact) could have altered the records on the chain, allowing the accused bad actors to either conceal or obscure their illicit activities.[147]

With too few nodes to reliably manage the blockchain ledger, the blockchain would itself be less reliable. If a litigation is particularly lengthy and requires information from an older, forked, and poorly maintained chain, then a court may reject that evidence because the blockchain does not bear the indicia of reliability required for a jury to hear it.[148]

Ultimately, these hypothetical scenarios present only two of the many issues that blockchain presents to evidence admissibility specifically because they show that forked blockchains are not always reliable. As more blockchains are developed, and inevitably forked for maintenance, there are bound to be chains that lack the reliability and authentication requirements necessary to be admitted at trial.[149] In such cases, courts must decide whether that evidence is unreliable so as to be excluded at trial.

CONCLUSION

Evidence on the blockchain is often assumed to be reliable. Yet, as blockchain technology evolves, communities will inevitably disagree as to their governance and maintenance—particularly, whether to prioritize security and reliability in exchange for scalability. Thus, forking will continue to be a normal part of blockchain operations as communities splinter and diverge. With every fork that results in inadequately managed dead

143. *Id.*
144. *See id.*
145. *Id.*
146. FED. R. CIV. P. 9(b).
147. *51% Attacks*, *supra* note 55.
148. *See supra* note 68 and accompanying text (noting that the Federal Rules of Evidence require evidence to be relevant, authentic, and reliable).
149. *Id.*

chains or every fork that sacrifices decentralization for scalability, the vulnerability to error or tampering means that some blockchains will become increasingly unreliable as evidence in litigation.

Without further validation, a blockchain should not be considered purely immutable evidence. Litigators should closely examine the quality of evidence stored on blockchains so that they can challenge its reliability, especially where the blockchain has been subject to the inherent security risks of forking. Ultimately, litigators who fail to challenge disputed data on forked blockchains will miss opportunities to inform courts and juries about how a complex technology may be abused or otherwise unreliable.