BLOCKCHAIN AS EVIDENCE: UNASSAILABLE RECORD KEEPER OR TRANSIENT TECHNOLOGY?

Scott Meyer

Blockchain, the decentralized record-keeping system, currently exists in a twilight state. Rising to public prominence, or perhaps infamy, in the late 2000's with the advent of Bitcoin,[1] the technology was trailed by a sense of undefined suspicion. From the anonymous nature of its transactions, to the doctorate in computer science it seemingly required to understand its processes, the public sentiment towards blockchain seemed to follow "where there is smoke there is fire," or, perhaps more accurately, where there is anonymity there is ill repute.[2] That being said, its obfuscated nature has not deterred pundits, tech giants, and everyone in between from declaring it everything short of the second coming.[3] As with e-commerce, software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and others before it, blockchain has become one of the next great technology windmills with which companies seem determined to tilt. Interestingly, what separates this technology from past paradigm shifts is that courtrooms are also taking notice of it.

WHAT IS BLOCKCHAIN?

The reason for this general widespread interest likely stems from what blockchain represents. At a very basic level, a blockchain is a decentralized database that stores transactions. Take, for example, a database for a bank, which captures all of that bank's transactions. A blockchain does just that, except it stores the data in more than one place, instead of one centralized database (see Figure 1 below).

---

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (Oct. 2008), https://bitcoin.org/bitcoin.pdf; *The great chain of being sure about things*, ECONOMIST (Oct. 31, 2015), https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

[2] Sean Foley, Jonathan R. Karlsen, & Tālis J. Putniņš, *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?*, OXFORD BUS. L. BLOG (Feb. 19, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/sex-drugs-and-bitcoin-how-much-illegal-activity-financed-through.

[3] *See, e.g.*, Kage Spatz, *Eight Ways Blockchain Will Impact the World Beyond Cryptocurrency*, FORBES (Mar. 9, 2018, 9:00 AM), https://www.forbes.com/sites/theyec/2018/03/09/eight-ways-blockchain-will-impact-the-world-beyond-cryptocurrency/#106b79d41883; Don Tapscott, Alex Tapscott, & Rik Kirkland, *How blockchains could change the world*, MCKINSEY & CO. HIGH TECH. (May 2016), https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world.

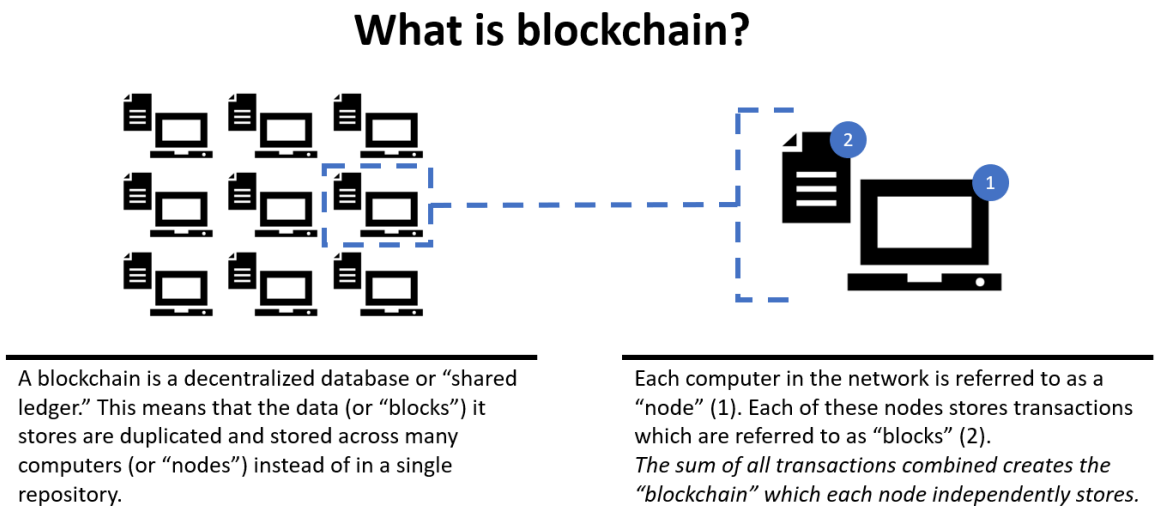

Figure 1

The central tenets of blockchain revolve around the redundancy and transparency of its data. By having each node store the entirety of all transactions (in "blocks"), double spending[4] is quickly identified and not validated. This is accomplished by comparing the transactions of all other computers (or "nodes") within the blockchain's network (see Figure 2).

[4] Double spending is the risk of spending a digital currency (such as cryptocurrencies) more than once. In the physical world, you cannot spend the same dollar twice because the dollar would, presumably, be handed over in the first transaction. Digital currency is also supposed to be "handed over," but, since it is a file stored on a computer(s), it can theoretically be duplicated or falsified much more easily than minting counterfeit bills would be. Double spending can be accidental (see Forks in the Blockchain below) or malicious (i.e., a 51% attack. *See infra* text accompanying note 10.).

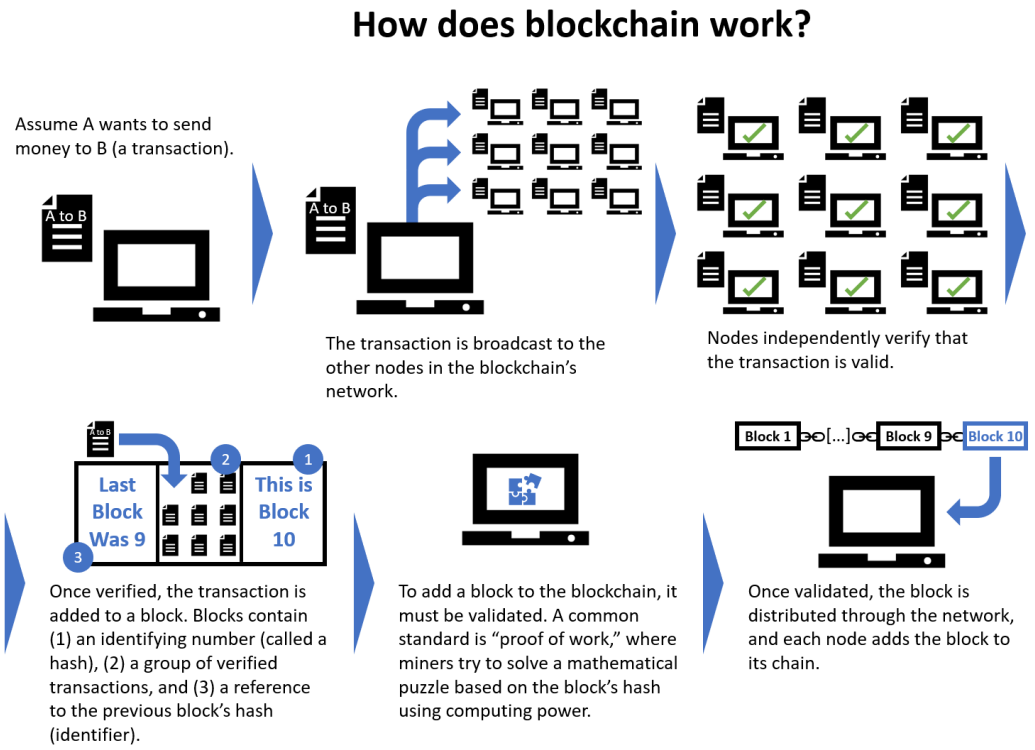

Figure 2

A small nuance in blockchain compared to traditional ledger systems is the fact that the ratio of transactions to "blocks" is not inherently one to one. For example, multiple transactions are grouped or "batched" to create a single block. The process is identical if blocks contain a single transaction or batches of them, except that batched blocks are not added to the blockchain until the block is "completed."

In most cases, each node in the blockchain stores the entirety of the transaction history. The point of this is to emphasize redundancy across the network and to avoid "stale blocks"[5] that are determined to be out of date. That being said, individual nodes, theoretically, do not need to store any part of the blockchain at all. The blocks exist to validate the history of the transactions, and so as long as some number more than zero of the nodes contains the full

[5] *See Stale Block*, BITCOIN, https://bitcoin.org/en/glossary/stale-block (A block that is successfully mined, but not part of the "correct" blockchain); *see also infra* Figure 3 (The abandoned blocks in the "B" fork would be considered stale).

blockchain (to validate transactions), the other nodes could simply delete their history.

This is not ideal from a blockchain model, however, as its strengths are redundancy and performance. If you only have a single node that contains the entirety of the transaction history, you are at the mercy of that single node—a risky proposition in what is assumed to be a purely anonymous marketplace (i.e., if that single node was compromised there would be no other nodes to contradict fake or bad transactions).

To further clarify, imagine a ledger that had three entries. Ideally, each node stores all three transactions, and "observes" that the other nodes are also storing the transactions correctly. Alternatively, one node could store all three transactions, and the other two nodes (to reduce storage cost) only save the most recent transaction. In this example, the two nodes are at the mercy of the sole node with the master ledger. Note, the three transactions are not stored across the three nodes, with the blockchain technology then "recombining" them to create the full ledger. Each node is independent of all the other nodes.

MINING THE BLOCKCHAIN

The strength of a blockchain is based in large part on the size of its network. To analogize, ten people independently reviewing a ledger for mistakes is better than five people, which is better than one person. So, who is verifying the data in a blockchain, and why are they bothering?

The people who store the blockchain are referred to as "miners"—they are "mining for blocks." These miners are essential to the blockchain because they provide the computing power that the blockchain uses to validate its blocks. Miners use their computers' computing power to validate each block, which, once validated, is then added to the blockchain. As a note, the number of miners and the number of computers does not need to be one to one. For instance, a single person could purchase many computers and set them all to "mine" blocks.

Blockchain miners are not acting altruistically in validating blocks in a blockchain. When a blockchain is used for a cryptocurrency (i.e., Bitcoin), miners receive some amount of the currency for validating the block (usually a fraction based on the size of the blockchain). The "coins" the miner receives are created from nothing. It is not a transaction fee docked from the transaction data stored in the blocks. This incentivizes the miners to validate as many blocks as possible to increase the amount they receive, thus sustaining the network. However, many cryptocurrencies have a

finite supply, which means once that number of coins/currency/etc. is mined, no more will be created.[6] Once that occurs, miners will likely switch to transaction fees to justify their computing expenses.

Imagine Pierre wants to become a Bitcoin miner (or any other cryptocurrency). He would buy a computer, and then download the necessary software onto the machine.[7] He would then run the software, which would begin "mining" for blocks by trying to validate them. If he successfully mined a block, he would receive a fraction of a Bitcoin into his "wallet" (a record associating accrued Bitcoins to a certain account number).

Cryptocurrency wallets store information regarding what the user has acquired via mining or transactions (since cryptocurrency does not tangibly exist, the information required revolves around transactions associated with that wallet). Even though a wallet is required, blockchain is still anonymous because the wallet only requires a public key, and a private key (no name, social security number, address, etc.). The "public key" lets blockchain and other users know where to send Bitcoin, while the "private key" is known only to the wallet's owner, and is used to send or spend Bitcoin they own.

The incentive of receiving cryptocurrency is the main reason people become miners. Thus, in applying blockchain to non-cryptocurrency applications, it will be important to consider how to incentivize miners.

FORKS IN THE BLOCKCHAIN

So, what happens if blockchain ledgers do not agree? To understand this, it is important to consider why this technology is called "blockchain." As stated above, groups or "batches" of valid transactions are combined to make a block. Once a block is completed, it is added to the end of the existing chain. Each block contains information from the block that was created before it, "linking" the two blocks. This is where the term "blockchain" originates. A "fork" in the blockchain occurs when different nodes do not agree on what the correct chain of blocks is.

---

[6] *See, e.g., How are bitcoins created?*, BITCOIN, https://bitcoin.org/en/faq#how-are-bitcoins-created (Bitcoin issuance will stop once 21 million are mined). *But see, e.g.*, Neer Varshney, *Ethereum's supply has crossed 100M, here's what that means*, The Next Web (Jun. 11, 2018), https://thenextweb.com/hardfork/2018/06/11/ethereums-total-supply/ ("Unlike Bitcoin which has its supply capped at 21 million, Ethereum has opted not to set an upper limit on its total coin supply.")

[7] *See, e.g.*, *Running a Full Node*, BITCOIN, https://bitcoin.org/en/full-node#what-is-a-full-node.

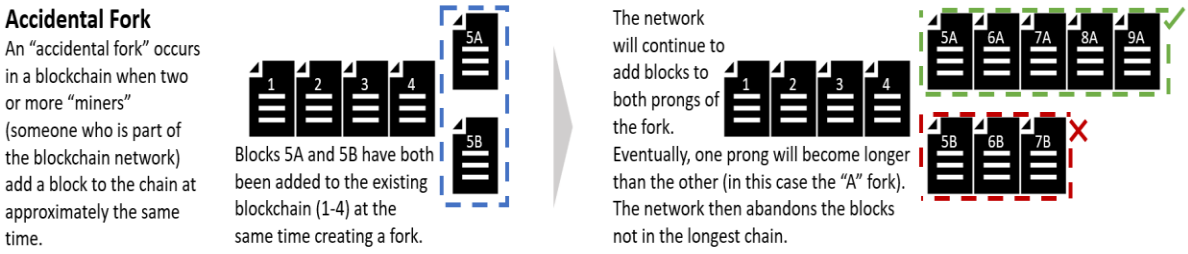

Figure 3

Forks can be accidental or intentional. Figure 3 shows an accidental fork. An accidental fork occurs when two (or more) nodes add a block to the blockchain at the same time. This type of fork is naturally corrected for as the blockchain continues to grow (adds more blocks). Nodes will continue to add blocks to either fork (5A or 5B in Figure 3) until the network can determine which fork is "correct." This is determined by which fork is longer (has more blocks added to it) because it means that the majority of the network is treating that fork as the "correct" one. In the example above, 5A is the "longer" chain, and therefore continues on, while 5B is abandoned. Since only the "correct" blockchain fork continues to exist, the problem of double spend is still solved because all other forks (and their transactions) are abandoned. Because miners are incentivized to mine only valid blocks, they want to avoid adding to forks that will be abandoned (i.e., 5B). This encourages miners to keep their ledgers as accurate as possible, which in turn strengthens the network as a whole.

In addition to accidental forks, there are intentional forks. Intentional forks are caused by updates to the rules that govern how the blockchain is made. There are two basic types of intentional forks: hard and soft.

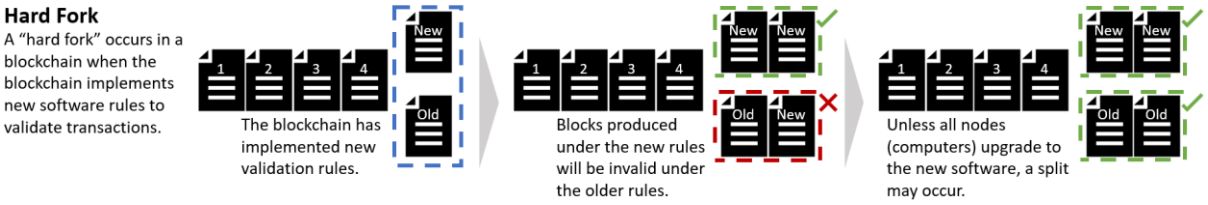

Figure 4

Figure 4 shows a "hard fork." This occurs when the blockchain implements new rules to validate transactions. It is called a hard fork because blocks created under the new rules are invalid under the old rules and vice-versa. In short, the old validation rules

and new validation rules cannot be reconciled. Nodes running the old validation rules will continue to validate only old blocks, and nodes running the new validation rules will validate only new blocks. Unless all users agree to either implement or not implement the rule, a permanent "hard fork" will be created.

Figure 5

Figure 5 shows a "soft fork." This is very similar to a hard fork, except the new software rules are also recognized as valid by the old software rules. So, blocks validated by the new rules can be added to a chain that uses either the new validation rules, or the old validation rules. However, a split may still occur if the blocks created under the new validation rules do not recognize blocks created under the old validation rules.

Since blockchain is decentralized, each individual node owner gets to decide whether to follow a software update. Unless there is consensus among the blockchain's node owners, meaning everyone agrees to accept or reject a software upgrade, a fork (either hard or soft) can become a permanent split in the blockchain with nodes using different versions of software.

To analogize, imagine a neighborhood association that has an ordinance on what color owners can paint their home. Initially, all owners must paint their homes blue. Now imagine the association decides on a new rule that all houses should be painted green. If all the owners agree with the new policy and paint their homes, the entire neighborhood will now be green (a single updated blockchain record). If no owners agree to paint their home the entire neighborhood will remain blue (a single non-updated blockchain record). If, however, some owners paint their homes, and some do not, there will be two types of homes, some blue, and some green (a forked blockchain that will remain forked unless the neighbors can all agree on a single color again).

TYPES OF BLOCKCHAIN NETWORKS

One final consideration of blockchain as an emerging technology is how it is being used. Currently, there are three basic derivations of blockchain: permissionless blockchains, federated blockchains, and private or permissioned blockchains. See the table below:

	Permissionless Blockchain	Federated Blockchain	Private Blockchain	Private Blockchain for Public Records
Example	Cryptocurrencies, such as Bitcoin, where anyone with the necessary technical equipment can join network.	A consortium of, for instance, banks working together to validate transactions.	All access is centralized in a single organization (such as a company). This differs from a federated model because there is only a single organization in control of the blockchain.	Functionally identical to a private blockchain, except maintained for public records purposes, such as a property register.
Incentive to join network?	Miners receive cryptocurrency in exchange for providing computing power to the network.	Individual users likely not individually incentivized since only people with permission have access (there is no reason to incentivize growing the network).	No reason to incentivize users since there is only a single organization managing the network.	Allows users to view public records while a central authority maintains them.
Access to Blockchain	Open to anyone	Must have permission to access	Must have permission to access	Must have permission to access
Identity of Users	Anonymous / pseudonymous	Identities of users are known and trusted	Identities of users are known and trusted	Variable depending on setup, viewing the data could be anonymous, while users maintaining the data would be known and trusted
Security	Consensus based	Pre-approved users only	Pre-approved users only	Variable based on setup
Key Differentiator	• No trust between users required • Slower transaction approval • Low cost (each user bears their own cost)	• Identified, trusted users • Faster transaction approval	• Identified, trusted users • Faster transaction approval • Similar to a centralized database	• Identified, trusted administrators • Public viewing access • Similar to a centralized database

The main differences between these derivations include anonymity, access, and incentives. When initially created, public blockchain allowed anonymous users a method of interacting through a shared ledger. The federated and private versions of the blockchain take the basic premise of blockchain and make it much more limited in access. This allows for a similar redundancy in validating transactions, but with faster transacting time due to the limited number of users. However, it also requires users to be known and given permission to access these types of blockchain networks. Some would argue these permissioned blockchains are simply uniquely set up databases and not actually blockchain networks, since the essence of blockchain technology—anonymity and free access—are not present.

LIMITATIONS OF BLOCKCHAIN

While the theory behind blockchain is sound, it is not infallible. As courts begin to interact further with blockchain, either through adoption or through general litigation regarding blockchain, it will be increasingly important to be aware of more than simply archetypal-like truths about blockchains as a whole.

One such hyped claim concerns the safety and security of storing information on blockchain. Many proponents of blockchain technology have claimed that the technology is immutable, virtually unchangeable, and, therefore, highly secure. However, it is becoming increasingly clear that blockchain technology is still vulnerable to security risks.[8]

Take for example a blockchain network of only four people. If three of the four decided to alter the transactional history of the blockchain, they would be able to succeed through sheer majority. To understand why this would work, refer back to Figure 3, which describes an "accidental fork." The blockchain decides which fork is correct based on majority decision—whichever fork has the most blocks added to it. Blockchain's reliance on redundancy across

[8] *See, e.g.*, Gina Clarke, *After Ethereum Classic Suffers 51% Hack, Experts Consider – Will Bitcoin Be Next?*, FORBES (Jan. 9, 2019, 2:04 AM), https://www.forbes.com/sites/ginaclarke/2019/01/09/after-ethereum-classic-suffers-51-hack-experts-consider-will-bitcoin-be-next/#3ccf603ba56b; Jordan French, *Ethereum Classic's '51% Attack,' $1 Million Loss, Raise Concerns About Security*, THESTREET (Jan. 14, 2019, 4:36 PM), https://www.thestreet.com/investing/bitcoin/attack-against-ethereum-classic-14832327; Alyssa Hertig, *Blockchain's Once-Feared 51% Attack is Now Becoming Regular*, COINDESK (June 8, 2018, 10:30 AM), https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular.

multiple nodes, at a basic level, means that the majority is always "right"—even if that majority is purposefully validating transactions that are actually wrong. While this particular hypothetical is, purposely, far-fetched,[9] it does represent a legitimate concern: with enough actors working in concert, a blockchain can be misled. This type of tampering is referred to as a "51% attack."[10] Blockchain networks that are relatively small are particularly susceptible to this kind of attack because relatively little computing power is necessary to control 51% (or more). However, recent hacks reveal that even large blockchain networks, like Ethereum Classic, are susceptible to 51% attacks.[11] This consideration becomes highly important when determining the validity of a blockchain's transaction evidence. Courts, and legal professionals in general, must not simply take the word of technologists that this newest creation is all but infallible.

Another potential problem, though on the opposite end of the spectrum, is blockchain's current immutability. While many of blockchain's current applications, such as cryptocurrencies, rely upon the unchanging nature of its records to establish legitimacy, future instances may require a more flexible approach. Take the banking industry, which seems to be championing this technology the fastest.[12] Imagine a bank sets up a private blockchain network completely under its control to ensure all its ledgers are in lockstep with each other and to reduce the time required to finalize transactions. As often happens with large corporations, a transaction is then broadcast (shared) to the blockchain and verified as being correct. Then, after it has been added to the ledger of all those nodes, something changes and the transaction needs to be scratched out, reversed, or cancelled because it is no longer valid—such as an accepted deal that has been subsequently rescinded or reneged, or a delinquent account has suddenly become solvent. At a more personal level, imagine someone has their Bitcoin wallet compromised (their private key is stolen) and the bad actor sends all the victim's Bitcoin to the bad actor's account.[13] This is technically

---

[9] It is safe to say that most blockchain networks consist of far more than just four users. *See* Luke Fortney, *Blockchain Explained*, INVESTOPEDIA (Jun. 25, 2019), https://www.investopedia.com/terms/b/blockchain.asp#how-blockchain-works ("These networks often consist of thousands (or in the case of Bitcoin, about 5 million) computers spread across the globe").

[10] *See, e.g.*, Jake Frankenfield, *51% Attack*, INVESTOPEDIA (May 6, 2019), https://www.investopedia.com/terms/1/51-attack.asp; *51% Attack, Majority Hash Rate Attack*, BITCOIN, https://bitcoin.org/en/glossary/51-percent-attack.

[11] *See, e.g.*, Clarke, *supra* note 8; French, *supra* note 8.

[12] Jemima Kelly, *Banks adopting blockchain 'dramatically faster' than expected: IBM*, REUTERS TECH. NEWS (Sept. 28, 2016, 11:50 AM), https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D.

[13] Adrianne Jeffries, *How to steal Bitcoin in three easy steps*, VERGE (Dec. 19, 2013, 1:10 PM), https://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps; *see e.g.*, Nathaniel Popper, *A Hacking of More Than*

a valid transaction; from the blockchain's perspective, Bitcoin has legitimately transferred from one party to another. Unless the thief decides to send the Bitcoin back (unlikely) the only way to be reimbursed would be to update the entire blockchain to make that transaction invalid.

The same reasons that make blockchain so hard to compromise also make it equally hard to remedy if a legitimate error is discovered. One potential solution to this is updating the entire blockchain; however, this can result in a fork in the chain if not all users agree and accept the update.

Furthering the hypothetical, imagine two businesses litigating in court over a deal between them: one points to a blockchain to assert their case that a transaction was valid, while the other opines that there was a mistake and, either lacking skill or desire, they failed to correct the blockchain ledger and instead have been keeping a traditional (non-blockchain) ledger of their own. The court will be forced to decide whose ledger takes priority or should receive deference. As industries decide to either embrace or discard blockchain technology, courts will have to determine if one form of record should overrule another.

A more concrete problem facing blockchain today is its massive energy requirement. As cryptocurrency becomes more prevalent, more users flock to its network. These users run computationally intensive processes to "mine" cryptocurrencies such as Bitcoin, which require massive amounts of energy. According to the International Energy Agency, the entire Bitcoin network alone now consumes more energy than over 100 countries.[14] That energy usage leaves an immense carbon footprint. The Nature Climate Change estimates that Bitcoin emissions alone could push global warming above 2 degrees Celsius in less than three decades.[15] While this side effect is not directly related to courts accepting blockchain technology, it is a tangential concern to be aware of, especially in weighing what impacts incentivizing blockchain may have.

$50 Million Dashes Hopes in the World of Virtual Currency, N.Y. TIMES (Jun. 17, 2016), https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html (hacker siphoned more than $50 million dollars of Ethereum, leading to a hard fork).

[14] BITCOIN ENERGY CONSUMPTION INDEX, DIGICONOMIST, https://digiconomist.net/bitcoin-energy-consumption (last visited Jan. 28, 2019).

[15] Camilo Mora, et al., *Bitcoin emissions alone could push global warming above 2°C*, NATURE (Oct. 29, 2018), https://www.nature.com/articles/s41558-018-0321-8.

A final consideration, in this non-exhaustive list, is that of longevity, or lack thereof. A key aspect of blockchain is that each individual node hosts the entirety of the decentralized ledger, and can compare it to any other node's ledger at (almost) any time. This means that each time a transaction is captured, and a block is added, the entire blockchain on each node grows. From a purely practical standpoint, that means that storage requirements have to become a consideration on a long enough timeline. While current computing power has largely kept this consideration off the table, it is also worth noting that relatively few enterprises have adopted blockchain technology in anything more than an experimental capacity.[16]

Imagine an extreme example: the NASDAQ running on blockchain. It averages approximately 13 million trades per day.[17] Compare that with Bitcoin which averages approximately 350 thousand trades per day[18]—a difference in trade volume of nearly 4,000 percent. A blockchain capturing that data would quickly become too large to store practically. In that case, is it allowed to restart? Do you simply break the blockchain up? How do you handle the size? Should these considerations impact the blockchain's legitimacy when presented in court? Additionally, since the ledgers of each node in the blockchain are supposed to match, there is the further question of whether to review a single instance of a blockchain, or every ledger stored by every node within the network.

CONCLUSION

In the end, blockchain represents one more shade of gray on the palette with which only the law seems to paint. This does not mean that blockchain does not belong in the courtroom, but simply that it must be understood. Courts must take steps to comprehend not only what blockchain represents, but also what it does not represent. It is not an infallible tool, but neither is it rife with fraud or criminal intent. By taking steps to understand how blockchain works, and where its limitations exist, courts will be that much more prepared to make rational, forward-facing decisions about implementing this new technology.

---

[16] *Hype Killer – Only 1% of Companies are Using Blockchain, Gartner Reports*, ARTIFICIAL LAW. (May 4, 2018), https://www.artificiallawyer.com/2018/05/04/hype-killer-only-1-of-companies-are-using-blockchain-gartner-reports/.

[17] NASDAQ DAILY MARKET SUMMARY, http://www.nasdaqtrader.com/Trader.aspx?id=DailyMarketSummary (last visited Oct. 10, 2019).

[18] *See* BLOCKCHAIN CHARTS, BLOCKCHAIN, https://www.blockchain.com/en/charts (last visited Oct. 10, 2019).