UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 20 | Issue 4 Article 2

4-1-2019

The Building Blocks of Blockchain

Deborah Ginsberg

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 20, ISSUE 4: APRIL 2019

THE BUILDING BLOCKS OF THE BLOCKCHAIN

Deborah Ginsberg*

Blockchain. The term is ubiquitous—it's going to protect everyone's data, provide the backbone of every supply chain, make every contract smart, and so much more. But what is blockchain, actually? And can it really do all of this? (No.)

This article is for those who want to learn the basics about this technology. I will describe the essential fundamentals of Bitcoin, other cryptocurrencies, and blockchain. I will explore the technology behind blockchain, including an explanation of what "mining" is and how it helps users trust information on a blockchain. I will also explain some of the ways that blockchain is changing the law and legal practice—and why lawyers and law faculty should pay attention to these developments.

I. INTRODUCTION

As someone who likes to live on the bleeding edge of technology, I would love to say I knew all about Bitcoin when it was first launched. However, I was completely unaware of "Bitcoin: A Peer-to-Peer Electronic Cash System," by the fictional Satoshi

* Deborah Ginsberg is the Educational Technology Librarian at the Chicago-Kent College of Law Library (Illinois Institute of Technology). MLS, 2001, Dominican University; JD, 1995, University of Illinois, Champaign-Urbana. I would like to thank Jean Wenger, Director, Chicago-Kent College of Law Library for her editorial suggestions.

Nakamoto[1]—the first white paper announcing this new kind of currency— as well as Bitcoin's launch on January 12, 2009 (happy 10th birthday).[2] And I did not notice the arrival of new cryptocurrencies such as Litecoin and Swiftcoin in 2011.[3]

Around 2013 and 2014, cryptocurrencies began to interest the mainstream media and people started asking me about it. Were these currencies real money? Sure. Could they be spent for goods and services outside the dark web? At the time, not really. Even 5 years after launch, cryptocurrencies were still considered fairly novel. I did not pay much attention to them.

In July and November 2016, Chicago-Kent hosted two conferences focused on the latest developments in legal technology.[4] These conferences were some of the most informative and transformative I have ever attended. A few speakers talked about cryptocurrencies, but others focused on the powerful database technology behind these currencies—the blockchain. Sessions covered everything from the power of blockchain database structures to new legal concepts such as smart contracts.

Not only did I come to realize that a blockchain is, "in fact, a chain of blocks! Cool," (my conference notes were very helpful), but I discovered that this method of organizing data was likely to transform finance, business, and the law. That said, beyond "a

---

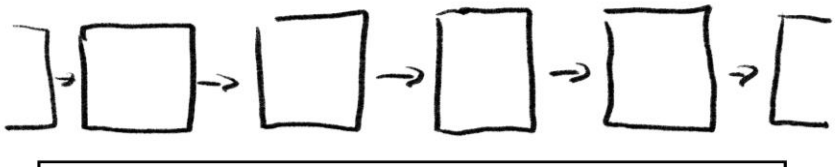
[1] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, https://bitcoin.org/bitcoin.pdf [https://perma.cc/DDB9-JXK7] (introducing Bitcoin as an electronic payment system without reliance on a financial institution).

[2] Rosemary Bigmore, *A Decade of Cryptocurrency: From Bitcoin to Mining Chips*, TELEGRAPH (May 25, 2018, 3:30 PM), https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/ [https://perma.cc/UZ7Z-P5YQ].

[3] *Id.*

[4] Janders Dean & Chicago-Kent Legal Horizons Conference, Chicago-Kent Coll. of Law Ill. Inst. of Tech. (July 14, 2016), http://calendar.kentlaw.iit.edu/EventList.aspx?fromdate=7/1/2016&todate=7/30/2016&display=&type=public&eventidn=4586&view=EventDetails&information_id=7316 (last visited Jan. 23, 2019); Fin (Legal) Tech Conference, Chicago-Kent Coll. of L. Ill. Inst. of Tech. (Nov. 4, 2016), https://calendar.kentlaw.iit.edu/EventList.aspx?fromdate=11/4/2016&todate=11/4/2016&display=Day&type=public&eventidn=4594&view=EventDetails&information_id=7332.

chain of blocks," I was unsure how this technology actually worked. It seemed so simple at first, but once I started to study it, the level of complexity grew. In this article, I will describe the fundamentals of cryptocurrencies, Bitcoin, and blockchain. I will explore the technology behind blockchain, including how mining helps users trust information on a blockchain. I will also explain why lawyers and law faculty should pay attention to developments in this technology.



Simple visualization of a blockchain database: it's just a bunch of blocks of information

II. BITCOIN AND BLOCKCHAIN: THE FOUNDATIONS

When learning about blockchain, it helps to discuss its foundations. For the blockchain, that foundation is Bitcoin. Bitcoin was the first technology to use a database based on a blockchain structure.[5] Indeed, the database that runs Bitcoin is called the Blockchain (capitalized; use lowercase when referring to other blockchains).[6]

Over the last decade, you have likely heard that Bitcoin is a new kind of currency. The transactions associated with it exist entirely online.

But other currencies can be exchanged online. So, what is different about Bitcoin? Unlike other online currency transactions, Bitcoin exchanges are one-to-one. If I send U.S. dollars to someone online, I will need to use some kind of third-party service, such as a

---

[5] *What Is Blockchain Technology? A Step-by-Step Guide for Beginners*, BLOCKGEEKS (Mar. 1, 2019), https://blockgeeks.com/guides/what-is-blockchain-technology/.

[6] Anthony Wing Kosner, *Tech 2015: Block Chain Will Break Free from Bitcoin to Power Distributed Apps*, FORBES (Dec. 31, 2014, 1:00 PM), https://www.forbes.com/sites/anthonykosner/2014/12/31/tech-2015-block-chain-will-break-free-from-bitcoin-to-power-distributed-apps/.

bank or PayPal.[7] A Bitcoin user, on the other hand, can send transfers directly to any other Bitcoin user. The transfers are direct and require no "middleman."[8] This means that transactions are fairly private (but not anonymous) and do not require expensive transaction fees.[9]

Buying and selling goods and services with this currency requires an online Bitcoin "wallet."[10] A wallet is an online space specifically dedicated to Bitcoin. Users can obtain wallets from sites like BTC.com or Coinspace[11] or from online exchanges such as Coinbase.[12]

Bitcoin wallets are identified using special alphanumeric addresses.[13] Each wallet has a public address, which tells other Bitcoin users where to send Bitcoin transactions.[14] The wallet also has private address, which allows the wallet owner to authorize transactions.[15] For example, if Beto wants to send Bitcoin to

---

[7] *See* Justin Pritchard, *How to Send Money Online*, BALANCE (Jan. 29, 2019), https://www.thebalance.com/send-money-online-315075.

[8] *FAQ - Bitcoin*, BITCOIN, https://bitcoin.org/en/faq (last visited Jan 31, 2019). That said, many users will use an exchange like Coinbase.com, which adds a "middleman" to the exchange. *See* COINBASE, https://www.coinbase.com/ (last visited Jan. 31, 2019).

[9] *FAQ – Bitcoin*, *supra* note 8. Many users will add fees on their own. *See How Did These Zero-Transaction Fee Transactions Make It into the Bitcoin Network?*, STACK EXCHANGE, https://bitcoin.stackexchange.com/questions/69030/how-did-these-zero-transaction-fee-transactions-make-it-into-the-bitcoin-network (last visited Feb. 4, 2019) [hereinafter *Zero-Transaction Fee Transactions*].

[10] *What Is Bitcoin? The Most Comprehensive Guide Ever!*, BLOCKGEEKS, https://blockgeeks.com/guides/what-is-bitcoin/ (last visited Nov. 12, 2018); Tal Yellin, Dominic Aratari & Jose Pagliery, *What Is Bitcoin?*, CNN: MONEY (Aug. 8, 2018), https://money.cnn.com/infographic/technology/what-is-bitcoin/.

[11] The Bitcoin.org site lists many sites that offer wallets. *See Choose your Bitcoin wallet*, BITCOIN, https://bitcoin.org/en/choose-your-wallet (last visited Jan. 31, 2019). Note that Bitcoin.org is an informational site; there is no central site for managing Bitcoin. Also, I am not recommending any of these as places to store Bitcoin – they are listed as examples only.

[12] COINBASE, *supra* note 8. I use Coinbase to manage the $20 of cryptocurrency I bought in June 2017.

[13] Yellin, Aratari & Pagliery, *supra* note 10.

[14] *Id.*

[15] *Id.*

Elizabeth, Beto will use his private Bitcoin wallet address to send the currency to Elizabeth's public address.[16]

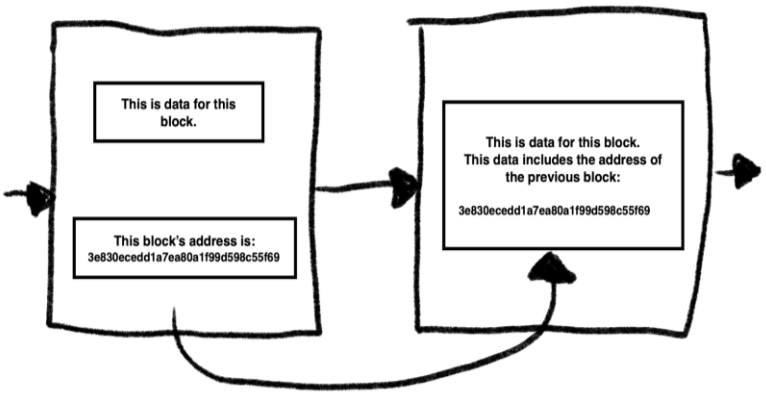
So far, this currency works much like many others. However, Bitcoin adds features that provide extra security and authenticity. Each transaction is encrypted, meaning that the details of who is sending and receiving the currency remain private. The senders and receivers use special encryption keys to protect their identities.[17] This encryption is why the currency is known as a "crypto" currency. Other cryptocurrencies use similar transaction structures.

These transactions are then logged into the Blockchain database. The database is structured in a way that is both simple and secure. Bitcoin transfers are recorded in blocks of data. Each block is then added to a chain of other blocks. Blocks are linked using a special identification known as a "hash" (a long string of numbers and

[16] These function similarly to the public keys and private keys used for standard encryption functions. *Encryption Made Simple for Lawyers*, GPO SOLO MAG. (Apr. 5, 2019), https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers/. Bitcoin wallets in fact use public and private keys, but these are mathematically related to the public and private wallets, not synonyms for them. Prypto, *Bitcoin Public and Private Keys*, DUMMIES, https://www.dummies.com/software/other-software/bitcoin-public-private-keys/ (last visited Mar. 8, 2019).

[17] *Id.*

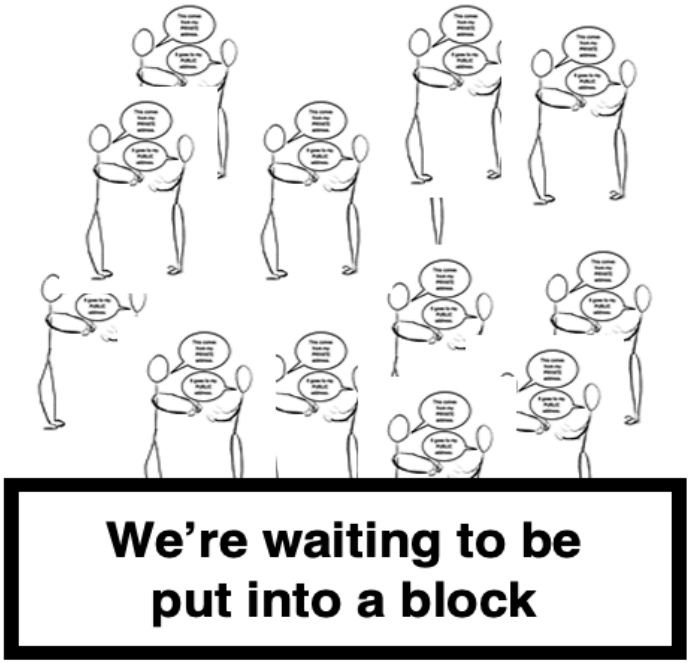
letters).[18] Each block's data includes the hash (referred to in the figures below as the "address") of the previous block in the chain. The structure looks something like this:



Let's look at this in more detail. Transactions take place initially outside of the Blockchain database. In the example above, Beto sells Elizabeth Bitcoin. When Beto exchanges Bitcoin with Elizabeth, this transaction is put into the Bitcoin network. However, this transaction does not automatically get added to the Blockchain. Instead, it is added to a group of other transactions waiting to be put into blocks.[19]

[18] Maryanne Murray, *Blockchain Explained*, REUTERS (June 15, 2018), http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html. This site is one of my favorite visual tools for understanding blockchain and Bitcoin.

[19] *FAQ - Bitcoin*, *supra* note 8.



Before a transaction can be added to the Blockchain, the Bitcoin community needs to accept it first. It does this using "miners." The job of miners is to add transactions to the chain by creating blocks of transfers in a way the Bitcoin community finds acceptable before adding those blocks to the database.[20] Acceptable transfers are those that can be verified and do not involve the Bitcoin holder trying to spend their currency more than once (this is known as "double spending").[21]

Here enters one of the most important concepts with Bitcoin and blockchains: establishing trust.[22] The community of Bitcoin users must trust that the transfers recorded in each block are acceptable. Currency transfers occur between strangers who have no reason to

[20] Yellin, Arateri & Pagliery, *supra* note 10.

[21] *FAQ - Bitcoin*, *supra* note 8.

[22] *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.

trust one another. Bitcoin mining adds a layer of security to establish that trust.

The Bitcoin Blockchain uses a concept called "proof of work" to establish this trust.[23] By doing the difficult work needed to create the blocks, the miners have shown that the transactions are trustworthy.[24] At least a majority of the community must then agree the block is acceptable (or at least not challenge it).[25] Only then will the block be added the database.[26]

At this point, the Bitcoin community adds another step to ensure security. There is not just one Blockchain database—there are over 10,000 known copies as of February 1, 2019.[27] The Blockchain community continually reviews these databases and the new blocks that are added to them. Once community members determine a new block is good, it is added to the many copies of the database.[28] These databases are observed by community members to make sure they are all the same.[29] There is not just one person or organization charged with securing the integrity of the Blockchain. The databases are, in fact, decentralized, which means that instead of only being stored on a central server or group, they are maintained and stored by members of the Blockchain community.[30]

---

[23] *FAQ - Bitcoin*, *supra* note 8.

[24] *Id*.

[25] *Bitcoin Is Not Ruled by Miners*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Bitcoin_is_not_ruled_by_miners (last updated Aug. 17, 2017).

[26] *FAQ - Bitcoin*, *supra* note 8.

[27] *Global Bitcoin Nodes Distribution*, BITNODES, https://bitnodes.earn.com/ [https://perma.cc/D4JD-R9G6] (last visited Mar. 8, 2019). There are likely additional nodes this site has not found—a decentralized system is difficult to track.

[28] *FAQ - Bitcoin*, *supra* note 8.

[29] Andreas M. Antonopoulos, *Mining and Consensus*, *in* MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES (2014), https://www.oreilly.com/ library/view/mastering-bitcoin/9781491902639/ ch08.html.

[30] This means that if 99% of a blockchain's servers were destroyed, the blockchain could be recreated out of the remaining 1%. Robert Greenfield IV, *The Failing Sustainability of Blockchain Magic*, MEDIUM (May 30, 2017), https://medium.com/@robertgreenfieldiv/the-failing-sustainability-of-blockchain-magic-4a5533db70a7.

Because the community's checks take some time to process, transactions are not instantaneous. That said, they do not take a lot of time. As of February 1, 2019, it takes about 9-10 minutes for miners to create a new block.[31] It then takes additional time for the block to be copied throughout the different Blockchains. Let's go back to the Beto and Elizabeth transaction above. Their transaction is not instantaneous. However, in most instances, in about ½ hour Beto and Elizabeth will be able to verify their transaction has been verified and accepted into the Blockchain.[32]

So how do miners create blocks that the community trusts? Miners work to generate the hashes that link each block to the next in the chain.[33] Each block a miner creates includes:

- About 1 megabyte worth of Bitcoin transactions (this ranges from less than .5 MB to 1.2 MB).[34]
- Other encrypted information, such as the citation to the newspaper article in Bitcoin's first block (this is not required).[35]
- The hash number of the previous block in the chain (this is how the blocks are connected to one another).[36]

---

[31] *Median Confirmation Time*, BLOCKCHAIN, https://www.blockchain.com/charts/median-confirmation-time [https://perma.cc/D8T4-76AM]. Note that this an average; sometimes new blocks are added in a few minutes, and sometimes it takes about ½ hour to add a block.

[32] *FAQ - Bitcoin*, *supra* note 8.

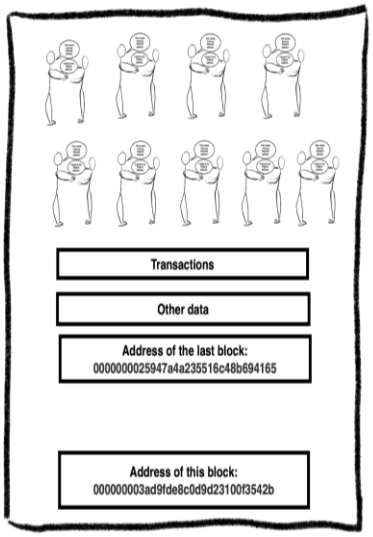
[33] Murray, *supra* note 18.

[34] *Average Block Size*, BLOCKCHAIN, https://www.blockchain.com/charts/avg-block-size [https://perma.cc/NL4M-V68Q].

[35] Jamie Redman, *Bitcoin's Quirky Genesis Block Turns Eight Years Old Today*, BITCOIN: NEWS (Jan. 3, 2017), https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/.

[36] Murray, *supra* note 18.

- A new hash that meets Bitcoin's specific acceptable criteria (one current criterion is the hash must start with 18 zeros).[37]



When miners create a block, they gather a certain number of transactions.[38] Miners then run a sophisticated computer program to find a hash number the community will accept. When they have identified an acceptable new hash, they add that hash to the block and add that block to a blockchain on the network.[39]

When other versions of the Blockchain database on the network see a new block of transactions has been added, those versions verify that the block is acceptable and then copy the block onto their own chains. This new block then "propagates" throughout the Bitcoin network[40] and the block becomes part of the community Bitcoin

[37] Damien Cosset, *Blockchain: What Is Mining?*, DEV.TO (Jan. 4, 2018), https://dev.to/damcosset/blockchain-what-is-mining-2eod.

[38] As of February 1, 2019, the average number of transactions per block was about 2000. *Average Number of Transactions Per Block*, BLOCKCHAIN, https://www.blockchain.com/charts/n-transactions-per-block [https://perma.cc/2JCM-4EES].

[39] *FAQ - Bitcoin*, *supra* note 8.

[40] *Network*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Network (last updated June 13, 2018).

Blockchain network.[41] Then, miners gather the next set of transactions, find a new acceptable hash, and create a new block. The Blockchain grows as a result of this method. As of February 1, 2019, the Blockchain had a "height" of 561,100 blocks.[42]

Sometimes, the Bitcoin community finds a version of the Blockchain database in the network that does not match others. Versions may not match if someone tried to change a previous transaction, someone added unapproved blocks, or tampered with the data in some other way.[43] The community would notice that some part of the data did not match and would drop the incorrect version of the database from the network.[44]

Can miners create an endless number of Bitcoins? No. The Bitcoin structure was created so that 21 million total coins could be mined.[45] At first, many coins were created because calculating acceptable hashes was fairly simple - a relatively powerful gaming computer could be used to create new hashes. As hashes became harder to calculate, more powerful computing technology was required.[46] For example, some miners used powerful video

---

[41] *FAQ - Bitcoin*, *supra* note 8.

[42] *Blockchain Explorer*, BLOCKCHAIN, https://www.blockchain.com/explorer [https://perma.cc/9XNH-CYBZ] (last visited Mar. 8, 2019). "Height" is the technical term for numbers of blocks in a blockchain. Each block has its own height, which is the number of blocks preceding it on the chain. The first block on the chain has a height of 0—no blocks precede it. Jake Frankenfield, *Block Height*, INVESTOPEDIA (Mar. 14, 2018), https://www.investopedia.com/terms/b/block-height.asp.

[43] If someone tried to change the data in a specific block, that change would affect the hash of the block involved, and the hash would no longer match the information stored in the subsequent block.

[44] Anders Brownworth, *Blockchain Demo - Part I*, ANDERS.COM, https://anders.com/blockchain/ (last visited Feb. 1, 2019). The video is a bit long but provides a good overview.

[45] *FAQ - Bitcoin*, *supra* note 8.

[46] *Id*. The Bitcoin system is designed to ensure that, on average, one block is created every 10 minutes. The system increases the difficulty of finding a has to create a block to maintain this average.

processors to create new hashes.[47] Today, most new blocks on the Blockchain are created by many servers working together.[48]

Why would miners go through all this trouble? When miners generate new blocks, they are rewarded with Bitcoins.[49] These rewards are how new Bitcoins are created. At first, miners received 50 Bitcoins.[50] On November 28, 2012, this award was cut to 25 Bitcoins to slow the rate of creation.[51] On July 9, 2016, the award was cut to 12.5 Bitcoins per block. Experts believe this award will be cut to 6.25 Bitcoins sometime in the spring of 2020.[52]

Additionally, while Bitcoin transactions do not require fees, many users include fees with their transactions to encourage miners to include them in their blocks.[53] Miners get to keep the transaction fees for the blocks they create.[54] Transactions without a fee may be added to the Blockchain at some point, but those transactions take longer than average, and may even be ignored because the transaction does not offer additional financial incentive beyond what the miner gets by creating a block.[55]

So has Bitcoin caught on as a viable, acceptable currency? To some extent, yes. Today, Bitcoin can be used for many day-to-day transactions. For example, Overstock.com accepts Bitcoin.[56] A city

---

[47] Tristan Greene, *A Brief History of Bitcoin Mining Hardware*, THE NEXT WEB: HARD FORK (Feb. 2, 2018), https://thenextweb.com/hardfork/2018/02/02/a-brief-history-of-bitcoin-mining-hardware/.

[48] *Blocks Mined on 01/02/2019*, BLOCKCHAIN, https://www.blockchain.com/btc/blocks/1549049279961 [https://perma.cc/MY8J-U6K8] (last visited Mar. 8, 2019). Of the over 350 blocks added to the Bitcoin Blockchain from 00:00 GMT to 19:30 GMT on February 1, 2019, only about 29 were created by "unknown" relays, possibly by individuals. The rest were created by companies and pools of miners.

[49] *Bitcoin Block Halving Schedule*, BITCOINNEWS (Aug. 27, 2018), https://bitcoinnews.com/bitcoin-block-halving-schedule/.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *FAQ - Bitcoin*, *supra* note 8.

[54] *Id.*

[55] *Zero-Transaction Fee Transactions*, *supra* note 9.

[56] *How Do I Pay with Bitcoin?*, OVERSTOCK.COM, https://help.overstock.com/help/s/article/Bitcoin [https://perma.cc/WZP9-6D94].

in Switzerland lets residents pay taxes in Bitcoin.[57] You can buy Bitcoin through ATM-like exchanges.[58]

Some dark web markets (both illegal and very private) will accept Bitcoin. That said, Bitcoin is losing traction in the dark web markets because other cryptocurrencies are more anonymous.[59] The Bitcoin database, though only showing an individual's address, is still public. Anyone can access it. Anyone can copy it.[60]

More importantly, anyone can analyze it.

Encrypting transactions goes a long way to preserving anonymity, but it is not a complete proof against hiding illegal activity. Detailed analysis can uncover enough information to enable the tracking of parties to the transaction. Criminals have been discovered this way already.[61] So, what use is a public blockchain? Several projects are exploring the possibilities.

Once Bitcoin started to gain popularity, other cryptocurrencies also joined the market.[62] Ethereum, launched in 2015, has become

---

[57] David Meyer, *This Place Lets You Pay Your Taxes In Bitcoin*, FORTUNE (Sep. 12, 2017), http://fortune.com/2017/09/12/switzerland-chiasso-bitcoin-tax-zug/.

[58] *Digital Mint Bitcoin ATM Chicago: Chicago Ave & Rush St*, DIGITALMINT, https://www.digitalmint.io/bitcoin-atm-locations/il-chicago-chicago-rush/ (last visited Feb. 1, 2019) (providing one of many ATM locations where you can used buy Bitcoin in Chicago).

[59] Annie Lowrey, *Bitcoin Is Falling Out of Favor on the Dark Web*, ATLANTIC (Mar. 1, 2018), https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/.

[60] *See, e.g.*, *Download Bitcoin Core*, BITCOIN, https://bitcoin.org/en/download (last visited Feb. 1, 2019).

[61] *See* Wilma Woo, *US DEA 'Actually Wants' Criminals to Keep Using Bitcoin*, BITCOINIST (Aug. 8, 2018), https://bitcoinist.com/dea-wants-criminals-use-bitcoin/ (noting that for this reason, illegal activity increasingly relies on more private currencies such as Monero or Zcash).

[62] *See* Bigmore, *supra* note 2. In 2017, some thought these currencies were good investments, exemplified by Bitcoin reaching a high of nearly $20,000 per coin in December 2017. *Bitcoin USD*, MARKETWATCH, http://www.marketwatch.com/investing/cryptocurrency/btcusd/charts (last visited Mar. 8, 2019). However, a good indicator there are better investments elsewhere is Bitcoin's value of $3,500 per coin in January 2019. *Bitcoin to US-Dollar Conversion*, MARKETS INSIDER, https://markets.businessinsider.com /currency-converter/btc_united-states-dollar (last visited Feb. 4, 2019).

one of Bitcoin's biggest rivals.[63] While no cryptocurrency matches Bitcoin on exchange value price, Ethereum has garnered a lot of interest because it can offer something Bitcoin cannot—more space in each block. This means that the Ethereum blockchain can be used for projects well beyond the scope of simple currency transactions.

Ethereum offers a way to use its blockchain to run online programs. The programming language used, called Solidity, can be programmed to create all kinds of specialized currency transactions.[64] Solidity programs have been used to buy and sell goods and create other smart contracts.[65]

Like Bitcoin, Ethereum uses proof-of-work to establish trust and to add new information to its blockchain.[66] This means that specialized problems must be solved to create new hashes to add to the blockchain.[67] However, Ethereum has been planning to switch to another way to prove that a block should be added to the blockchain, called "proof-of-stake."[68] When using proof-of-stake, the community votes on whether to add new information to a blockchain rather than rely on miners to generate a hash.[69] The more Ethereum a user controls, the more votes they will have in the system.[70] While proof-of-work is difficult to hack, it is not impossible.[71] Proof-of-stake provides additional protections.

---

[63] Peter Dockrill, *Bitcoin Just Hit an All-Time High, But New Rival Ethereum Is Rapidly Outpacing It*, SCIENCE ALERT (May 26, 2017), https://www.sciencealert.com/bitcoin-just-hit-an-all-time-high-but-cryptocurrency-rival-ethereum-is-rapidly-outpacing-it.

[64] Ryan Molecke, *How to Learn Solidity: The Ultimate Ethereum Coding Tutorial*, BLOCKGEEKS, https://blockgeeks.com/guides/solidity/ (last visited Mar. 8, 2019).

[65] *See* Fábio José, *Building a Smart Contract to Sell Goods*, MEDIUM: COINMONKS (Feb. 18, 2018), https://medium.com/coinmonks/build-a-smart-contract-to-sell-goods-6cf73609d25 (providing an overview on the technological basics of creating a smart contract).

[66] *Proof of Work vs Proof of Stake: Basic Mining Guide*, BLOCKGEEKS, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/ (last visited Jan. 31, 2019).

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] Gareth Jenkinson, *Ethereum Classic 51% Attack — The Reality of Proof-of-*

III. WHAT THIS MEANS FOR THE LAW

The first part of this article focused on explaining cryptocurrencies. And yet, the "currency" part of cryptocurrencies is not their most interesting aspect. Indeed, the structure that has rendered Bitcoin secure for the last 10 years is far more useful. The Blockchain database has shown that we can create data structures that are reasonably secure, practically immutable, and can withstand years of additions.

These qualities have captured the imagination of many. Can the robustness of Blockchain be emulated by other kinds of databases? In pursuit of this, many companies, governments, and other agencies have begun to explore blockchain projects of their own.[72]

For example, banks are exploring using blockchain databases to create transaction trails that are easy to audit.[73] The blockchain structure would mean the data could be easily observed, updated, and trusted. Auditors like Erich Braun (Audit Partner at KPMG LLP) predict that blockchains will "enhance auditing and create a far more efficient environment for conducting, tracking and verifying transactions."[74]

Work, COINTELEGRAPH (Jan. 10, 2019), https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work (explaining that if a user or a group of users gets a hold of 51% of a blockchain's computing power they can modify the blockchain, which recently happened to a cryptocurrency called "Ethereum Classic").

[72] *See* Forbes Technology Council, *What Does the Future of Blockchain Hold? 10 Predictions from Tech Experts*, FORBES (Sept. 6, 2018, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/09/06/what-does-the-future-of-blockchain-hold-10-predictions-from-tech-experts/#3936ba63301a (providing a list of examples).

[73] Penny Crosman, *Northern Trust Adds Auditing to Distributed Ledger*, AM. BANKER (Mar. 19, 2018, 11:27 AM), https://www.americanbanker.com/news/northern-trust-adds-auditing-to-its-distributed-ledger; *see also* Wolfie Zhao, *All 'Big Four' Auditors to Trial Blockchain Platform for Financial Reporting*, COINDESK (July 19, 2018, 9:30 AM), https://www.coindesk.com/all-big-four-auditors-trial-blockchain-platform-for-financial-reporting (providing that in the summer of 2018, the "Big Four" – Deloitte, EY, KPMG, and PwC – announced a trial with a blockchain company in Taiwan to test "auditing public companies' interim financial reports").

[74] *For Auditors, Blockchain Has Blockbuster Potential*, FORBES (Sept. 19, 2018, 10:17 AM), https://www.forbes.com/sites/insights-kpmg/2018/09/19/for-

These blockchains would not be publicly accessible like the Bitcoin Blockchain, but would be monitored by internal communities. Permission to access them would be private.[75]

Companies are experimenting with blockchain to track the production of goods from materials to factory production to transport to sales.[76] These blockchains—also private—would allow companies to track product issues quickly and accurately. Walmart—an industry leader in using blockchain for businesses—has been working with blockchains to track products like fresh produce.[77]

Governments have been exploring ways blockchain might make their services safer and more efficient. Some have started with focused projects like adding real estate titles to blockchain databases.[78] Other governments are planning to fully transition important functions to blockchain databases in the next few years.[79] The Illinois Blockchain Initiative,[80] for example, has been working on testing a number of projects. These include testing using blockchain for real estate titles in Cook County as well as using blockchain for birth certificate registries.[81]

---

auditors-blockchain-has-blockbuster-potential/.

[75] *Private Blockchain vs Public Blockchain*, MEDIUM: HACKER NOON (Mar. 4, 2018), https://hackernoon.com/private-blockchain-vs-public-blockchain-cc3b71bc95f8.

[76] Hilary George-Parkin, *How Blockchain Will Allow for Fewer Counterfeit Goods and Faster Product Recalls*, VOX (Oct. 18, 2018, 7:10 AM), https://www.vox.com/the-goods/2018/10/18/17989610/blockchain-retail-counterfeit-supply-chain-data.

[77] Geoffrey Mohan, *Walmart to Salad Growers: If You Want to Sell, You Have to Blockchain*, L.A. TIMES (Sept. 25, 2018, 7:00 AM), http://www.latimes.com/business/la-fi-walmart-lettuce-20180925-story.html.

[78] Frisco d'Anconia, *Georgia Becomes First Country to Register Property on Blockchain*, COINTELEGRAPH (Feb. 8, 2017), https://cointelegraph.com/news/georgia-becomes-first-country-to-register-property-on-blockchain.

[79] Suparna Dutt D'Cunha, *Dubai Sets Its Sights on Becoming the World's First Blockchain-Powered Government*, FORBES (Dec. 18, 2017, 1:08 AM), https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/.

[80] *The Illinois Blockchain Initiative*, MEDIUM, https://illinoisblockchain.tech/ (last visited Sep. 27, 2017).

[81] Sara Friedman, *Illinois Builds Momentum for Blockchain*, GCN (Feb. 5,

As for the law itself, blockchain promises several interesting developments. It has the potential to change the nature of firm practice and to reconstruct some of the fundamental instruments of the law, not to mention change the law itself.

As businesses and other potential clients explore blockchain, they are hiring firms whose lawyers understand this technology and what it means for their interests. Some firms are offering blockchain services.[82] Firms have been formed focusing entirely on these new technologies.[83] To ensure their graduates are prepared for this new practice, law schools have begun to offer blockchain classes to interested students.[84]

Meanwhile, blockchain is changing the way common legal transactions function. The Ethereum programming language, for example, is being used to create smart contracts.[85] These contracts are designed to be launched and run automatically—the parties rely on the code to handle the transaction on its own.

These contracts can be simple or complex. For example, Buyer Company contracts with Manufacturer Company to purchase 10 widgets for $100. The companies decide to create a smart contract that will ensure Buyer Company automatically pays Manufacturer Company when the widgets are received.[86] It might be programmed to look something like this:

2018), https://gcn.com/articles/2018/02/05/illinois-blockchain.aspx.

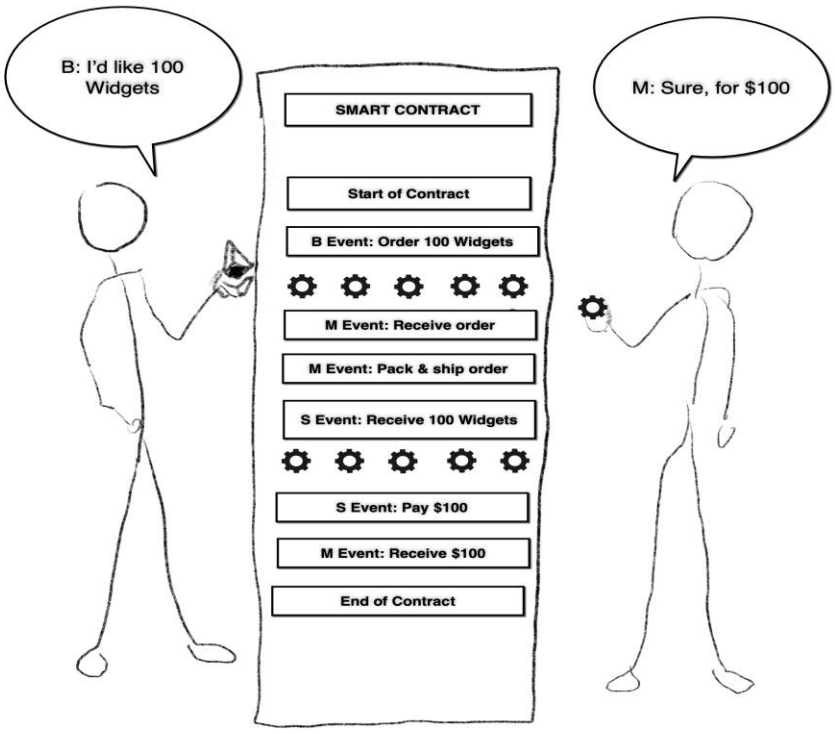
[82] Stephanie Russell-Kraft, *Blockchain Makes New Waves as Law Firms Build Expertise*, BLOOMBERG L.: BIG L. BUS. (Jan. 9, 2018), https://biglawbusiness.com/blockchain-makes-new-waves-as-law-firms-build-expertise/.

[83] *See, e.g.*, NELSON M. ROSARIO, https://www.nelsonmrosario.com/ (last visited Feb. 4, 2019).

[84] *See, e.g.*, BLOCKCHAIN LAW CLASS, https://www.blockchainlawclass.com/ (last visited Feb. 4, 2019) (providing information on a class in Blockchain and the Law starting in spring 2018 at Chicago-Kent); *see also* Gabrielle Orum Hernández, *Blockchain 101: Law Schools Tackle the New Frontier*, LEGALTECH NEWS (Feb. 8, 2018, 8:00 AM), https://www.law.com/legaltechnews/sites/legaltechnews/2018/02/08/blockchain-101-class-now-in-session/.

[85] *How Do Ethereum Smart Contracts Work?*, COINDESK, https://www.coindesk.com/information/ethereum-smart-contracts-work (last visited Feb. 5, 2019).

[86] Gear icon used with permission from "Saifurrijal100" at https://thenounproject.com/search/?q=gear&i=2186710 (author has NounPro

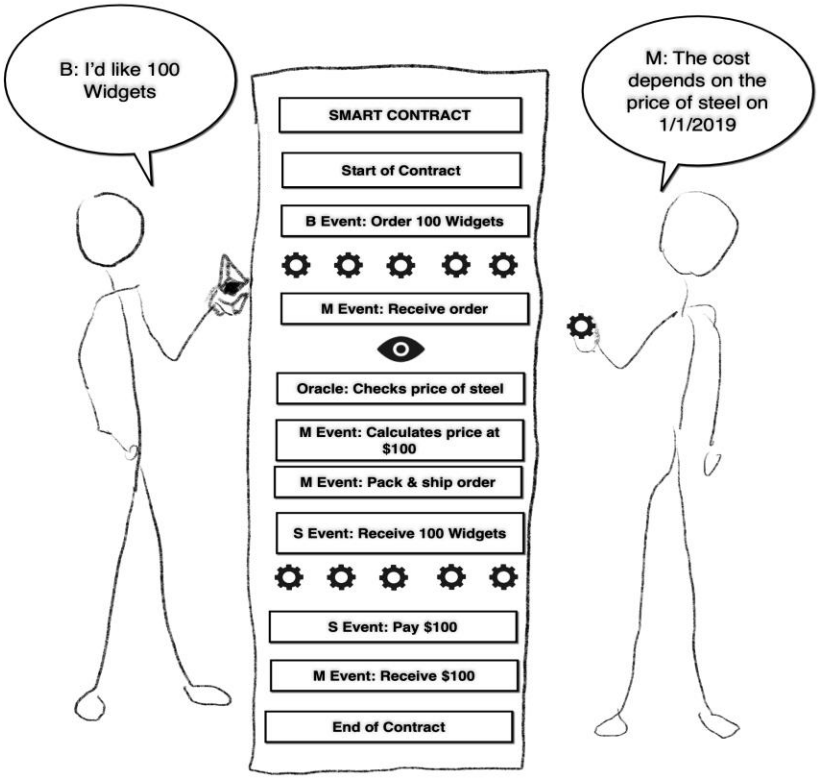


Smart contracts can also incorporate information outside of the main body of the contract using information gathering tools called "oracles."[87] If the price of the widgets is based on the cost of steel on January 1, 2019, as reflected in the database at GreatSteelMarket.com, the smart contract's oracle would check the database for the price and add that information to the smart contract, like this:[88]

subscription).

[87] *Blockchain Oracles*, BLOCKCHAINHUB, https://blockchainhub.net/blockchain-oracles/ (last visited Feb. 5, 2019).

[88] Eye icon used with permission from "Celcius Creative" at https://thenounproject.com/search/?q=eye&i=2187793.



Other legal professionals are considering using blockchain in a similar manner. Real estate transactions are complex because the parties need to establish trust in one another.[89] Since the technology of blockchain incorporates technologies designed to allow strangers to trust one another, many of these complexities (e.g., escrow) might be eliminated in a smart real estate transaction.[90]

New laws are also being passed that incorporate blockchain into current legal structures and to define expected parameters for this

[89] Gina Clarke, *How Real Estate Is Breaking the Blockchain Mold*, FORBES (Nov. 20, 2018, 5:03 AM), https://www.forbes.com/sites/ginaclarke/2018/11/20/how-real-estate-is-breaking-the-blockchain-mold/.

[90] Katalyse.io, *Blockchain Disrupting Finance — Payments and Escrow*, MEDIUM: CRYPTODIGEST (July 15, 2018), https://cryptodigestnews.com/blockchain-disrupting-finance-payments-and-escrow-c2af0a224d4d.

new technology. Several states, such as Delaware,[91] Wyoming,[92] and Arizona,[93] have already passed blockchain legislation. Other states are considering their options.[94]

However, a few of these initial laws suffer from technological misunderstandings. For example, Arizona's law states that blockchains are immutable. They are in theory, but like any other technology, they are not flawless and can be changed under certain conditions.[95] Legislators should work closely with blockchain and FinTech experts when drafting new laws to avoid these kinds of issues.

IV. CONCLUSION

All this said, this technology is still new. Recently, so much hype has been published about blockchains that some experts claim it cannot possibly live up to its expectations.[96] That is true, but the

---

[91] Doneld G. Shelkey, *Delaware Blockchain Law Goes into Effect*, MORGAN LEWIS (Aug. 11, 2017), https://www.morganlewis.com/blogs/sourcingatmorganlewis/2017/08/delaware-blockchain-law-goes-into-effect.

[92] *Wyoming Passes 5 Pro-Blockchain Laws, Points the Way in Digital Asset Regulation*, CONSENSYS MEDIA (Mar. 15, 2018), https://media.consensys.net/wyoming-passes-5-pro-blockchain-laws-points-the-way-in-digital-asset-regulation-6fae9e07d129.

[93] Jeffrey D. Neuburger, *Arizona Passes Groundbreaking Blockchain and Smart Contract Law – State Blockchain Laws on the Rise*, NAT'L L. REV. (Apr. 20, 2017), http://www.natlawreview.com/article/arizona-passes-groundbreaking-blockchain-and-smart-contract-law-state-blockchain; Deborah Dobson, *Ohio Jumps on the Bandwagon of States Legally Recognizing Blockchain Data*, INT'L LEGAL TECH. ASS'N (Aug. 9, 2018, 1:57 PM), http://iltanet.org/blogs/deborah-dobson/2018/08/09/ohio-jumps-on-the-bandwagon-of-states-legally-reco.

[94] Ted Knutson, *State Lawmakers Dipping Toes into Crypto, Blockchain*, FORBES (Feb. 4, 2019, 9:05 AM), https://www.forbes.com/sites/tedknutson/2019/02/04/state-dipping-toes-into-crypto-blockchain/.

[95] Mike Orcutt, *States That Are Passing Laws to Govern "Smart Contracts" Have No Idea What They're Doing*, MIT TECH. REV. (Mar. 29, 2018), https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/.

[96] Matt Higginson, Marie-Claude Nadeau & Kausik Rajgopal, *Blockchain Development and the Occam Problem*, MCKINSEY (Jan. 2019), https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem.

technology is not completely stagnant. New blockchain projects are being launched all the time.[97]

Moreover, even if blockchain does not revolutionize law or finance, lawyers should still pay attention to it because it is likely the foundation of a larger movement. Blockchain databases are linked by blocks and hashes, but this is not the only solution for creating decentralized, secure databases. The blockchain is one of a series of related databases that tech experts are looking at to better organize information. Blockchain and its related databases are known as distributed ledger technologies.[98] The related databases use other ways of handling the information that do not rely on the computing power and linear structure of blockchain. Financial, legal, and other industries will need newer kinds of database structures in the future to operate at peak efficiency. If blockchain proves to not be the structure they need, one of the related databases will fill that niche.

---

[97] *See, e.g.*, Steve Kaaru, *Blockchain Startup DOVU Will Reward Users for Sharing Transport Data*, COINGEEK (Feb. 4, 2019), https://coingeek.com/blockchain-startup-dovu-will-reward-users-sharing-transport-data/; Yogita Khatri, *Fujitsu Claims 40% Efficiency Boost for Blockchain Electricity Exchange*, COINDESK (Jan. 30, 2019), https://www.coindesk.com/fujitsu-claims-40-efficiency-boost-for-blockchain-electricity-exchange; Kevin Truong, *New Blockchain Collaboration Launches with Aetna, Anthem and HCSC*, MEDCITY NEWS (Jan. 24, 2019, 2:57 PM), https://medcitynews.com/2019/01/new-blockchain-collaboration-launches-with-aetna-anthem-and-hcsc/.

[98] Antony Lewis, *What's the Difference Between a Distributed Ledger and a Blockchain?*, BITS ON BLOCKS (Feb. 20, 2017), https://bitsonblocks.net/2017/02/20/whats-the-difference-between-a-distributed-ledger-and-a-blockchain/.