Arkansas Law Review

Volume 73 | Number 2 Article 4

August 2020

Crypto and Blockchain Fundamentals

Mary C. Lacity
University of Arkansas, Fayetteville

Recommended Citation
Mary C. Lacity, *Crypto and Blockchain Fundamentals*, 73 Ark. L. Rev. 363 (2020).
Available at: https://scholarworks.uark.edu/alr/vol73/iss2/4

CRYPTO AND BLOCKCHAIN FUNDAMENTALS

Mary Lacity[*]

I. FROM THE "INTERNET OF INFORMATION" TO THE "INTERNET OF VALUE"

"I believe blockchain will do for trusted transactions what the Internet has done for information." — Ginni Rometty, CEO of IBM[1]

Since the 1990s, we have had an "Internet of Information" that allows us to seamlessly share *information* such as documents, images, emails, and videos over the Internet. While most Internet users do not need to understand the details of the technical protocols[2] operating underneath user-friendly software interfaces, it is helpful to understand how they work at a high-level. With the "Internet of Information," *copies* of information are routed

[*] Dr. Mary C. Lacity is a Walton Professor of Information Systems and Director of the Blockchain Center of Excellence in the Sam M. Walton College of Business at the University of Arkansas. She was previously the Curators' Distinguished Professor at the University of Missouri-St. Louis. She has held visiting positions at MIT, the London School of Economics, Washington University, and Oxford University. She is a Certified Outsourcing Professional® and Senior Editor for *MIS Quarterly Executive*. Her recent research focuses on improving business services using Robotic Process Automation (RPA), Cognitive Automation (CA), and Blockchain technologies. She has given keynote speeches and executive seminars worldwide, and has served as an expert witness for the U.S. Congress. She was inducted into the IAOP's Outsourcing Hall of Fame in 2014, one of only three academics to ever be inducted. She has published twenty-nine books, including, A Manager's Guide to Blockchains for Business. Her publications have appeared in the *Harvard Business Review*, *Sloan Management Review*, *MIS Quarterly, MIS Quarterly Executive, IEEE Computer, Communications of the ACM,* and many other outlets.

[1] Ginni Rometty, CEO, IBM, Keynote Address at IBM InterConnect (Mar. 21, 2017), [https://perma.cc/M87K-WZGT].

[2] Transmission Control Protocol/Internet Protocol (TCP/IP) is the Internet's primary protocol. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1221 n.111 (1998). It breaks messages into packets and routes them to their destination as defined by a unique address called an "IP address." *Id.* Every device connected to the Internet has a unique IP address, including computers, mobile phones, laptops, printers, IoT devices, servers, routers, etc. *Id.*

over the Internet.[3] If a sender emails a friend, the sender keeps the original email, and the friend receives a copy of the email.[4] To transact *value*, i.e., money, over the Internet, one cannot send a copy. Instead, after the transfer of value is complete, the sender should no longer have the money, but rather the recipient should.

The best way to understand how blockchain technologies enable the "Internet of Value" is to compare them to the way trading partners transact today. Before adopting blockchain technologies, parties transact value over the Internet (and other networks) by: (1) using government-issued currencies as legal tender; (2) engaging trusted third parties (TTPs) to mitigate counter-party risks—the risk each trading party bears that the other party will not fulfill its contractual obligations; and (3) maintaining separate accounting systems to record transactions. Each of these transaction facilitators have the following advantages and disadvantages:

Government-issued currencies: Governments issue and regulate legal tender. The advantages of government-issued currencies are that they serve as legal mediums of exchange for the payment of debts, as common measures of value, and as stores of value that aim to retain their worth over time. The United Nations recognizes 180 currencies as legal tender.[5] On what some consider to be the downside, most sovereign currencies are now fiat, backed solely on the promises of governments.[6] Governments can print fiat money at will, causing inflation, and change regulations on a whim.[7] Governments can also freeze, seize, or restrict access to one's assets.[8]

[3] JEAN-HERVÉ LORENZI & MICKAËL BERREBI, PROGRESS OR FREEDOM: WHO GETS TO GOVERN SOCIETY'S ECONOMIC AND TECHNOLOGICAL FUTURE? 53 (Dina Leifer trans., 2019).

[4] *Id.*

[5] Benjamin Elisha Sawe, *How Many Currencies Exist in the World?*, WORLDATLAS (June 28, 2018), [https://perma.cc/SGJ9-JPZB].

[6] Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 576 (2015).

[7] Stephanie A. Lemchuk, *Virtual Whats?: Defining Virtual Currencies in the Face of Conflicting Regulatory Guidances*, 15 CARDOZO PUB. L. POL'Y & ETHICS J. 319, 320-21 n.6-7 (2017).

[8] For example, the Greek banks would not allow account holders to withdraw more than 60 euros a day in 2015.

Trusted third parties: When transferring value, "parties rely on [TTPs] to . . . mitigate counter-party risks."[9] Banks, credit card companies, money transmitters, notaries, and other TTPs "provide independent 'truth attestations' such as notarizing signatures; verifying identity; verifying ownership; authenticating assets;" assuring accounts are funded before value is transferred to prevent double spending; and "attesting that agreements have been properly executed."[10] TTPs provide these and many other vital services to facilitate trade (the advantages), for which they earn significant transaction fees (a disadvantage).[11] Additionally, banks lose money on checking accounts and have few financial incentives to service low-income people.[12] Consequently, over a quarter of the world's population does not have access to financial services.[13]

Party-level record keeping: Before a blockchain application, every party maintains its own accounting records.[14] Some advantages are that each party can swiftly and unilaterally execute decisions about accounting rules, transaction reversals, and software upgrades within the boundaries of the firm. However, with party-level record keeping, every party has its own version of the transaction that needs to be reconciled with trading partners, and reconciliations are expensive and time-consuming.[15] Once reconciled, there is nothing to prevent trading partners from

Associated Press, *The Latest: Strict Limits on Bank Withdrawals Will Not Apply to Foreign Credit Cards*, U.S. NEWS & WORLD REP. (June 28, 2015), [https://perma.cc/76BD-B34T].

[9] Mary Lacity et al., *Special Issue Editorial: Delivering Business Value Through Enterprise Blockchain Applications*, 18 MIS Q. EXECUTIVE ix, x (2019).

[10] *Id.*

[11] According to McKinsey & Company, the world sends more than $135 trillion across borders each year. MCKINSEY & CO., GLOBAL PAYMENTS 2016: STRONG FUNDAMENTALS DESPITE UNCERTAIN TIMES 2, 14 (2016), [https://perma.cc/9YT6-2JYN]. Third-party intermediaries collect about $2.2 trillion in revenue to facilitate these transactions. *Id.* at 2.

[12] On average, American banks incurred costs of $349 a year per checking account and recovered only $268 in transaction fees. AM. BANKERS ASS'N, FEES AND PRICING OF BANKING PRODUCTS 108 (2016), [https://perma.cc/6VPZ-2F8B].

[13] ASLI DEMIRGÜÇ-KUNT ET AL., THE WORLD BANK GROUP, THE GLOBAL FINDEX DATABASE 2 (2017) (". . . 69 percent of adults now have [a bank] account, up from 62 percent in 2014 and 51 percent in 2011.").

[14] MARY C. LACITY, A MANAGER'S GUIDE TO BLOCKCHAIN FOR BUSINESS: FROM KNOWING WHAT TO KNOWING HOW 42 (2018).

[15] *Id.* at 42-43.

modifying records after the fact.[16] Thus, partners cannot be confident that they are dealing with the same historical record of transactions through time.

Satoshi Nakamoto—a pseudonym used by an unknown person or persons who remains anonymous to this day—imagined a world where people could safely, securely, and anonymously transfer value directly with each other (1) without using government-issued currencies, (2) without relying upon trusted third parties, and (3) without the need to reconcile records across trading partners.[17] Nakamoto's innovation is Bitcoin, described in a white paper posted to a cryptographic mailing list on October 31, 2008.[18] The timing of Bitcoin was no accident. After the 2008 Global Financial Crisis—possibly the greatest economic disruption since the Great Depression of 1929—people became increasingly distrustful of financial institutions.[19] Movements like Occupy Wall Street ranted against wealth inequality and the influence of large financial institutions on government policy.[20] People rallied against the government's power to control money.[21] Bitcoin has its roots in Libertarian and Cypherpunk values, which aim to create social and political change by circumventing governments and large financial institutions through privacy-enhancing technologies.[22]

[16] *Id.* at 43; *see also* Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 REV. BANKING & FIN. L. 713, 736-37 (2017).

[17] *See* Deniz Appelbaum & Sean Stein Smith, *Blockchain Basics and Hands-on Guidance, Taking the Next Step Toward Implementation and Adoption,* THE CPA J. (June 2018), [https://perma.cc/9DFC-SLF6].

[18] Paul Vigna, *Bitcoin Turns 10: Still Not All Grown Up*, WALL ST. J., (Oct. 31, 2018), [https://perma.cc/SMX6-34NT].

[19] David De Cremer, *Why Our Trust in Banks Hasn't Been Restored*, HARV. BUS. REV. (Mar. 3, 2015), [https://perma.cc/R9TS-CVV7].

[20] John L. Hammond, *The Anarchism of Occupy Wall Street*, 79 SCI. & SOC'Y 288, 288-89 (2015).

[21] *See id.*

[22] LACITY, *supra* note 14, at 53-54; *see also* Nathaniel Popper, *Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin*, N.Y. TIMES (May 15, 2015), [https://perma.cc/D8ZA-DQ2C].

II. THE INGENUITY AND LIMITATIONS OF BITCOIN

"Bitcoin[] is a remarkable cryptographic achievement [and] the ability to create something which is not duplicable in the digital world has enormous value." – Eric Schmidt, former CEO of Google[23]

"I think the fact that within the Bitcoin universe an algorithm replaces the functions of [the government] . . . is actually pretty cool. I am a big fan of Bitcoin." – Al Gore, 45th Vice President of the United States[24]

Nakamoto's nine-page white paper specified the technical requirements for the "Internet of Value."[25] Quite simply, Nakamoto proposed "[a] purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[26] Bitcoin achieves this by shifting: (1) from government-issued currencies to a cryptocurrency; (2) from trusted third parties to automated and community-driven counter-party risk mitigation; and (3) from party-level record keeping to shared record keeping.

1. From government-issued currencies to a cryptocurrency: Rather than use a government-issued currency, Bitcoin created a new *cryptocurrency*—a digital currency secured by cryptography that makes it nearly impossible to counterfeit.[27] It is not controlled by any government or institution. Rather, Bitcoin's monetary policies are programmed into the software.[28]

[23] IDG News Service, *Google's Schmidt: Bitcoin Is a Remarkable Cryptographic Achievement*, YOUTUBE (Mar. 3, 2014), [https://perma.cc/59QE-4H67].

[24] Kyle Samani, *How Crypto Will Reshape Capitalism as We Know It*, FORBES (Oct. 4, 2017), [https://perma.cc/X83C-2MUT].

[25] *See generally* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), [https://perma.cc/TL4X-DAY7]; *see also The Internet of Value: What It Means and How It Benefits Everyone*, RIPPLE (June 21, 2017), [https://perma.cc/R4TT-6V7E].

[26] NAKAMOTO, *supra* note 25, at 1.

[27] Cryptography is "a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it." Margaret Rouse, *Cryptography*, TECH TARGET, [https://perma.cc/P59E-EJF3] (last visited Mar. 4, 2020).

[28] *See* Nakamoto, *supra* note 25, at 1-3.

Specifically, Bitcoin's software capped the total monetary supply at 21 million bitcoins and has an automatic monetary distribution schedule.[29] The last bitcoin will be released in the year 2140.[30]

2. From TTPs to automation and community-driven counter-party risk mitigation: Rather than rely on TTPs to mitigate counter-party risks, Bitcoin automates some of the services normally done by TTPs and engages a community to perform other services.[31] For an automation example, Bitcoin (and many blockchain applications that followed) relies on cryptographic private-public key pairs to verify account ownership.[32] Whoever is in possession of the private key is assumed to be the legitimate owner of the account.[33] Validating transactions to prevent double spending is a bit trickier to solve without trusted third parties. Senders cannot be trusted to verify that they have enough cryptocurrency in their accounts to fund their transactions. An independent verifier is needed, but Nakamoto did not want to rely on traditional financial institutions to provide the validation.[34] Here was Nakamoto's brilliant solution: reward other people in the network (called "miners")[35] with newly issued bitcoins to validate all the recently submitted

[29] Paul Vigna et al., *Why Bitcoin? Why Now?*, WALL ST. J. (Dec. 9, 2017), [https://perma.cc/T4FK-S8UH].

[30] *Id*.

[31] *See* Nathan Reiff, *Blockchain Won't Cut Out Intermediaries After All*, INVESTOPEDIA (Mar. 5, 2020), [https://perma.cc/Y3CP-9BGB].

[32] *See* Demiro Massessi, *Blockchain Public/Private Key Cryptography in a Nutshell*, MEDIUM (Mar. 5, 2020), [https://perma.cc/S42R-VGRS].

[33] *See* Evan S. Strassberg & Brad R. Jacobsen, *Regulation of the Unregulated: How Bitcoin and Cryptocurrencies Show That the Government Can Regulate Anything*, 24 WESTLAW J. 6, 6 (2018).

[34] *See* NAKAMOTO, *supra* note 25, at 1.

[35] The Bitcoin protocol is based on a gold mining metaphor. Just as gold miners *work* using physical resources to excavate gold from gold mines, Bitcoin miners *work* using computer resources to release new bitcoins; Bitcoin, like gold, has a limited supply, making it a rare commodity. *See* Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. LAW J. 441, 446 (2014); Benjamin Akins et al., *The Case for the Regulation of Bitcoin Mining as a Security*, 19 VA. J. L. & TECH. 669, 677-78 (2015). Just as it gets harder to mine gold as a gold mine is depleted, Bitcoin releases fewer new digital coins over time. *See* Adam Barone, *What Happens to Bitcoin After All 21 Million Are Mined?*, INVESTOPEDIA (Oct. 22, 2019), [https://perma.cc/TYP4-CX2A].

transactions.[36] The economic incentives of the Bitcoin network motivate validators to play by the rules.[37]

3. From party-level record keeping to shared record-keeping: The Bitcoin network maintains a digital ledger, called a *blockchain*,[38] to serve as the universal record of truth. The ledger is distributed to all the host computers (called "nodes")[39] that run the Bitcoin network. There were over 9,000 Bitcoin nodes as of December 2019.[40]

Overall, Bitcoin promises to deliver the following benefits:

[36] Bryans, *supra* note 35, at 446; Akins, *supra* note 35, at 678-79.

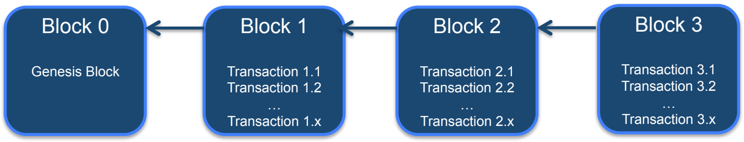
[37] Nakamoto wrote this about the economic incentives to motivative miners to behave honestly:

> If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

NAKAMOTO, *supra* note 25, at 4.

[38] The term "blockchain" is used several ways. Sometimes the term refers broadly to an entire "blockchain application." For example, people call the entire Bitcoin network a "blockchain." *See* Nathan Reiff, *Blockchain Explained*, INVESTOPEDIA (Feb. 1, 2020), [https://perma.cc/4BBW-VPKM]. The term can also be used to describe the structure of the digital ledger within an application. *Id*. With a blockchain structure, newly submitted transactions are sequenced and collected into a block (see Figure below). *Id*. The block comprises a header and a payload of transactions. *See* Le Su et al., *Securing Intelligent Transportation System: A Blockchain-Based Approach with Attack Mitigation*, *in* SMART BLOCKCHAIN (Meikang Qiu ed., Springer Nature Switz. 2019). The block header includes a pointer to the previous block of transactions, forming a chain of sequenced blocks over time, all the way back to the first block, called the "genesis block." *See id*; *see also* Carla Tardi, *Genesis Block*, INVESTOPEDIA (Sept. 11, 2019), [https://perma.cc/48UG-N3MP].

Distributed Ledger Structured as a Chain of Blocks



[39] Each Bitcoin node is a host computer that runs the Bitcoin software and keeps a copy of the digital ledger; each node within the network has a unique identifier called an Internet Protocol (IP) address. *See* LACITY, *supra* note 14, at 227.

[40] The actual number of Bitcoin nodes is difficult to track because some nodes operate behind firewalls. *See* David Hundeyin, *Number of Reachable Bitcoin Nodes Fell 19% in 2018*, CCN.COM (Dec. 13, 2018), [https://perma.cc/W3LE-CM52]. This site tracks "reachable" nodes: *Global Bitcoin Nodes Distribution*, BITNODES, (Mar. 19, 2020), [https://perma.cc/5JYT-XDXE].

No need for reconciliations. Bitcoin's blockchain has one distributed ledger that is copied on every node, serving as one version of the truth.[41] Once transactions are added to the ledger, they are never deleted or modified, a property known as *immutability*.[42] The process for updating the ledger works as follows: New transactions submitted to the Bitcoin network are verified or rejected by miners' computers competing to create the next block of transactions.[43] Verified transactions are time-stamped, sequenced, secured with unique cryptographic identifiers, and appended to the ledger.[44] The first miner that updates the ledger distributes the update to the other nodes in the Bitcoin network.[45] Once the nodes accept the update, the network reaches *consensus*, meaning that they all agree, this is the "record of truth."[46]

Anonymity. Bitcoin's blockchain allows two parties to exchange value in anonymity.[47] The public ledger records payments from and to Bitcoin accounts (called "addresses"), but no personal information is tracked or stored.[48] Anyone with access to the Internet can view the entire blockchain.[49]

Predictable and lower transaction fees. Bitcoin's blockchain was designed to require very low transaction fees from trading partners.[50] People sending bitcoins from an address

[41] *See* LACITY, *supra* note 14, at 45.

[42] *See id.* at 221.

[43] *See* Brandon Ferrick, *Modernizing the Stockholder Shield: How Blockchains and Distributed Ledgers Could Rescue the Appraisal Remedy*, 60 B.C. L. REV. 621, 652-53 (2019).

[44] *See* LACITY, *supra* note 14, at 213.

[45] *See id.* at 47.

[46] *See* MICHAEL J. CASEY & PAUL VIGNA, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING 64-65 (2018); NAKAMOTO, *supra* note 25, at 3; *Consensus*, BITCOIN, [https://perma.cc/DK6J-AA3T] (last visited Feb. 26, 2020).

[47] *See* Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J. L. & TECH. 587, 593 (2014).

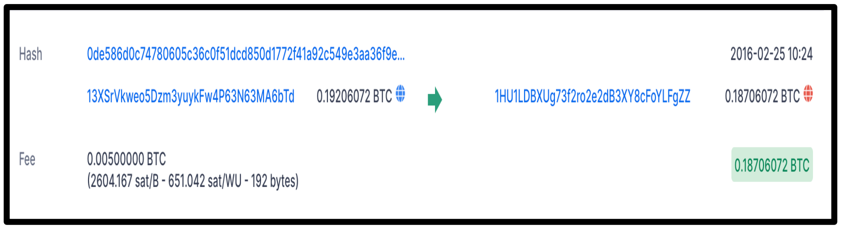
[48] *Id.*

[49] *See Block Explorer*, BLOCKCHAIN.COM, [https://perma.cc/X7PQ-S9F4] (last visited Feb. 27, 2020).

[50] *See* NAKAMOTO, *supra* note 25, at 4; Jonathan B. Turpin, *Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework*, 21 IND. J. GLOBAL LEGAL STUD. 335, 336 (2014). Miners are primarily incentivized to verify and

are supposed to offer a small fee to incentivize miners to verify their transactions, but an additional purpose of the fees is to prevent Denial of Service (DoS) attacks.[51] Planning ahead, Nakamoto also realized that once there were enough bitcoins in circulation, transaction fees could become the sole miner incentive.[52]

Figure 1: An Example of a Transaction Stored on Bitcoin's Public Ledger



Hash 0de586d0c74780605c36c0f51dcd850d1772f41a92c549e3aa36f9e... 2016-02-25 10:24

13XSrVkweo5Dzm3yuykFw4P63N63MA6bTd 0.19206072 BTC → 1HU1LDBXUg73f2ro2e2dB3XY8cFoYLFgZZ 0.18706072 BTC

Fee 0.00500000 BTC
(2604.167 sat/B - 651.042 sat/WU - 192 bytes)

0.18706072 BTC

This transaction, which occurred on February 25, 2016, shows a transfer of value from the sender's address on the right to the receiver's address on the left. The sender also provided a small transaction fee for the miner of .005 bitcoins. The "hash" is a unique transaction identifier calculated from the inputs.

add transactions to the blockchain by winning a block reward of newly released bitcoins. Turpin, *supra*, at 340-41. The initial mining reward was 50 bitcoins per block, with the reward being halved every 210,000 blocks. Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213, 218 (2015); Christine Kim, *With 18 Million Bitcoins Mined, How Hard Is That 21 Million Limit?*, COINDESK, [https://perma.cc/UP2G-9DZT] (last updated Oct. 21, 2019). This website tracks the current mining reward (which was 12.5 bitcoins per block in January 2020): *Bitcoin Block Reward Halving Countdown*, [https://perma.cc/GU7S-C5WG] (last visited Feb. 27, 2020).

[51] *See* NAKAMOTO, *supra* note 25, at 4; Böhme et al., *supra* note 50, at 218. A Denial of Service (DoS) attack is a type of malicious attack that floods a network with so many transactions that it disrupts service for legitimate users. Böhme et al., *supra* note 50, at 228; Marcel T. Rosner & Andrew Kang, *Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study*, 114 MICH. L. REV. 649, 659 (2016). By requiring a small transaction fee, a malicious actor would soon find it too expensive to flood the Bitcoin network with millions of phony transactions. *See* NAKAMOTO, *supra* note 25, at 4.

[52] NAKAMOTO, *supra* note 25, at 4.

- **Financial Inclusion.** Bitcoin provides a way for lower income people to transfer value without owning a checking account or relying on expensive money transmitters.[53]
- **Rapid settlement times compared to TTPs.** Bitcoin's blockchain is designed to create a new block of recent transactions—on average, every ten minutes.[54]
- **Democratic and predictable changes in the rules.** Bitcoin's blockchain provides a non-fiat, universal cryptocurrency guided by an open community.[55] Anyone can propose ideas to improve Bitcoin by submitting a Bitcoin Improvement Proposal (BIP).[56] The whole Bitcoin community (miners, developers, and users) can vote on the proposal based on its merit.[57]
- **Heightened security.** The nodes in the Bitcoin network constantly chatter with each other to make sure no party tampers with the records after-the-fact.[58] If anyone cheats, the other parties' nodes automatically ignore it.[59] An attacker would need to commandeer over fifty percent of the network and try to rewrite history before any of the other nodes noticed.[60] Additionally, anyone who could take over fifty percent of the network would devalue his or her own fortune.[61] Thus, Nakamoto

[53] DAVID ORRELL & ROMAN CHLUPATÝ, THE EVOLUTION OF MONEY 201-02 (2016).

[54] *Id.* at 200; Böhme et al., *supra* note 50, at 217.

[55] *See* Kien-Meng Ly, *supra* note 47, at 589-90; Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041, 1066 (2017); Alice Lynx, *Is Bitcoin a Fiat Currency? Why? or Why Not?*, CRYPTALKER, [https://perma.cc/54JP-6FFV] (last visited Feb. 28, 2020).

[56] Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 548 (2018); Harsh Agrawal, *What Is a BIP (Bitcoin Improvement Proposal)? Why Do You Need to Know About It?*, COINSUTRA, [https://perma.cc/6SR2-U7WJ] (last updated Sept. 6, 2019).

[57] Agrawal, *supra* note 56. As of this writing, 342 BIPs have been submitted, of which 37 have been finalized. *Bitmark Improvement Process*, GITHUB, [https://perma.cc/CM75-24WR] (last visited Feb. 28, 2020).

[58] *See* NAKAMOTO, *supra* note 25, at 3, 5; Chris Grundy, *How to Run a Full Node*, THE COIN OFFERING (Sept. 13, 2018), [https://perma.cc/2HAE-NST9]; Jameson Lopp, *Bitcoin's Security Model: A Deep Dive*, COINDESK, [https://perma.cc/8GJB-MTK5] (last updated Feb. 22, 2019).

[59] *See* NAKAMOTO, *supra* note 25, at 6.

[60] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 25 (Harvard Univ. Press 2018); Lopp, *supra* note 59.

[61] *See* DE FILIPPI & WRIGHT, *supra* note 61, at 25.

> designed the protocol to be computationally and financially impractical for an attack. Thus far, there has been only one major attack on the Bitcoin network, which occurred back in 2010.[62] Nakamoto quickly remedied the software vulnerability.[63] (Most heists of bitcoins and other cryptocurrencies happen at the vulnerable access points of digital wallets where private keys are stored, not on the ledger itself.)[64]

Bitcoin is the most visible on-going, live experiment for an open, public, secure, non-governmental, non-TTP reliant "Internet of Value." All are welcome to participate. Millions of people use it—over 32 million Bitcoin wallets have been created.[65] Thousands of people help secure it by being miners. Bitcoin proves that the "Internet of Value" is technically feasible and that a shared digital ledger is highly secure. However, Bitcoin—like all innovations—has advantages and disadvantages. Bitcoin's limitations include:

- **Low transactions per second (TPS).** Bitcoin's network processes about two to six TPS.[66] By comparison, Visa and Mastercard can process thousands of TPS.[67]
- **Slower settlement times than other blockchains.** While Bitcoin has faster settlement times than traditional TTPs, Bitcoin is one of the slowest blockchain networks.

[62] LACITY, *supra* note 14, at 138.

[63] "The Bitcoin blockchain was hacked in August 2010 when someone exploited a software vulnerability to create 184 *billion* bitcoins, a highly suspicious act given the maximum money supply is only 21 *million* bitcoins." *Id.* (emphasis added). "Nakamoto quickly hard forked the blockchain to remove the [184 plus] billion [b]itcoins." Charlie Shrem, *Bitcoin's Biggest Hack in History: 184.4 Billion Bitcoin from Thin Air*, HACKERNOON (Jan. 11, 2019), [https://perma.cc/WP7V-HZL5].

[64] Henry S. Zaytoun, *Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*, 97 N.C. L. REV. 395, 407-08 (2019).

[65] Alex Lielacher, *How Many People Use Bitcoin in 2020?*, BITCOIN MKT. J. (Feb. 5, 2020), [https://perma.cc/824U-SLZ7].

[66] *See Transaction Rate*, BLOCKCHAIN, [https://perma.cc/4KAK-M95P] (last visited Mar. 26, 2020).

[67] Ryan Vlastelica, *Why Bitcoin Won't Displace Visa or Mastercard Soon*, MARKETWATCH (Dec. 18, 2017), [https://perma.cc/U6MV-GVA5].

Transactions are not considered to be truly settled for at least an hour.[68]

- **Threats to anonymity.** Although Bitcoin transactions are anonymous in that no personal identities are revealed on the public ledger, meta patterns can emerge where identities could be deduced.[69] People thus consider Bitcoin to be "pseudonymous" rather than "anonymous."[70]
- **Traditional enterprises need confidentiality, not anonymity.** Traditional enterprises need information about their transactions to be visible, but only to authorized parties. Most enterprises do not see use cases for public blockchains like Bitcoin.
- **Poor store of value.** Compared to fiat currencies, Bitcoin's price volatility is high.[71] In 2019, Bitcoin's price ranged from $3,400 to over $12,600 per bitcoin.[72]
- **Poor user access and experience.** Users connect directly to the Bitcoin network by using a digital

[68] Although a new block is created every ten minutes on average, the actual settlement time is longer due to the possibility of a temporary divergence of the network. *See* Joseph Bonneau, *How Long Does It Take for a Bitcoin Transaction to be Confirmed?*, COIN CENTER (Nov. 3, 2015), [https://perma.cc/78H9-3A4T]. Sometimes two nodes in a distributed blockchain network create the next block at the same time, resulting in two versions of the top of the ledger called a "soft fork." *See id.*; John Light, *The Differences Between a Hard Fork, a Soft Fork, and a Chain Split, and What They Mean for the Future of Bitcoin*, MEDIUM (Sept. 25, 2017), [https://perma.cc/MRB2-Z5CQ]. For a short while, different nodes in the network work off of different branches of the ledger until one branch is established as the longest and therefore the valid branch. *See id.* To confidently consider a bitcoin transaction to be settled, it is generally recommended to wait until the transaction is six blocks deep, which takes an hour on average. *See* Bonneau, *supra*.

[69] LACITY, *supra* note 14, at 148. For example, if two parties to an exchange know each other's identities, each can trace subsequent transactions in or out of those addresses. *See id.* Moreover, "[m]any transactions are funded with multiple addresses," allowing a party to tie an identity to even more addresses. *Id.*

[70] *Bitcoin Anonymity-Is Bitcoin Anonymous?*, BUY BITCOIN WORLDWIDE, [https://perma.cc/2UPP-9HEW] (last visited Feb. 26, 2020).

[71] Bitcoin's price is more volatile than emerging fiat currencies, oil, gold, and U.S. stocks. *See Bitcoin Volatility vs Other Assets*, WOODBULL CHARTS, [https://perma.cc/F4RX-3QGN] (last visited Feb. 26, 2020).

[72] *Bitcoin Price*, COINBASE, [https://perma.cc/QWW4-29YA] (last visited Feb. 26, 2020).

wallet.[73] Few users are technically sophisticated enough to protect their wallets.[74]

- **High resource consumption.** To successfully compete for new bitcoins, Bitcoin miners use specialized computer hardware that consumes a lot of electricity.[75]
- **Limited functionality.** Bitcoin is just a payment system to send and receive bitcoins. It cannot do much else.
- **Regulatory uncertainty.** At first, regulators around the world ignored Bitcoin.[76] However, regulatory bodies have since responded, as discussed in this issue of *The Arkansas Law Review*.[77]

The blockchain innovations that followed Bitcoin aimed to improve upon Bitcoin's limitations.

III. Beyond Bitcoin: Other Technical Innovations

"*I think that there is effective forward motion in the resolution and the ability to address some of the technical challenges that exist*." — Eamonn Maguire, Global Lead, Digital Ledger Services, KPMG[78]

Following Bitcoin's launch in 2009, a proliferation of blockchain innovations emerged. Some notable examples are plotted on a timeline in Figure 2, listed in Table 1, and described below.

[73] *Some Bitcoin Words You Might Hear*, BITCOIN, [https://perma.cc/E536-24G7] (last visited Feb. 26, 2020).

[74] A digital wallet stores the private keys that controls Bitcoin accounts (addresses). LACITY, *supra* note 14, at 217. If the private key is lost or stolen, there is no way to recover the private keys. *Id.*

[75] Digiconomist, a site that tracks Bitcoin's energy consumption, reports that a single Bitcoin transaction consumes enough electrical energy to power an average U.S. household for twenty-two days. *Bitcoin Energy Consumption Index Chart*, DIGICONOMIST, [https://perma.cc/99AZ-K737] (last visited Feb. 26, 2020).

[76] *See* LACITY, *supra* note 14, at 32-33.

[77] *See generally* Carol Goforth, *The Case for Preempting State Money Transmission Laws for Crypto-Based Businesses*, 73 ARK. L. REV. 301 (2020).

[78] Telephone Interview with Eamonn Maguire, Global Lead, Digital Ledger Services, KPMG (July 10, 2017).

Figure 2: Timeline of Notable Blockchain Innovations

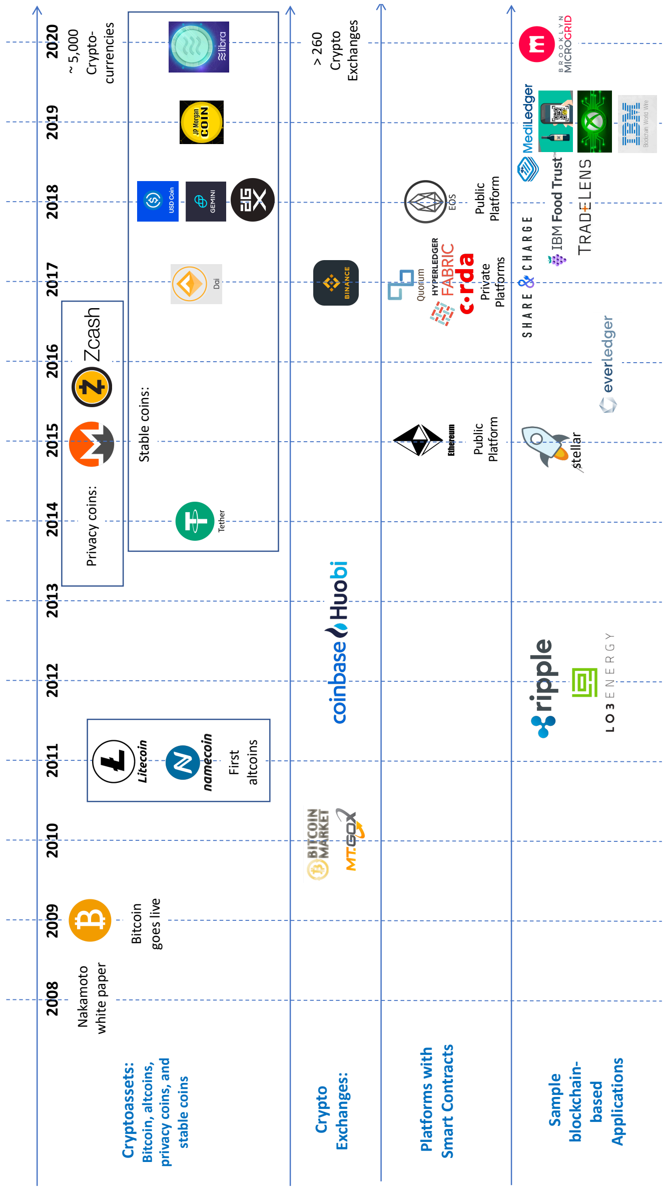


Table 1: Blockchain Innovations Since Bitcoin

Improvements compared to Bitcoin	**Altcoins**	**Privacy Coins**	**Stablecoins**	**Crypto-tokens**	**Exchanges**	**Public Platforms with Smart Contracts**	**Private Platforms with Smart Contracts**
Increased TPS	✓					✓	✓
Faster settlement times	✓					✓	✓
Increased anonymity		✓					
Increased confidentiality							✓
More stable store of value			✓				
Improved user access & experience					✓		
Decreased resource consumption						✓ *(some)*	✓
More functionality	✓			✓			✓
Higher regulatory compliance					✓ *(some)*		✓

A. Cryptoassets

Alternative coins. After Bitcoin, many alternative cryptocurrencies called "altcoins" were created, aiming to improve upon Bitcoin's protocol.[79] In 2011, the first altcoins—Namecoin and Litecoin—were created by copying and then

[79] *See* Larry D. Lahman, *Bitcoins, Blockchains and Satoshi Nakamoto*, 89 OKLA. B.J. 18, 19 (2018).

modifying the Bitcoin codebase.[80] ***Namecoin*** aimed to extend Bitcoin's functionality by storing more data in the transaction;[81] ***Litecoin*** aimed to speed settlement times by a factor of four.[82] By February 2020, there were more than 1,700 altcoins.[83]

Privacy coins. Several cryptocurrencies aim to increase anonymity by using advanced cryptography such as ring signatures to mask senders' addresses, stealth addresses to mask receivers' addresses, and zero-knowledge proofs.[84] "These methods allow only the parties to a particular transaction to decipher data and to access funds stored on the blockchain even when posted on a public blockchain."[85] For example, ***Monero,*** launched in 2014, is a cryptocurrency with increased data obfuscation compared to Bitcoin using ring signatures and stealth addresses.[86] ***Zcash*** is another major privacy coin, launched in

[80] James Frankenfield, *AltCoin*, INVESTOPEDIA, [https://perma.cc/C3LB-4J6R] (last updated Feb. 2, 2020).

[81] NAMECOIN, [https://perma.cc/QMJ5-JHDZ] (last visited Mar. 7, 2020).

[82] *About*, LITECOIN, [https://perma.cc/K2MA-ZZWE] (last visited Mar. 7, 2020).

[83] Frankenfield, *supra* note 80.

[84] *See* MARY LACITY ET AL., BLOCKCHAIN GOVERNANCE MODELS: INSIGHTS FOR ENTERPRISES 22, 45 (2019), [https://perma.cc/UPV9-KS5F].

> *Zero[-]knowledge proofs* are a method for one party . . . to verify possession of a piece of information to other parties . . . without revealing the information. As a simple example, suppose Alice wants to prove to Bob that she knows the exact number of jellybeans that fills a large barrel without telling Bob the exact number. What might Alice do to convince Bob that she knows the amount? Alice could instruct Bob to take any number of jellybeans out of the barrel after she leaves the room. Bob makes his choice. Alice reenters the room and Bob exits the room. Alice recounts the beans and compares the current count with the previous count to calculate exactly how many jellybeans (if any) Bob removed. When Bob returns, Alice tells Bob exactly how many jellybeans he took. If Bob thinks Alice made a lucky guess, rounds of the same choice could be made over and over again. Eventually, Bob will be convinced that Alice possesses the knowledge of the exact number of jellybeans without ever revealing the number. In blockchain applications, zero-knowledge proofs are used to guarantee that transactions are valid without revealing information about the sender, receiver, and/or transaction.

Id. at 46 (emphasis added).

[85] *Id.* at 22.

[86] *See Why Monero Is Different*, MONERO, [https://perma.cc/HN4N-ABB3] (last visited Mar. 8, 2020); *About Monero: A Brief History*, MONERO, [https://perma.cc/S2AC-77WX] (last visited Mar. 8, 2020). Monero uses the CryptoNote protocol, developed by Nicolas van Saberhagen, that defines an algorithm with increased data obfuscation compared to Bitcoin. *See generally* NICOLAS VAN SABERHAGEN, CRYPTONOTE V 2.0 (2013), [https://perma.cc/P8NG-7YSS]. With Monero, a recipient's address is only used once, so that the sender cannot trace subsequent transactions on the ledger. *Id.* at 6. When the recipient spends money out of that address (thus becoming a "sender" address in a subsequent transaction), the address gets hidden within a group signature. *Id.*

2016.[87] Designed by professors from Johns Hopkins, MIT, Technion, and Tel Aviv University, Zcash uses a cryptographic zero-knowledge proof which allows users to mask their addresses.[88]

Stablecoins. Several cryptocurrencies aim to create a more stable store of value compared to Bitcoin by pegging the coin to a stable asset outside the network, such as pegging a digital coin to a fiat currency or to a commodity like gold.[89] ***Tether*** was the first stablecoin, launched in 2014, by a company called Tether Limited.[90] Buyers exchange one U.S. dollar for one tether coin, with Tether Limited allegedly storing each U.S. dollar in a bank reserve.[91] Crypto traders use tethers to take advantage of the price arbitrage across cryptocurrency exchanges.[92] They can buy cryptocurrencies at a lower price with tethers on one exchange without having to first withdraw fiat currency from another exchange.[93]

Other notable stablecoins pegged to fiat currencies have launched since Tether, including USD Coin and Gemini in 2018, JPM Coin in 2019, and the proposed Libra coin, to be launched in 2020. The ***USD Coin***—created by Coinbase and Circle—launched the coin as part of a consortium, promising transparency over its U.S. dollar reserve management.[94] ***Gemini*** was founded

[87] ZCASH, [https://perma.cc/MS4V-PB3Z] (last visited Mar. 8, 2020).

[88] *Id.*

[89] BARRY EICHENGREEN, GLOBALIZING TITLE: A HISTORY OF THE INTERNATIONAL MONETARY SYSTEM 244 (3d ed. 2019).

[90] *See* James Frankenfield, *Tether (USDT)*, INVESTOPEDIA, [https://perma.cc/A9ZE-6TFW] (last updated June 25, 2020).

[91] *About Us*, TETHER, [https://perma.cc/RA7F-9FZN] (last visited Mar. 8, 2020). Tether Limited promised that at any time, a buyer could get its U.S. dollar back and the coin would be destroyed. *See* Paul Vigna, *Large Bitcoin Player Manipulated Price Sharply Higher, Study Says*, WALL ST. J. (Nov. 4, 2019), [https://perma.cc/4T38-RNZH]. In 2017, however, the company could not meet withdrawal demands and stands accused of currency manipulation and fraud. *Id.* It has never provided a legal audit, despite many promises to do so. *Id.* Despite the risks, nearly 75 percent of all bitcoin trades were facilitated by Tether in 2019. *Id.*

[92] *Tether Day Trading 2020*, DAY TRADING, [https://perma.cc/JZ52-L53Q] (last visited Mar. 6, 2020).

[93] *See id.*

[94] Coinbase, *Coinbase and Circle Announce the Launch of USDC – a Digital Dollar*, MEDIUM: THE COINBASE BLOG (Oct. 23, 2018), [https://perma.cc/JG6N-NA8N].

by Cameron and Tyler Winklevoss.[95] The Gemini coin is another 1-to-1 peg with the U.S. dollar.[96] JP Morgan uses its ***JPM Coin*** to facilitate institution-to-institution transfers.[97] It is also pegged to the U.S. dollar.[98] ***Libra***, the new token proposed by Facebook, will be pegged to a basket of fiat currencies (or perhaps to a local currency)[99] and will be managed by the Libra Association, a non-profit membership organization based in Switzerland.[100] The U.S. Congress has fiercely questioned Facebook founder Mark Zuckerberg and Facebook's Head of Calibra, David Marcus, over Libra.[101]

Besides pegging to fiat currencies, some stablecoins are pegged to commodities (e.g., ***DGX*** pegs one coin to one gram of gold)[102] or to other cryptocurrencies (e.g., ***Dai***, launched in 2017, is pegged to the U.S. dollar but is also backed by ***ether,*** Ethereum's cryptocurrency).[103] In the future, some cryptocurrencies may use algorithms to maintain a stable base price by automatically adjusting supply and demand.

Crypto-tokens. A cryptocurrency is one type of cryptoasset, one that aims to function as digital money.[104] Other cryptoassets are *digital tokens* that represent other types of assets

[95] Dante Alighieri Disparte, *Gemini: The Winklevoss Twins Break New Ground on Digital Trust*, FORBES (Jan. 29, 2019), [https://perma.cc/6FSM-VKXA].

[96] Jack Mathis, *Gemini's New USD Cryptocurrency Stablecoin: A Whitepaper Deep Dive*, CCN.COM (Sept. 12, 2018), [https://perma.cc/Y3KH-X53S].

[97] Jesse Damiani, *JPMorgan Announces 'JPM Coin,' a USD-Pegged Cryptocoin for Cross-Border Payments, Security, and More*, FORBES (Feb. 14, 2019), [https://perma.cc/7Y7B-W6J9].

[98] *Id.*

[99] Jonathan Shieber, *In a Big Reversal, Libra Reportedly Could Peg Its Cryptocurrencies to National Currencies*, TECHCRUNCH (Oct. 20, 2019), [https://perma.cc/SU8R-R46G].

[100] CleanApp, *Who Owns the Libra Association?*, MEDIUM: CRYPTO L. REV. (Oct. 24, 2019), [https://perma.cc/ZNZ8-3EH8].

[101] *Id.*; Charlie Wood, *Facebook's Blockchain Boss David Marcus Defends the Feasibility of Libra After a Quarter of Its Partners Drop Out*, BUS. INSIDER (Oct. 16, 2019), [https://perma.cc/3NZ6-8AFW].

[102] Lucent Exchange, *Gold-Backed Cryptocurrencies: Everything You Need to Know*, MEDIUM: CRYPTODIGEST (Sept. 12, 2019), [https://perma.cc/R7J5-LVPN].

[103] Tom Wilson, *Crypto Backed by Crypto: Dai Seeks to Change 'Stablecoin' Game*, REUTERS (Nov. 18, 2019), [https://perma.cc/G4TD-CPF4].

[104] Adam Haeems, *What Is a Crypto-Asset?*, MEDIUM: BABB (Apr. 27, 2018), [https://perma.cc/2UFM-R7UK].

besides money.[105] Crypto-tokens can be used to represent *fungible* (non-unique) assets, such as loyalty rewards and airline frequent flyer miles, in which one token is interchangeable with another.[106] Crypto-tokens can also be used to represent *non-fungible* (unique) assets, where the token represents a particular asset in the real world, creating what one may consider to be the digital twin.[107] For example, a unique token could be created to represent a particular diamond, a particular medical device, a particular plot of land, or a particular work of art. Crypto-tokens create new ways to track assets through supply chains (discussed below).

B. Cryptocurrency Exchanges

Initially, the only way to interact with the Bitcoin network was to become a miner or to manage one's own digital wallet, which requires significant technical skills. Many people saw the need for an exchange where users could easily buy and sell bitcoins with fiat currency. The first bitcoin exchange was ***Bitcoin Market***, launched in March 2010 by a Bitcoin Talk member using the pseudonym "dwdollar."[108] Jed McCaleb (born in Little Rock, Arkansas) soon after launched the most famous bitcoin exchange called ***Mt. Gox*** in 2010.[109] McCaleb sold the site to Mark Karpelès in 2011.[110] Early exchanges operated under

[105] **Tokenization vs. Encryption.** While encryption uses public-private key pairs to protect data, tokenization uses a token to protect data. *Tokenization vs. Encryption: Which One Is Better for Your Business?*, TOKENEX (July 19, 2013), [https://perma.cc/J4LF-3ANY] [hereinafter *Tokenization vs. Encryption*]. Specifically, "[t]okenization is the process of protecting sensitive data by replacing it with an algorithmically generated number called a token." *Tokenization Explained*, PARIVARTHAN (Jan. 13, 2019), **[https://perma.cc/7TKK-DPLH**]. To access the original data, an encryption solution decodes the encrypted data with a private key, whereas a tokenization solution exchanges the token for the sensitive data. *Tokenization vs. Encryption*, *supra*.

[106] Jake Frankenfield, *Crypto Tokens*, INVESTOPEDIA, [https://perma.cc/MN35-PW46] (last updated Apr. 3, 2018).

[107] Carol R. Goforth, *How Blockchain Could Increase the Need for and Availability of Contractual Ordering for Companies and Their Investors*, 94 N.D. L. REV. 1, 10 n.41 (2019).

[108] Nathaniel Whittemore & Clay Collins, *A History Of Crypto Exchanges: A Look At Our Industry's Most Powerful Institutions*, NOMICS (Nov. 14, 2019), [https://perma.cc/V9R5-ZQ5N].

[109] *See* V. Gerard Comizio, *Virtual Currencies: Growing Regulatory Framework and Challenges in the Emerging Fintech Ecosystem*, 21 N.C. BANKING INST. 131, 138 (2017).

[110] *Id.*

the radar of regulatory bodies, and many consumers were at risk for shams and heists.[111] Mt. Gox—and other exchanges that followed—were lucrative targets for hackers because exchanges controlled the users' private keys.[112] One of the largest heists occurred in August 2014 when 850,000 bitcoins, worth $387 million, were stolen from the wallets managed by Mt. Gox.[113]

Today, there are over 260 cryptocurrency exchanges, including ***Coinbase***, founded in 2012 in the United States;[114] ***Huobi***, founded in China in 2013;[115] and ***Binance***, founded in China in 2017, but which has since moved to Malta.[116] Many exchanges now comply with regulations, including Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.[117] For example, Coinbase had money transmitter licenses from 44 U.S. states and a New York State Virtual Currency License by 2019.[118] Coinbase also has commercial criminal insurance that is greater than the value of digital currency maintained in online storage (ninety-eight percent of the private keys are stored offline).[119] Increased compliance means a loss of user anonymity, a consequence that runs counter to the Cypherpunk values of the initial Bitcoin adopters.

[111] *See id.* at 140.

[112] *See id.*

[113] *Japan Arrests MtGox Bitcoin Head Over Missing $387m*, ALJAZEERA (Aug. 1, 2015), [https://perma.cc/SX42-XAEW].

[114] Trautman & Harrell, *supra* note 55, at 1058.

[115] Eunice Yoon, *Behind China's Love Affair with Bitcoin*, CNBC (Dec. 20, 2013), [https://perma.cc/C8AE-RKA4].

[116] *See* Priyeshu Garg, *Binance Set to Move to Malta with Their Prime Minister Welcoming*, BLOCKONOMI (Mar. 31, 2018), [https://perma.cc/UAJ4-445M]. Coin.Market tracks cryptocurrency exchanges on its website. *See Top Cryptocurrency Exchanges List*, COIN.MARKET, [https://perma.cc/VR6N-L2HZ] (last visited Feb. 27, 2020).

[117] *See* Craig Adeyanju, *What Crypto Exchanges Do to Comply with KYC, AML and CFT Regulations*, COIN TEL. (May 17, 2019), [https://perma.cc/KDN8-JYTJ].

[118] *See Licenses*, COINBASE: LEGAL, [https://perma.cc/CG3M-YHBH] (last visited Feb. 27, 2020) (not licensed in California, Hawaii, Indiana, Massachusetts, Missouri, or Wisconsin); Virtual Currency License, N.Y. DEPT. FIN. SERVS. (Jan. 17, 2017), [https://perma.cc/RCP6-EKGH].

[119] *See* Carol Goforth, *The Lawyer's Cryptionary: A Resource for Talking to Clients About Crypto-Transactions*, 41 CAMPBELL L. REV. 47, 67 (2019); *Security*, COINBASE, [https://perma.cc/5X5T-2EWN] (last visited Feb. 27, 2020).

C. Public Platforms with Smart Contracts

Ethereum was the first blockchain platform designed to overcome Bitcoin's limited functionality as a single application that only tracks payments.[120] Launched in 2015, Ethereum uses *smart contracts* so that developers can build decentralized applications on the platform.[121] A smart contract, a concept developed by Nick Szabo in 1994, is "a piece of software that stores rules of negotiating the terms of a contract, automatically verifies [the contract,] and [then] executes the terms."[122] Anything that can be coded within the rules of logic can be programmed into a smart contract that is secured, automatically executed, and permanently stored on a blockchain.[123] (The legality and limitations of smart contacts are addressed in other papers in this issue.) Smart contracts are commonly used to automatically move value around accounts based on agreed upon conditions.[124] Use cases include lotteries; voting; crowdsourcing; asset sharing; asset tracking; identity management; bidding; rating; gaming; and gambling.[125] As of January 2020, there were

[120] *See* Chris Brummer & Yesha Yadav, *Fintech and Innovation Trilemma*, 107 GEO. L.J. 235, 272 (2019). Vitalik Buterin wrote the 2015 Ethereum white paper when he was only 19 years old. Orna Rabinovich-Einy & Ethan Katsh, *Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution*, 2019 J. DISP. RESOL. 47, 51 (2019). Buterin, Gavin Wood, and Jeffrey Wilcke began work on Ethereum by launching The Ethereum Foundation, a non-profit organization based in Switzerland. *History of Ethereum*, ETHEREUM HOMESTEAD, [https://perma.cc/M8XD-D3PB] (last visited Mar. 16, 2020).

[121] *See* Rabinovich-Einy & Katsh, *supra* note 120, at 51.

[122] MJ Kim, *The Future of Blockchain Technology: Smart Contracts*, TECHNODE (Nov. 14, 2016), [https://perma.cc/63RY-GZE6].

[123] Tsui S. Ng, *Blockchain and Beyond: Smart Contracts*, BUS. L. TODAY, Sept. 2017, at 1.

[124] *Id.* at 1-2.

[125] In general, smart contracts can be classified as either 'deterministic' or 'non-deterministic.'

A deterministic smart contract means that [terms of the agreement] . . . can execute autonomously without the need for any outside information. A lottery is a good example. A smart contract for a lottery could define the time period when people could send value to the smart contract account to 'buy' lottery tickets. The smart contract could specify how the winning lottery number would be selected, perhaps by taking the hash of a randomly selected block and awarding the account that is closest to that number as the winner. The smart contract could automatically transfer the money to the winning account. If the lottery was regulated, the smart contract could be coded to deduct taxes.

A non-deterministic smart contract means that outside information is needed to execute the contract. Horse race betting is an example. Like a lottery, a smart contract for horse race betting could be coded to define when people could send value to the smart contract account nearly 5,000 smart contracts deployed on Ethereum, although many of them are inactive.[126] Because Ethereum uses the same consensus mechanism as Bitcoin (called a "proof-of-work"), it improved but still has some of the same limitations as Bitcoin as far as resource consumption[127] and few TPS (about fifteen TPS).[128]

EOS was developed to keep all of the advantages of a public blockchain platform like Ethereum—open, secure, and decentralized—but without the latency, scalability, and resource intensity. Launched in 2018, anyone can transact and build apps using smart contracts on EOS.[129] Blocks are produced about every 500 milliseconds due to a faster consensus mechanism called *Delegated Proof-of-Stake (DPoS)*.[130] Rather than having miners compete, EOS users stake their EOS token to elect twenty-one block producers, with each of the twenty-one producers getting a turn to create the next block.[131] Block producers are rewarded with the issuance of new EOS tokens.[132]

D. Private Platforms with Smart Contracts

Traditional enterprises mostly ignored Bitcoin for the first few years, but enterprises began to explore the strategic

to place their bets. The rules for adjusting odds could also be mechanized in the contract. However, smart contracts for horse racing cannot run autonomously; they need outsiders (called '***oracles***') to inform the smart contract of the winning animal. Unlike trusted third parties, an oracle in this scenario does not control the funds, the smart contract does.

LACITY, *supra* note 14, at 60 (emphasis added).

[126] *DApp Statistics: Platforms*, STATE OF THE DAPPS, [https://perma.cc/4H83-GCEJ] (last visited Mar. 5, 2020).

[127] *Ethereum Energy Consumption Index (Beta)*, DIGICONOMIST, [https://perma.cc/4WZ4-G5W4] (last visited Mar. 5, 2020). Digiconomist, a site that tracks Ethereum's energy consumption, reports that a single transaction consumes enough electrical energy to power an average U.S. household for 1.2 days. *Id.*

[128] Abhimanyu Krishnan, *Vitalik on Ethereum: "Right Now It Can Process 15 Transactions Per Second. Really, We Need 100,000,"* INVEST IN BLOCKCHAIN (Mar. 21, 2019), [https://perma.cc/8LZK-JGRF].

[129] *About Us*, EOISO, [https://perma.cc/6YCU-YVNF] (last visited Mar. 5, 2020). *See Why Build on EOSIO?*, EOSIO, [https://perma.cc/X6C8-ANUP] (last visited Mar. 5, 2020).

[130] *Coins*, CRYPTOSLATE, [https://perma.cc/66CV-B9D2] (last visited Mar. 5, 2020).

[131] *See Block Producers*, BLOKS.IO, [https://perma.cc/79YT-B6RW] (last visited Mar. 5, 2020).

[132] Chrisjan Pauw, *EOS BP, Explained*, BEQUANT, PRO (May 23, 2019), [https://perma.cc/NV8Z-VB7C].

opportunities and threats posed by Bitcoin and related blockchain technologies by 2014 with the formation of R3, a consortium of global banks based in New York City.[133] Additional consortia, working groups, and non-profits began to define blockchain standards and develop code bases for enterprise applications.[134] There are nearly 103 blockchain consortia of significance.[135] In 2017, three significant code bases for private blockchains were released as open source software. JP Morgan released ***Quorum***, a private version of Ethereum;[136] R3 released ***Corda***, a peer-to-peer code base aimed at enterprises that want strict data and transaction privacy;[137] and the HyperLedger Project released ***Fabric***, much of whose code was donated by IBM.[138] These ***permissioned blockchains***—where joining the network is by invitation-only—use some form of Practical Byzantine Fault Tolerance (PBFT) as a consensus protocol.[139] With PBFT, nodes need permission to serve as validator nodes, forming a member list, which provides traditional enterprises with the confidentiality and control they need.[140] So, what do enterprises actually build with these blockchain innovations? The next section covers use case examples.

[133] *Blockchain Applications in Banking*, DELOITTE, [https://perma.cc/5DCJ-2SZB] (last visited Mar. 5, 2020).

[134] LACITY, *supra* note 14, at 29.

[135] *Top Four Enterprise Blockchain Consortia Trends*, ESG INTELLIGENCE (June 19, 2019), [https://perma.cc/79AD-XCZK].

[136] Robert Hackett, *Why J.P. Morgan Chase Is Building a Blockchain on Ethereum*, FORTUNE (Oct. 4, 2016), [https://perma.cc/3D8F-Z9HZ].

[137] *The Network*, CORDA, [https://perma.cc/RZW2-U3DT] (last visited Mar. 2, 2020); RICHARD GENDAL BROWN, THE CORDA PLATFORM: AN INTRODUCTION 6 (2018), [https://perma.cc/G8J9-A39H].

[138] BRENN HILL ET AL., BLOCKCHAIN DEVELOPER'S GUIDE 139 (2018).

[139] Libo Feng et al., *Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain*, 8 APPLIED SCIS. 1, 1 (2018).

[140] With PBFT, a node from the member list is selected as leader for the next round of validation. Brian Curran, *What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide*, BLOCKONOMI (May 11, 2018), [https://perma.cc/9J4F-3AYM]. A client node sends a request to the leader node to validate a transaction. *Id.* The leader node multicasts the request to all the other authorized nodes. *Id.* The authorized nodes execute the request independently and then send to each other and reply to the client. *Id.* The client waits for a certain percentage of replies to confirm validation, typically waiting for 2/3 of the nodes to agree. *Id.* The leader node changes for the next round. *Id.*

IV. BLOCKCHAIN-BASED APPLICATION EXAMPLES

"*Distributed ledger technology will significantly increase transparency between market participants*." –- World Economic Forum Report.[141]

Bitcoin has served as our most visible example of a functioning blockchain application. Beyond payments, there are many other blockchain use cases. Here, we examine a small subset of blockchain applications from three sectors—financial services, energy, and supply chain. For traditional enterprises, blockchain applications promise a significant amount of business value, like transacting directly with trading partners, eliminating the need for reconciliations, instantly tracking assets, providing robust data provenance, settling transactions quickly and cheaply, and enabling a security model that is fault tolerant, resilient, and available.[142] However, the technology is still maturing, standards are still being established, and concerns over regulatory uncertainty still overshadow many c-suite discussions.

A. Financial Services

Enterprises in the financial services sector have been among the first players to recognize the threats and opportunities afforded by Bitcoin's underlying blockchain technology. Incumbent enterprises, including banks like Barclays, State Street, and Wells Fargo, that have been in continuous operation for hundreds of years, were among the early explorers of blockchain technologies.[143] Over 250 FinTechs also have entered

[141] WORLD ECON. FORUM, THE FUTURE OF FINANCIAL INFRASTRUCTURE: AN AMBITIOUS LOOK AT HOW BLOCKCHAIN CAN RESHAPE FINANCIAL SERVICES 26 (2016), [https://perma.cc/XWR2-C6ME].

[142] LACITY, *supra* note 14, at 166.

[143] *Our History*, BARCLAYS, [https://perma.cc/TE6D-NYVH] (last visited Mar. 4, 2020); *225 Years and We're Just Getting Started*, STATE ST., [https://perma.cc/UB83-2PFT] (last visited Mar. 4, 2020); *History of Wells Fargo*, WELLS FARGO, [https://perma.cc/GEE7-FEUH] (last visited Mar. 4, 2020); *See* Hugh Harsono, *Bank-Based Blockchain Projects Are Going to Transform the Financial Services Industry*, TECHCRUNCH (Jan. 28, 2018), [https://perma.cc/9348-6CUQ].

the space, such as Ripple and Stellar.[144] **Ripple,** founded in 2012 by Chris Larsen and Jed McCaleb, aimed to overcome Bitcoin's inability to trade other currencies, relatively slow settlement times, and massive electricity consumption, while still being inexpensive, transparent, private, and secure.[145] It is a universal fiat currency exchange, where its digital assets (called "ripples") serve as a bridge currency.[146] Ripple works with established institutions, a direction with which McCaleb and other Cypherpunks disagreed.[147] McCaleb and Joyce Kim launched **Stellar** in 2015 to focus on a mission of financial inclusion.[148] Stellar is based on Ripple's code, but with changes to its protocol.[149] Stellar's network for global payments settles transactions in two to five seconds.[150] Stellar can process over 1,000 operations per second.[151] It is used by IBM and Deloitte for cross border payment applications, mostly in the Pacific region.[152]

B. Energy

The world over, large electric utilities are the primary suppliers of electricity. These large, centrally-managed organizations have been operating with the same business models for over 100 years and they are markedly energy inefficient.[153] Most of the electric energy generated by utilities is wasted through the processes of conversion, transmission, and

[144] *The Fintech 250: The Top Fintech Startups of 2018*, CB INSIGHTS (Oct. 22, 2018), [https://perma.cc/SZ9F-B6GS]; *Our Company*, RIPPLE, [https://perma.cc/3GRU-YZ93] (last visited Mar. 4, 2020); *Intro to Stellar*, STELLAR, [https://perma.cc/7C47-E78Q] (last visited Mar. 4, 2020).

[145] LACITY, *supra* note 14, at 81-82.

[146] *XRP*, XRP LEDGER, [https://perma.cc/9SBP-6E2M] (last visited Mar. 5, 2020); LACITY, *supra* note 14, at 81-83.

[147] *See The Ripple Story*, BITMEX (Feb. 6, 2018), [https://perma.cc/VG95-CFKE].

[148] LACITY, *supra* note 14, at 87.

[149] *Id.* at 88-89.

[150] *Id.* at 87; Siddharth Sitpure, *Stellar Lumens Blockchain – Tech and Business Overview*, MEDIUM (Jan. 29, 2018), [https://perma.cc/XG8M-YXF7].

[151] LACITY, *supra* note 14, at 87.

[152] *Id.* at 87-88.

[153] According to Lawrence Livermore National Laboratory, of the 101.2 quadrillion BTUs (quads) of energy produced in the U.S. in 2018, 67.7 percent, or 68.5 quads, was waste or "rejected energy." *See* Anne M. Stark, *U.S. Energy Use Rises to Highest Level Ever*, LAWRENCE LIVERMORE NAT'L LAB. (Apr. 11, 2018), [https://perma.cc/8LDW-ZB6J].

consumption.[154] Large petroleum companies are the primary suppliers for gasoline used to fuel vehicles.[155] Consumers are increasingly concerned about the pollution, waste, expense, and lack of control over their energy supplies. Consequently, many households have installed solar panels on their properties, and many people now drive battery-operated cars. Several blockchain applications have been developed to help consumers share their energy-efficient resources with neighbors. For example, ***LO3 Energy***—founded in 2012 in Brooklyn, New York—built a blockchain technology platform to create peer-to-peer markets to enable neighbors to buy and sell their locally produced energy credits.[156] The LO3 "Brooklyn Microgrid" has been run as a test project since 2016; however, New York State only granted permission in late 2019 to operate the microgrid in a regulatory sandbox.[157] Innogy, a recently purchased subsidiary of the German-based electric utility E.ON, was established in 2016 by E.ON competitor RWE to focus on renewable energy solutions.[158] One of its projects is ***Share&Charge***, a startup venture developed with Slock.It, that went live in 2017, to create a peer-to-peer

[154] Conversion waste generally happens when burning fossil fuels to produce energy; however, while more efficient, converting renewable resources to electricity also produces small amounts of waste. *See 6 Ways to Cut Big Waste in Our Energy System, Switch to Renewable Energy*, ENVTL. DEF. FUND, [https://perma.cc/5R87-MP87] (discussing the amount of waste loss when converting fossil fuels to energy, and how that waste could be minimized by using renewable sources). Transmission waste occurs when pushing electricity over long distances. *See Frequently Asked Questions, How Much Electricity Is Lost in Electricity Transmission and Distribution in the United States?*, U.S. ENERGY INFO. ADMIN. (Dec. 31, 2019), [https://perma.cc/6C6Z-SU5S]. About 5 percent of electric energy is lost in transit annually. *Id.* Consumption waste occurs when consumer appliances lose electric energy to heat, for example. *The Brooklyn Microgrid: Blockchain-Enabled Community Power*, POWER TECH. (Apr. 11, 2017), [https://perma.cc/2B6J-NLXM] [hereinafter *The Brooklyn Microgrid*].

[155] *Gasoline Explained: Where Our Gasoline Comes From*, U.S. ENERGY & INFO. ADMIN. (Dec. 3, 2019), [https://perma.cc/DZ8E-YCJ2].

[156] *The Brooklyn Microgrid*, *supra* note 154.

[157] *See* Peter Maloney, *New York Approves Regulatory Sandbox for Brooklyn Microgrid*, MICROGRID KNOWLEDGE (Dec. 30, 2019), [https://perma.cc/S4PH-HA2L] (discussing a campaign in October 2019 to petition the State of New York to allow deployment of the Brooklyn Microgrid Sandbox, which was recently approved and will launch in 2020).

[158] Andrea Biancardi & Matteo di Castelnuovo, *A New Paradigm in the Electricity Sector: Key Trends and Stock Performance of European Utilities*, 9 EUR. ENERGY & CLIMATE J. 31, 47 (2020); *see also* LACITY, *supra* note 14, at 106.

marketplace for electric car charging.[159] Share&Charge aims to expand Germany's infrastructure by enabling 60,000 private charging stations to join Germany's 6,500 public charging stations.[160]

C. Supply Chains

Today's global supply chains are a complex web of trading partners and trusted third parties. While manufacturers, exporters, couriers, freight forwarders, customs, inspectors, exporters, shippers, and importers are all moving physical goods, they are also creating data about those movements with bills of lading, certifications, consignments, customs forms, inspections data, insurance forms, invoices, lines of credit, purchase orders, shipping manifestos, and receiving documents, to name a few. As a consequence of so many players with their own centralized systems and so much paperwork, assets get lost, shipping containers get delayed in ports because of missing paperwork, inconsistent records across trading partners trigger disputes, and counterfeit products slip through supply chains, to name but a few challenges. Blockchains have the potential to solve many of these challenges.

By 2016, enterprises began moving blockchain applications for asset tracking into production. For example, ***Everledger*** tracks diamonds from diamond mines to retail stores; over 1 million diamonds were represented on the ledger as of March 2017.[161] Everledger has since expanded its business model to track and trace other valuable assets such as art, wine, and antiquities.[162] ***TradeLens*** tracks shipping containers.[163] ***MediLedger*** tracks pharmaceuticals in the U.S. supply chain.[164] The ***IBM Food Trust*** traces food from farm and fishery to retail

[159] Steven Tual, *Share&Charge Launches Its Mobile App, On-Boards over 1,000 Charging Stations on the Blockchain*, MEDIUM: SLOCK.IT BLOG (May 1, 2017), [https://perma.cc/QV2E-5K8G].

[160] LACITY, *supra* note 14, at 106.

[161] *Id.* at 109-10.

[162] *Id.* at 110.

[163] LACITY ET AL., *supra* note 84, at 11.

[164] *Id.*

stores.[165] ***WineChain*** tracks and authenticates wine bottles.[166] And ***Microsoft*** uses a blockchain application to track royalty payments owed to Xbox application owners.[167] While none of these applications are fully scaled yet, they demonstrate the possibilities of getting business value from blockchain technologies.[168]

Beyond these applications, other innovations are particularly relevant for legal professionals to understand. Namely, the new fundraising models that accompanied many blockchain projects.

V. New Fundraising Models

"*A major reason attributed to the success of fundraising through token offerings is the liquidity provided through the reduced trading friction enabled through the blockchain.*" — Jonathan Chester, Founder & President of Bitwage[169]

Nakamoto launched Bitcoin without raising funds.[170] Other proposed blockchain projects, however, sought to raise funds using new financing mechanisms such as Initial Coin Offerings (ICOs), Security Token Offerings (STOs), and Initial Exchange Offerings (IEOs).[171]

[165] *See* Rachel Wolfson, *Understanding How IBM and Others Use Blockchain Technology to Track Global Food Supply Chain*, FORBES (Jul. 11, 2018), [https://perma.cc/GB3B-KYVJ] (discussing IBM Food Trust's use of blockchain technology to track dozens of food items, such as vegetables and fish, to help retailers identify contamination).

[166] LACITY ET AL., *supra* note 84, at 41.

[167] *Xbox Game Publishers Access Royalties Statements Even Faster Now That Microsoft Uses Azure Blockchain Service*, MICROSOFT (May 2, 2019), [https://perma.cc/W7HL-YTH6].

[168] *See* LACITY ET AL., *supra* note 84, at 13 (comparing organizational mission statements regarding business benefits of blockchain).

[169] Jonathan Chester, *How to Run A Successful Security Token Offering in Compliance with New SEC Guidance*, FORBES (Apr. 15, 2019), [https://perma.cc/7E4V-K5AJ].

[170] *See* Nathaniel Popper, *What Is Bitcoin, and How Does It Work?*, N.Y. TIMES (Oct. 1, 2017), [https://perma.cc/53DT-ZS5Y] (claiming Nakamoto created rules for Bitcoin and simply released the software to the world).

[171] Michael Mendelson, *From Initial Coin Offerings to Security Tokens: A U.S. Federal Securities Law Analysis*, 22 STAN. TECH. L. REV. 52, 61, 63 (2019); *What Is a Security Token Offering (STO)?*, CRYPTONEWS, [https://perma.cc/7KLE-J4G2] (last visited Feb. 28, 2020); Gertrude Chavez-Dreyfuss, *Explainer: Initial Exchange Offerings Flourish in Crypto Market*, REUTERS (June 20, 2019), [https://perma.cc/F5WC-EDLP].

A. Initial Coin Offerings

With an ICO, people exchange money (typically bitcoins) for new coins released by the project's founders.[172] ***Mastercoin*** was the first ICO, which raised $5.5 million in 2014.[173] Ethereum was the second ICO, raising $16 million in 2014.[174] With an ICO, projects raise cash by launching a new coin or token, i.e., a new cryptocurrency.[175] Investors buy the coins (but not shares in a company)—which bypassed many onerous regulations until regulators like the SEC finally investigated their legality.[176] ICOs raised about $14 billion dollars from 2014 to 2018.[177] However, when regulators around the world started intervening, the market fell precipitously.[178] In 2018, ICOs raised $7.8 billion worldwide compared to $370 million in 2019.[179] While ICOs fell in popularity, two new funding models rose in popularity: STOs and IEOs.[180]

B. Security Token Offerings

STOs are legally compliant, licensed ICOs which protect investors against fraud.[181] The value of the token is based on the company's valuation.[182] STOs are only available for accredited investors.[183] In 2018, 119 security tokens were launched by capital investor firms, raising over $17 billion, with the majority

[172] LACITY ET AL., *supra* note 84, at 29.

[173] *Id.*

[174] *Id.*

[175] Jay Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. SEC. & EXCHANGE COMM'N (Dec. 11, 2017), [https://perma.cc/FZ6Z-5KMG].

[176] LACITY ET AL., *supra* note 84, at 29.

[177] Billy Bambrough, *A Gold Standard of ICOs Is Needed – But It Won't Be Easy*, FORBES (July 4, 2018), [https://perma.cc/XJ6E-52C5].

[178] *See* Jeff Kauflin, *Security Tokens Were Supposed to Transform Crypto. So Far, They've Flopped.*, FORBES (May 21, 2019), [https://perma.cc/4L4X-BGQ3].

[179] *Funds Raised in 2018*, ICODATA.IO, [https://perma.cc/MKG8-EACW] (last visited Feb. 25, 2020); *Funds Raised in 2019*, ICODATA.IO, [https://perma.cc/MGN9-ECV7] (last visited Feb. 25, 2020).

[180] *What Is a Security Token Offering (STO)?*, *supra* note 171; Chavez-Dreyfuss, *supra* note 171.

[181] *What Is a Security Token Offering (STO)?*, *supra* note 171.

[182] Roger Aitken, *Bitcoin Aside, After ICO's Are STO's the Everyman's IPO?*, FORBES (Feb. 18, 2019), [https://perma.cc/U2M5-ESPS].

[183] Chrisjan Pauw, *What Is an STO, Explained*, COINTELEGRAPH (Feb. 21, 2019), [https://perma.cc/44GC-U32H].

of that in the last quarter of the year.[184] A number of STO standards are emerging, which will make it easier for investors to liquidate.[185]

C. Initial Exchange Offerings

IEOs are a funding round conducted on a cryptocurrency exchange. Investors fund their exchange wallets with coins and use those funds to buy the fundraising company's tokens.[186] Many exchanges now comply with AML and KYC regulations on customers and also vet the fundraisers, making IEO investments less risky than ICOs.[187] Binance, Huobi, OKEX, KuCoin, and BitMax are examples of exchanges with IEO services.[188]

[184] *See* Tim Fries, *STOs v. ICOs: What's the Difference?*, THE TOKENIST (Sept. 15, 2019), [https://perma.cc/4X9M-4GBK].

[185] ERC-20, ST-20, R-Token, ERC-1400, and ERC-1404 are token standards gaining acceptance. Jonathan Chester, *How to Run a Successful Security Token Offering in Compliance with New SEC Guidance*, FORBES (Apr. 15, 2019), [https://perma.cc/R2EZ-FLX9].

[186] *See* Andrey Sergeenkov, *Initial Exchange Offering—The Next Popular Fundraising Scheme in Crypto?,* HACKERNOON (Mar. 27, 2019), [https://perma.cc/3GAT-YN28].

[187] *Id.*

[188] Thomas Winslet, *Top 3 Initial Exchange Offerings (IEOs) to Watch in the Crypto Market*, THE DAILY HODL (Apr. 11, 2019), [https://perma.cc/7M57-EGWE]; Artur Boystov, *Ultimate List of IEO Platforms/Launchpads: Top 15+ Exchanges*, HACKERNOON (Apr. 4, 2019), [https://perma.cc/JX3Z-58E4].

Table 2: Comparison of Crypto Funding Models

Attributes	**Initial Coin Offering (ICO)**	**Security Token Offering (STO)**	**Initial Exchange Offerings (IEO)**
Investor accessibility	Open to anyone	Accredited investors only	Open to anyone with an account on the exchange
Regulatory compliance	Low	Fully compliant	Higher for exchanges with AML and KYC compliance
Investor risk disclosure	Low	High	Medium
Ease of setting up for the fundraiser	High	Low	Medium
Cost of setting up for the fundraiser	Low	High	Medium

VI. WHY THE "INTERNET OF VALUE" NEEDS LEGAL PRACTITIONERS

"2020 will be the year of regulatory clarification and broader enterprise adoption. . . . [P]ractitioners will need to continuously monitor this fast-moving aspect of the blockchain space" — Accounting Today[189]

While the innovations discussed in this paper—altcoins, privacy coins, stablecoins, crypto-tokens, exchanges, platforms and smart contracts, ICOs, STOs, and IEOs—cover some of the

[189] Sean Stein Smith et al., *5 Blockchain Trends to Watch in 2020*, ACCOUNTING TODAY, [https://perma.cc/WE8D-MXYJ] (last visited Feb. 26, 2020).

major technical and financial innovations since Bitcoin, the coverage is not exhaustive. There are projects addressing *interoperability* to allow digital assets to be processed across blockchains;[190] *quantum-proofing cryptography* to prevent future quantum computers from guessing private keys;[191] new consensus algorithms besides those discussed above (proof-of-work; delegated proof-of-stake, and practical byzantine fault tolerance);[192] and *scalability* projects to increase transactions per second.[193] As of January 2020, over 4,900 cryptocurrencies exist, with a combined market capitalization of $180 billion.[194] Thousands of enterprise applications have been built and tested, with hundreds now moving into production.[195] No doubt, blockchain technologies are enabling an "Internet of Value." However, ***legal practitioners are needed to help influence sound regulations and policies that protect the environment, investors, and consumers while still fostering innovation***.

For the United States, the stakes cannot be higher. Other countries—particularly China—are ahead of the United States in

[190] Stephen O'Neal, *Blockchain Interpolarity, Explained*, COINTELEGRAPH (Sept. 5, 2019), [https://perma.cc/ZD7A-GYM5].

[191] Ambika Choudury, *Quantum-Proof Cryptography & Its Role in Security*, ANALYTICS INDIA MAGAZINE, [https://perma.cc/8452-YMLZ] (last visited Feb. 26, 2020).

[192] ***Proof-of-Stake (PoS)*** is a consensus protocol created by Sunny King and Scott Nadal in a 2012 white paper. *See* SUNNY KING & SCOTT NADAL, PPCOIN: PEER-TO-PEER CRYPTO-CURRENCY WITH PROOF-OF-STAKE (2012), [https://perma.cc/CS66-MN7C]. Instead of "mining" for coins, the protocol selects a member to "forge" new currency as a reward for validating the transactions and creating the next block. *Id.* Essentially, the selected member node is awarded a transaction fee. *Id.* It is called a "Proof-of-Stake" because the members with the highest "stake" (i.e., those who have the largest account balances and hold the coins the longest periods of time) are giving priority in the selection algorithm. *Id.* Proof-of-Stake uses much less energy than Proof-of-Work and settles transactions faster than Proof-of-Work. *Id.* However, critics claim it is less secure than Proof-of-Work because people with small stakes have little to lose by voting for multiple blockchain histories, which leads to consensus never resolving. *Id.* Other consensus protocols include ***Proof-of-Authority (PoA), Proof-of-Capacity (PoC), and Proof-of-Elapse-Time (PoET).*** *See Different Blockchain Consensus Mechanisms*, HACKERNOON (Nov. 10, 2018), [https://perma.cc/GS54-4YUT].

[193] Connor Blenkinsop, *Scalability on Blockchain: Is There a Solution?*, COINTELEGRAPH (Sept. 27, 2019), [https://perma.cc/FA2N-DT7Y].

[194] Horus Hughes, *4 Things You Must Know Before Trading Bitcoin and Cryptocurrency*, COINTELEGRAPH (Dec. 16, 2019), [https://perma.cc/S4XQ-YRPT]; Aaron Hankin, *Crypto Market Value Surges $30 Billion in 36 Hours; Bitcoin Cash Doubles in Value*, MARKETWATCH (Apr. 3, 2019), [https://perma.cc/5Q52-38T7].

[195] *Guide to the Rise of Cryptocurrency, Digital Currency and Bitcoin*, NE. UNIV. D'AMORE-MCKIM SCH. OF BUS., [https://perma.cc/P3PE-RSRJ] (last visited Feb. 26, 2020).

developing *sovereign cryptocurrencies* and obtaining blockchain-related patents. China, for example, will likely launch a digital currency to commercial banks and payment networks like WeChat Pay and Alibaba's Alipay in early 2020.[196] Our research at the Blockchain Center of Excellence at the University of Arkansas found that China is ahead of the United States on granting blockchain related patents.[197] China's patent office, the National Intellectual Property Administration (CNIPA), has awarded 2,218 blockchain patents compared to 227 by the U.S. Patent and Trademark Office (USPTO).[198] Legal practitioners need us to help narrow the gap. We hope the papers in this special issue of the *Arkansas Law Review* will inspire legal practitioners to better understand and influence public policy.

[196] Yen Nee Lee, *China Could Launch Its Own Digital Currency in the Next 2-3 Months, Predicts Investor*, CNBC (Nov. 11, 2019), [https://perma.cc/7NPM-NGVF].

[197] Mary Lacity et al., *US and China Battle for Blockchain Dominance*, COINTELEGRAPH (Nov. 29, 2019), [https://perma.cc/8W7K-GMQJ].

[198] *Id.*