

June 2023

The Aim to Decentralize Economic Systems With Blockchains and Crypto

Mary Lacity

The Sam M. Walton College of Business at the University of Arkansas

Follow this and additional works at: <https://scholarworks.uark.edu/alr>



Part of the [Other Computer Engineering Commons](#), [Software Engineering Commons](#), and the [Systems Architecture Commons](#)

Recommended Citation

Mary Lacity, *The Aim to Decentralize Economic Systems With Blockchains and Crypto*, 76 Ark. L. Rev. (2023).

Available at: <https://scholarworks.uark.edu/alr/vol76/iss2/5>

This Article is brought to you for free and open access by the School of Law at ScholarWorks@UARK. It has been accepted for inclusion in Arkansas Law Review by an authorized editor of ScholarWorks@UARK. For more information, please contact scholar@uark.edu.

THE AIM TO DECENTRALIZE ECONOMIC SYSTEMS WITH BLOCKCHAINS AND CRYPTO

Mary Lacity*

I. INTRODUCTION¹

As an information systems (“IS”) professor, I wrote this Article for legal professionals new to blockchains² and crypto.³ This target audience likely is most interested in crypto for its legal implications—depending on whether it functions as currencies, securities, commodities, or properties; however, legal professionals also need to understand crypto’s origin, how transactions work, and how they are governed. Let’s begin the learning journey with the reason blockchains and crypto were invented:

The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat

* **Dr. Mary C. Lacity** is the David D. Glass Chair and Distinguished Professor of Information Systems in the Sam M. Walton College of Business at the University of Arkansas. She was previously Curators’ Distinguished Professor at the University of Missouri. She has held visiting positions at MIT, the London School of Economics, Washington University, and Oxford University. She has published more than 30 books, most recently co-authoring *Blockchain Fundamentals for the Web 3.0* (2022) with Steve Lupien and co-editing *Blockchains and the Token Economy* (2022) with Horst Treiblmaier.

1. An earlier version of the paper appeared in Mary Lacity, *Crypto and Blockchain Fundamentals*, 73 ARK. L. REV. 363 (2020). The content has been significantly updated with new material, including select excerpts from MARY C. LACITY & STEVEN C. LUPIEN, *BLOCKCHAIN FUNDAMENTALS FOR WEB 3.0* (2022).

2. **Blockchain:** The term “blockchain” is used several ways. Sometimes it 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. See *infra* notes 17-18 and accompanying text.

3. **Crypto:** Instead of “crypto,” some people use the umbrella terms “cryptoassets,” “digital assets,” or “crypto-tokens.” At this stage of development, there is no definitive nomenclature. See *Crypto Glossary*, COINMARKETCAP, [<https://perma.cc/MGE6-JGC6>] (last visited Feb. 26, 2023).

currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. —**Satoshi Nakamoto, inventor of Bitcoin**⁴

Bitcoin was the first fully decentralized blockchain application for payments.⁵ Satoshi Nakamoto and other cypherpunks⁶ were wary of governments and banks mediating our economic activities, charging us high fees, invading our privacy, monitoring our behaviors, exposing us to fraud and identity theft, and controlling access to our financial assets.⁷ Cypherpunks believe people must come together and create computer systems that allow anonymous transactions to take place.⁸

In addition to the distrust of governments and banks, many people also are wary of the giant tech companies that own and monetize our data. Billions of individuals trade their data for free services without realizing the extent to which they are being monitored and manipulated. Companies' algorithms watch and process what we do to make predictions on our behaviors, such as what we will buy and how we might vote, and sell this knowledge to advertisers.⁹ Shoshana Zuboff, Harvard Business School professor, coined the term “surveillance capitalism” to describe how companies use our data for the sole purpose of making a profit.¹⁰ She believes that surveillance capitalism is an existential threat to our human liberty, autonomy, and well-being.¹¹

Blockchains, crypto, and the other technologies discussed in this Article are all part of the movement to decentralize online

4. Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, P2P FOUND. (Feb. 11, 2009), [https://perma.cc/3DBB-ZFDV].

5. See Reiff, *supra* note 2.

6. According to the Oxford English Dictionary, a cypherpunk is a “person who uses encryption when accessing a computer network in order to ensure privacy, especially from government authorities.” *Cypherpunk*, OXFORD ENG. DICTIONARY, [https://perma.cc/RM4U-5PZX] (last visited Mar. 8, 2023).

7. See Nakamoto, *supra* note 4.

8. Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM (Mar. 9, 1993), [https://perma.cc/HM2S-WNY3].

9. Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, FORBES TECH. COUNCIL (Feb. 24, 2022), [https://perma.cc/Y2C8-SPNH].

10. See SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 8 (2019).

11. See *id.* at 11-12.

economic and social activities. The umbrella term “Web3” captures the various movements aiming to enhance individual privacy and control through decentralized technologies and governance.

By the end of the Article, readers will understand the ingenuity and limitations of Bitcoin (Section II), the different types of crypto (Section III), and the challenges of decentralization (Section IV). To realize the benefits of decentralization, more people need to understand the risks and benefits of blockchains and crypto.

II. THE INGENUITY AND LIMITATIONS OF BITCOIN

The importance of Bitcoin cannot be overstated. It is THE reference point for understanding blockchain and crypto. Everyone should know Bitcoin’s story because all subsequent innovations in blockchain and crypto are an extension of or departure from the original Bitcoin blockchain.

Satoshi Nakamoto 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.¹² Nakamoto described Bitcoin in a white paper posted to a cryptographic mailing list on October 31, 2008.¹³ The timing of Bitcoin was no accident. After the 2008 Global Financial Crisis—possibly the greatest economic disruption since the Great Depression—Nakamoto became increasingly distrustful of financial institutions.¹⁴ He aimed to circumvent governments and large financial institutions through privacy-enhancing technologies.¹⁵

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

13. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2 (Oct. 31, 2008) (unpublished manuscript), [<https://perma.cc/BA26-AFPU>].

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

15. See Nakamoto, *supra* note 13, at 1, 6; 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>].

Nakamoto used existing algorithms but assembled them in a way to do something entirely new. 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.”¹⁶ Bitcoin achieves this by tackling some very old problems with algorithms and behavioral incentives (*see* Figure 1).

Figure 1: Value Exchange Before and After Bitcoin

Problems with establishing trust in value exchange	Traditional way to exchange value	Bitcoin’s way to exchange value
Counter-party risks (e.g., double spend)	Trust Trusted third parties (TTPs) mitigate counter-party risks	Computer algorithms and an incentivized community mitigate counter-party risks
Bookkeeping errors and reconciliations	Each party keeps and reconciles their own records	A digital ledger (called a blockchain) that is verified, transparent and immutable is shared, so reconciliations are not needed
Medium of exchange	Parties use fiat money, regulated by sovereign governments	Parties use a cryptocurrency, governed by software and an incentivized community

16. Nakamoto, *supra* note 13, at 1.

Cybersecurity threats	Each party protects its IT perimeter or relies on a TTP to do it for them	Cryptography and other computer algorithms secure the data and the network
-----------------------	---	--

A. Counter-Party Risk Mitigation

Before Bitcoin, a network of global financial systems and regulators mitigate counter-party risks—the risk each trading party bears that the other party will not fulfill its contractual obligations. Banks, credit card companies, money transmitters, notaries, lawyers, and other trusted third parties (“TTPs”) provide independent “truth attestations,” such as ensuring senders’ accounts are funded; preventing a double spend;¹⁷ notarizing signatures; verifying identity; verifying ownership; authenticating assets; and attesting that value exchanges have been properly executed.¹⁸ TTPs provide these and many other vital services to facilitate trade (the advantages), for which they earn significant transaction fees (a major disadvantage).¹⁹ Transaction costs for remittances are typically 2% to 8% of the value of the transaction.²⁰ The process to transact value is expensive, and it is often opaque in that tracking transactions through the knotwork of TTPs can be difficult.

Bitcoin solved the double spend and other counter-party risks by automating some of the services normally done by TTPs and by engaging a community to perform other services.²¹ For an

17. **Double spend:** the risk that the same value might be spent more than once. Jake Frankenfield, *Understanding Double-Spending and How to Prevent Attacks*, INVESTOPEDIA (Jan. 7, 2022), [<https://perma.cc/9GUX-A4VV>].

18. LACITY & LUPIEN, *supra* note 1, at 44.

19. *Id.*

20. The World Bank estimated that sending remittances cost an average of 7.99% of the amount sent. PAYONEER, NAVIGATING THE WORLD OF CROSS-BORDER PAYMENTS 11 (n.d.), [<https://perma.cc/A33E-XYGX>]. The administrative costs for tracking containers in the global supply chain was roughly 22% of the retail costs. James E. Anderson & Eric van Wincoop, *Trade Costs*, 42 J. ECON. LITERATURE, 691, 692 (2004).

21. LACITY & LUPIEN, *supra* note 1, at 45.

automation example, Bitcoin (and all blockchains that followed) rely on cryptographic private-public key pairs to verify account ownership; whoever is in possession of the private key is assumed to be the legitimate owner of the account.²² The private key is stored off the blockchain in the owner's digital wallet.²³ The public key is stored on the blockchain.²⁴ Bitcoin's software easily verifies that only the person with the private key could have submitted a transaction from that account.²⁵

Validating transactions to prevent double spending was a bit thornier to solve without TTPs. Senders cannot be trusted to verify that they have enough money 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. Nakamoto's brilliant solution was to reward other people in the network (called "miners"²⁶) with newly issued bitcoins to validate all recently submitted transactions.²⁷ The economic incentives of the Bitcoin network motivate validators to play by the rules.²⁸

22. "Address" is a more accurate term, but for now, readers can think of a Bitcoin address as a bank account number without the need of a bank. The main difference is that a bank customer typically has only a few bank accounts whereas a Bitcoin user will use hundreds of addresses to help protect their privacy. *Id.*

23. Jake Frankenfield, *Private Key: What It Is, How It Works, Best Ways to Store*, INVESTOPEDIA (Mar. 24, 2022), [<https://perma.cc/2NVZ-QTUE>].

24. *What are Public and Private Keys?*, GEMINI (June 28, 2022), [<https://perma.cc/4HEZ-NV36>].

25. *See* Nakamoto, *supra* note 13, at 2.

26. 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. Just as it gets harder to mine gold as a gold mine is depleted, bitcoin releases fewer new digital coins over time. MARY C. LACITY, BLOCKCHAIN FOUNDATIONS FOR THE INTERNET OF VALUE 46-47 (2020) [hereinafter BLOCKCHAIN FOUNDATIONS].

27. *Id.*

28. Nakamoto wrote this about the economic incentives to motivate 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 13, at 4.

B. Bookkeeping

We also have the ancient challenge of bookkeeping. We need a record for every transfer of value upon which all parties agree. Before Bitcoin, every party manages its own systems of records (software and data, including ledgers that track debits and credits) or relies on a TTP.²⁹ Parties, each with their own version of the transaction, must reconcile information about the transaction. Reconciliations are expensive and time-consuming.³⁰ Once reconciled, there is nothing to prevent trading partners from modifying records after the fact; partners cannot be confident they are dealing with the same historical record of transactions through time. Therefore, we have millions of people with accounting skills working on processing everyday receipts and payables.

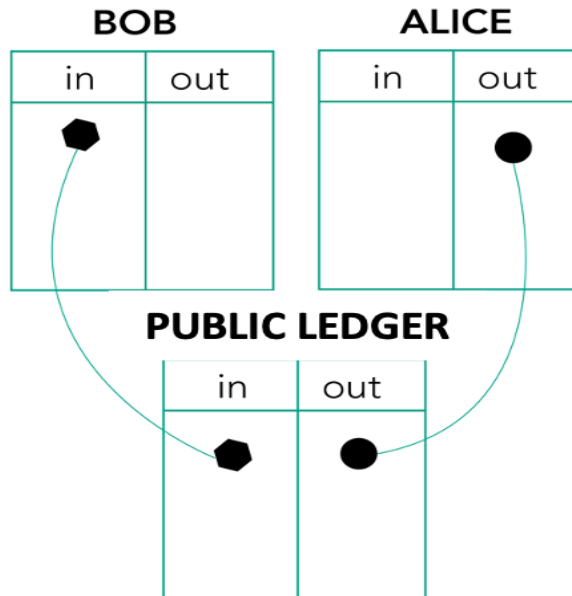
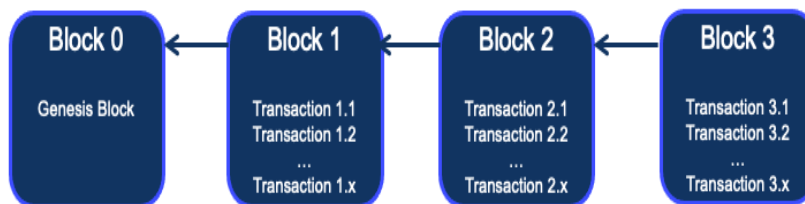
Nakamoto solved the bookkeeping problem by moving from the longstanding double-entry system to triple-entry bookkeeping in which every transaction has three entries: the credit in the sender's digital wallet, the debit in the receiver's digital wallet, and the public receipt stored on a shared ledger (*see* Figure 2).³¹ Bitcoin's public receipt is stored on a digital ledger, called a *blockchain* (*see* Figures 3 and 4).³² Trading parties no longer need to reconcile records because every party agrees that "this is what transpired."

29. BLOCKCHAIN FOUNDATIONS, *supra* note 26, at 47.

30. *Id.*

31. *See* Yuji Ijiri, *Momentum Accounting and Triple-entry Bookkeeping: Exploring the Dynamic Structure of Accounting Measurements*, in 31 AM. ACCT. ASS'N, STUDIES IN ACCOUNTING RESEARCH 1, 62 (1989).

32. "With a blockchain structure, newly submitted transactions are sequenced and collected into a block." BLOCKCHAIN FOUNDATIONS, *supra* note 26, at 408 (*see* Figure 3). 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 109, 114 (Meikang Qiu ed., 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: Bitcoin Definition, Mysteries, Secret Message*, INVESTOPEDIA (July 2, 2021), [<https://perma.cc/48UG-N3MP>].

Figure 2: Bitcoin's Triple-entry Bookkeeping³³**Figure 3: Distributed Ledger Structured as a Chain of Blocks**

33. Adapted from [<https://perma.cc/ZRA7-2JYS>].

Figure 4: An Example of a Transaction Stored on Bitcoin's Public Ledger



Figure 4: 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 ledger is distributed to all the host computers (i.e., nodes³⁴) that run the Bitcoin network. Anyone can view the ledger using a Bitcoin explorer.³⁵ The nodes in the Bitcoin network constantly reconfirm the ledger to make sure no party tampers with the records after the fact.³⁶ If anyone cheats, the other parties' nodes automatically ignore it.

C. Medium of Exchange

We also have the ancient problem of an acceptable medium of exchange. Money was invented more than 10,000 years ago to facilitate trade.³⁷ Money serves three functions: as a medium of exchange for purchases and payment of debts; as a common

34. *Note:* A node is an independent computing entity that communicates with other nodes in a network to work together collectively to complete and store transactions. HYPERLEDGER PERFORMANCE & SCALE WORKING GRP., HYPERLEDGER BLOCKCHAIN PERFORMANCE METRICS 6 (2018), [https://perma.cc/6VWB-LQ2G].

35. For example, see *Block Chain Explorer*, BLOCKCHAIN.COM, [https://perma.cc/D3UL-9WAG] (last visited Feb. 26, 2023).

36. BLOCKCHAIN FOUNDATIONS, *supra* note 26, at 47.

37. *Id.* at 48.

measure of value; and as a store of value that aims to retain its worth over time.³⁸ Most sovereign currencies are now *fiat*, backed solely on the promises of governments rather than by gold reserves, as was common in the past.³⁹

Granted, fiat currencies have several advantages. They have defined laws and regulations, so individuals and enterprises know how to be compliant when using them. Many fiat currencies are reasonable, stable stores of value that hold their worth over time. People understand fiat currencies as a unit of measure; if a quart of milk costs \$2.25, most Americans have a mental model of its value. However, fiat currencies have several disadvantages. Governments can mint fiat money at will, causing inflation, and can change regulations on a whim (recall Nakamoto's quote above). Governments can also freeze, seize, or restrict access to one's assets. Criminals can counterfeit currencies.

Rather than use a government-issued currency, Nakamoto created a new *cryptocurrency*—a digital currency secured by cryptography that makes it nearly impossible to counterfeit.⁴⁰ Moreover, Bitcoin's monetary policies are programmed into the software. Specifically, Bitcoin's software capped the total monetary supply at 21 million bitcoins; scarcity contributes to Bitcoin's value.⁴¹ Bitcoin also has an automatic monetary distribution schedule. The last bitcoin will be released in the year 2140.⁴²

D. Cybersecurity

Lastly, cybersecurity is a newer problem. If we are sending value over the Internet, how do we prevent someone from stealing it? Or stealing our identity? Organizations secure their own information technology ("IT") perimeters or outsource to a TTP.

38. *Id.*

39. *Id.*

40. *Id.* **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." Kathleen Richards, *Cryptography*, TECHTARGET, [https://perma.cc/E88Z-WFV6] (last visited Feb. 26, 2023).

41. David Khalif, *What Happens When All 21 Million Bitcoin Are Mined?*, NASDAQ (June 8, 2022, 9:35 AM), [https://perma.cc/8PQS-C3PW].

42. *Id.*

Either way, data is processed through a centralized node (server) that receives all incoming data from other nodes and, in turn, routes data to other nodes, then is stored in organizational databases.⁴³ Network centralization creates vast pools of data that attract cyberthieves.⁴⁴

In contrast to a centralized network, no single node is in charge in Bitcoin's network (*see* Figure 5).⁴⁵ Decentralized networks like Bitcoin are resilient to cybersecurity attacks because the attack surface is diffused across many locations. There were more than 15,000 public Bitcoin nodes (and many more private nodes) by the end of 2022, each with its own identical copy of the ledger.⁴⁶ The only way to infiltrate the network is to commandeer more than 50% of the processing power of nodes.⁴⁷ So far, the Bitcoin network has never been breached!⁴⁸ (The large heists one hears about happen at centralized exchanges, as explained below.) Cybersecurity gets stronger as more nodes are added to the network because hackers will need to attack more nodes.⁴⁹

43. *Beyond Distributed and Decentralized: What Is a Federated Network?*, INST. OF NETWORK CULTURES, [https://perma.cc/4WGG-7FXK] (last visited Feb. 6, 2023) [hereinafter *Beyond Distributed and Decentralized*].

44. MARY LACITY ET AL., WHAT TYPE OF METAVERSE WILL WE CREATE? 5 (2022), [https://perma.cc/P4WJ-FB67].

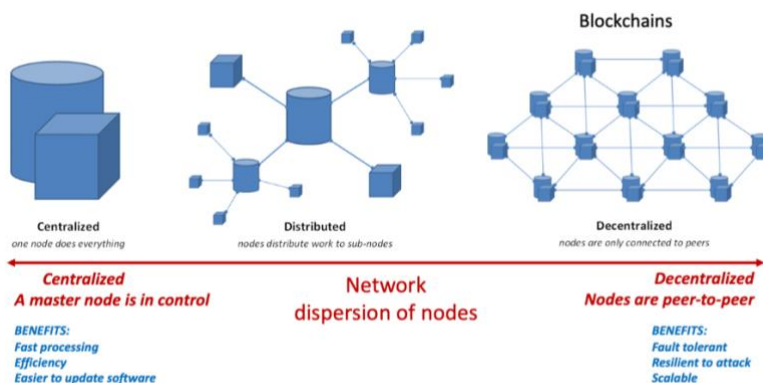
45. Be aware, many people use the terms “decentralized” and “distributed” as synonyms in common vernacular. Here, we use the term “decentralized.” In a decentralized network, data travels to its closest neighbors and is independently validated by each node until all targeted recipient nodes receive the data. In computer science, a distributed network is a hybrid, resulting in a distributed network of centralized networks. *See Beyond Distributed and Decentralized, supra* note 43.

46. The actual number of Bitcoin nodes is difficult to track because some nodes operate behind firewalls. This site tracks “reachable” nodes: BITNODES, [https://perma.cc/V5F8-UG82] (last visited Feb. 26, 2023) (scroll down to the “Nodes” chart and hover over Dec. 31, 2022); *Setting Up Your Bitcoin Full Node*, LEDGER (Feb. 23, 2023), [https://perma.cc/X2C8-36SF].

47. LACITY ET AL., *supra* note 44, at 6.

48. Joey Prebys, *Can Bitcoin Be Hacked?*, COINFLIP (June 22, 2021), [https://perma.cc/V4VR-4E85].

49. Caveat: This is a high-level description written for non-specialists. In actuality, the safety of the network also relies on N-versioning of software (i.e., the same logic programmed in different languages), node independence (i.e., operated by different parties), and a variety of hardware implementations.

Figure 5: (De)centralization of Networks

Scalability is another benefit of network decentralization—just add more machines to the network to get more computing power. Architectural decentralization offers quite a bounty of benefits, but there are downsides as well.⁵⁰ Processing is slower compared to a centralized network because results need to be diffused and checked by the other nodes in the network.⁵¹ Software cannot be updated unless most nodes agree to adopt it—it takes a lot of coordination to make any changes, which is where governance comes in.⁵²

E. Bitcoin's Governance

Decentralization of governance is the dispersion of functions and power to the many. It discourages abuse of power and ideally promotes more inclusive participation, unity around decisions,

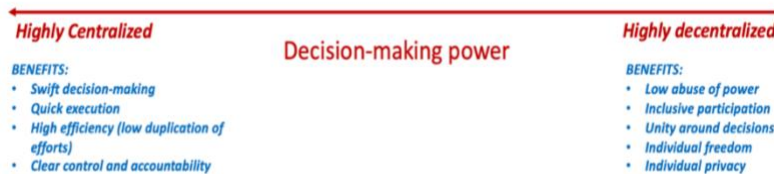
50. Moreover, Brewer's Theorem states that when some nodes are down in a distributed network, the network can either be designed to be available or consistent. In most blockchain networks, the choice is availability over consistency unless the community rallies to stop processing. So, blockchains tolerate some short-term inconsistency to gain the benefits of availability.

51. Anshika Bhalla, *Centralized Vs. Decentralized Digital Networks: Understanding the Differences*, BLOCKCHAIN COUNCIL (Nov. 18, 2022), [<https://perma.cc/4DE3-G6LD>].

52. *Centralized, Decentralized, & Distributed Networks*, CRYPTOEDIA (July 12, 2021), [<https://perma.cc/VB9H-BY6V>].

and individual empowerment, freedom, and privacy (*see* Figure 6).

Figure 6: Centralized vs. Decentralized Governance



All blockchains start out with centralized governance, but many aim to decentralize over time.⁵³ Bitcoin was initially governed by Nakamoto.⁵⁴ Nakamoto wrote the Bitcoin white paper and coded the Bitcoin Core software.⁵⁵ Soon after launch, Nakamoto gave Martti Malmi and Gavin Andresen access rights to update Bitcoin’s website and source code.⁵⁶ In April 2011, Nakamoto walked away from Bitcoin by sending an email that read, “I’ve moved on to other things” and added that Bitcoin was in good hands.⁵⁷

Today, Bitcoin is governed by a community. Anyone can propose improvements by submitting a Bitcoin Improvement Proposal (“BIP”).⁵⁸ The entire Bitcoin community debates the

53. Hanna Halburda & Christoph Mueller-Bloch, *Will We Realize Blockchain’s Promise of Decentralization?*, HARV. BUS. REV. (Sept. 4, 2019), [https://perma.cc/UK48-PKBV].

54. Adam Hayes, *Who Is Satoshi Nakamoto*, INVESTOPEDIA (Jan. 3, 2023), [https://perma.cc/VBW5-2UE9].

55. U.S. SENT’G COMM’N, BITCOIN GLOSSARY: 2018 ANNUAL NATIONAL SEMINAR, [https://perma.cc/6KK5-TW99].

56. Ryan Sheets, *Blockchain Governance: Turning Competition into Teammates*, UNIV. OF ARK. SAM M. WALTON COLL. OF BUS. (Jan. 15, 2021), [https://perma.cc/2HJZ-3T93].

57. Grace Kay, *The Many Alleged Identities of Bitcoin’s Mysterious Creator, Satoshi Nakamoto*, BUS. INSIDER (Nov. 28, 2021, 11:49 AM), [https://perma.cc/R48A-Z3Q5].

58. *What Is a Bitcoin Improvement Proposal (BIP)?*, RIVER FIN., [https://perma.cc/3EFN-QFPF] (last visited Feb. 10, 2023).

proposals based on their merit.⁵⁹ By 2022, 386 BIPs had been submitted, of which 41 had been finalized.⁶⁰ Bitcoin miners (individuals who operate a node in the Bitcoin network) “vote” by either installing or failing to install changes to the source code.⁶¹ The not-for-profit Bitcoin.org helps to coordinate the community’s efforts.⁶²

Unlike Bitcoin, some blockchain founders retain a high degree of centralized control by possessing most of the blockchain’s digital assets and voting rights or by operating the majority of its nodes.⁶³ The degree of centralization is of concern to regulators of securities, particularly if the nonfounding member crypto holders expect a profit based solely on the efforts of the founders.

F. Bitcoin’s Legacy

Bitcoin is important because it is the most visible ongoing, live experiment for an open, public, secure, nongovernmental, and non-TTP-reliant application. All are welcome to participate. Millions of people use it—more than 100 million Bitcoin wallets have been created.⁶⁴ Tens of thousands of people help secure it by being miners.⁶⁵ Bitcoin proves that peer-to-peer value exchange is technically feasible and that a shared digital ledger is highly secure.

However, like all innovations, Bitcoin has limitations and there is room for improvement. It has a higher price volatility compared to other major fiat currencies.⁶⁶ Bitcoin has limited

59. *Id.*

60. *Bitcoin Improvement Proposals*, GITHUB, [https://perma.cc/WYD5-CLSB] (last visited Feb. 10, 2023).

61. *Git-Democracy*, GITHUB, [https://perma.cc/C94W-5VP3] (last visited Feb. 26, 2023).

62. Lyle Daly, *What Is a Blockchain Node?*, THE MOTLEY FOOL (June 9, 2022, 6:37 PM), [https://perma.cc/7BZJ-8LKD].

63. *Id.*

64. Eddie Mitchell, *How Many People Use Bitcoin*, BITCOIN MKT. J. (Nov. 23, 2020, 8:00 AM), [https://perma.cc/49BQ-9TX4].

65. *Bitcoin Security: Here’s What Makes the OG Blockchain Safer Than Fort Knox*, FINIMIZE, [https://perma.cc/T3N8-PV68] (last visited Mar. 9, 2023).

66. Dirk G. Baur & Thomas Dimpfl, *The Volatility of Bitcoin and Its Role as a Medium of Exchange and a Store of Value*, 61 EMPIRICAL ECON. 2663, 2663 (2021).

functionality—it is just a payment system to send and receive bitcoins; it cannot do much else. Ethereum, Cardano, Polkadot, Solana, and other blockchain platforms overcame this limitation by allowing users to build and operate their own decentralized applications.⁶⁷ Bitcoin is rather pokey, only capable of processing about two to six transactions per second (“TPS”).⁶⁸ Innovations in “layer 2” solutions that run on top of Bitcoin (and other platforms) improve processing speed and reduce transaction fees.⁶⁹ Bitcoin is not user friendly, so most people end up relying on a TTP anyway, called an exchange (explained below). Bitcoin’s consensus protocol to make sure copies of the ledger agree, called proof-of-work,⁷⁰ is highly secure, but the miners who operate computers to secure the Bitcoin network consume a lot of electricity.⁷¹ New consensus protocols are more energy efficient, like proof-of-stake,⁷² which Ethereum moved to in

67. *Polkadot vs Cardano vs Solana: Which Third-Generation Blockchain Should You Choose?*, PIXELPLEX (Nov. 8, 2022), [https://perma.cc/AY7W-FTH7].

68. Mary C. Lacity, *Blockchain: From Bitcoin to the Internet of Value and Beyond*, 37 J. INFO. TECH. 326, 327 (2022).

69. *Id.* at 329.

70. **Proof-of-Work:** Cynthia Dwork and Moni Naor created the “proof-of-work” protocol in 1993 to prevent junk email. See Cynthia Dwork & Moni Naor, *Pricing via Processing or Combatting Junk Mail*, in *ADVANCES IN CRYPTOLOGY—CRYPTO ‘92* (Ernest F. Brickell ed., 1992), [https://perma.cc/9LUU-NF2J]. Satoshi Nakamoto adopted the “proof-of-work” consensus protocol for Bitcoin in the 2008 white paper. *Proof-of-Stake vs. Proof-of-Work: Pros, Cons, and Differences Explained*, COINTELEGRAPH, [https://perma.cc/F9KJ-FPUB] (last visited Feb. 27, 2023).

71. Oscar Gonzalez, *Bitcoin Mining: How Much Electricity It Takes and Why People Are Worried*, CNET (July 18, 2022, 2:08 PM), [https://perma.cc/X45G-B6ER].

72. **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.* at 2. Essentially, the selected member node is awarded a transaction fee. *Id.* at 4. It is called a “Proof-of-Stake” because the members with the highest “stake” (i.e., those who have the largest account balances in escrow accounts) are given priority in the selection algorithm. *Id.* at 2. Proof-of-Stake uses much less energy than Proof-of-Work and settles transactions faster than Proof-of-Work. *Id.* at 4. 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; and that the rich may get richer because the algorithms favor large balances in escrow accounts.

2022.⁷³ Bitcoin was designed as a standalone application; interoperability solutions aim to connect blockchain networks.

To recap, Bitcoin was the first decentralized application that restored trust in economic exchanges of value without relying on governments and corporations. Next, we'll look at the Cambrian explosion of crypto since Bitcoin.

III. THE CAMBRIAN EXPLOSION OF CRYPTO

Following Bitcoin's launch in 2009, more than 21,000 cryptos were listed on the website coinmarketcap.com.⁷⁴ In 2022, the entire crypto market capitalization fluctuated from \$810 billion to \$2.6 trillion (see Figure 7).

Figure 7: Total Crypto Market Cap December 1, 2021 to December 1, 2022⁷⁵



Each crypto has its own back story with its own set of founders, missions, and functionality. They are all crypto because they are controlled with cryptographic private-public keys pairs. Initially, new crypto were created by downloading, altering, and launching a new network based on the open-source code for

73. Amy Castor, *Why Ethereum Is Switching to Proof of Stake and How It Will Work*, MIT TECH. REV. (Mar. 4, 2022), [<https://perma.cc/GBG4-69GL>].

74. James Royal, *Cryptocurrency Statistics 2023: Investing in Crypto*, BANKRATE (Jan. 5, 2023), [<https://perma.cc/N4R5-KBL5>].

75. *Global Cryptocurrency Charts*, COINMARKETCAP, [<https://perma.cc/6RJH-RS7V>] (last visited Feb. 26, 2023).

Bitcoin Core.⁷⁶ It is now more common to launch a new crypto by using a smart contract on an existing platform like Ethereum.⁷⁷

At this stage of development, there is no official standard to consistently label, define, or categorize crypto. Let's look at some classifications.

Wyoming recognizes three types: cryptocurrencies, security tokens (subject to Securities and Exchange Commission (SEC) regulations), and utility tokens.⁷⁸ Wyoming passed the nation's first utility token taxonomy act in 2019.⁷⁹ The law introduces a new token type, defined as a "utility" or "consumer" token, used exclusively for the purpose of consumption.⁸⁰ In the nondigital world, consumer tokens are commonly used at arcades, theme parks, and other entertainment venues. One token, such as a metal coin or printed ticket, always has the same consumptive value—i.e., one token allows the holder to play one game, ride one ride, or redeem one drink. The Wyoming law allows for digital utility tokens.⁸¹ As an example of a digital utility token, consumers might buy tokens to raise money for a startup that could later be redeemed to access the startup's services. A utility token is not considered a security token under Wyoming law, provided the coin will have the same expected value in the future.⁸²

Technologists and business professionals tend to classify crypto by its function. Alex Tapscott, co-founder of the Blockchain Research Institute, for example, uses the umbrella term "digital asset" and identified nine types: cryptocurrencies (digital money); protocol tokens (tokens native to a platform like Bitcoin, Ethereum, or Cosmos); governance tokens (provide holders with decision-making rights for decentralized autonomous organizations ("DAOs")); non-fungible tokens

76. Alyssa Hertig, *Open Source: What It Is and Why It's Critical for Bitcoin and Crypto*, COINDESK (Oct. 6, 2022, 12:49 PM), [https://perma.cc/8D3D-YTYM].

77. Nathan Reiff, *Bitcoin vs. Ethereum: What's the Difference?*, INVESTOPEDIA (Oct. 4, 2022), [https://perma.cc/XA99-UEK2].

78. Caitlin Long, *Wyoming's Pro-Blockchain Laws Tame the Wild West of Crypto*, SYGNA, [https://perma.cc/6XZU-YUZF] (last visited Feb. 27, 2023).

79. Rachel Wolfson, *U.S. State of Wyoming Defines Cryptocurrency 'Utility Tokens' as New Asset Class*, FORBES (Mar. 13, 2018), [https://perma.cc/4PTE-ABTF].

80. 2019 Wyo. Sess. Laws 485.

81. *Id.*

82. *Wyoming Passes Bill Exempting Some Tokens from Securities Laws*, HOGAN LOVELLS (Mar. 9, 2018), [https://perma.cc/GSS5-K8PX].

(“NFTs”) that represent unique assets; exchange tokens that are native to exchange platforms (like Binance); securities tokens that represent stocks, bonds, and derivatives; stable coins that are pegged to fiat currencies; natural asset tokens that are pegged to commodities like gold; and central bank digital currencies (“CBDCs”) that are crypto versions of fiat currencies.⁸³ Let’s look at stable coins and NFTs more closely.

A. Stable Coins

Stable coins are fungible crypto tokens that are pegged to assets outside the blockchain network.⁸⁴ Stable coins are often tied to a fiat currency, most commonly to the U.S. dollar, but also to the euro, British pound, the Japanese yen, and other fiat currencies.⁸⁵ Stable coins are “stable” in that holders should always be able to exchange them for the pegged asset. However, stable coins are managed by a TTP, so it’s not always clear whether the TTP stores total or fractional reserves, nor is the true risk to investors always apparent.⁸⁶

Stable coins are primarily used to facilitate trades across cryptocurrency exchanges.⁸⁷ Arbitrage traders need to quickly buy and sell crypto from multiple exchanges to generate a profit by taking advantage of the slightly different prices across exchanges. For example, at the moment of this writing, the price of bitcoin is \$16,947 on the Binance exchange and \$16,951 on Coinbase. If traders had to convert one cryptocurrency to dollars before buying another cryptocurrency, they would add transaction costs and lose speed. Holding stable coins allows them to trade immediately.⁸⁸

83. See ALEX TAPSCOTT, *DIGITAL ASSET REVOLUTION: HOW BLOCKCHAIN IS DECENTRALIZING FINANCE AND DISRUPTING WALL STREET*, at xvii (2022).

84. Adam Hayes, *Stablecoins: Definition, How They Work, and Types*, INVESTOPEDIA (Oct. 4, 2022), [<https://perma.cc/69HA-ESZT>].

85. See Madana Prathap, *Top 6 Stablecoins in the Crypto Market—What Are They, How They Work and Why They Have Governments Worried*, BUS. INSIDER INDIA (Dec. 24, 2021, 12:39 AM), [<https://perma.cc/U2JQ-J7JJ>].

86. James Royal, *What Are Stablecoins and How Do They Affect the Cryptocurrency Market?*, BANKRATE (May 12, 2022), [<https://perma.cc/QD5A-GDF8>].

87. Prathap, *supra* note 85.

88. *Id.*

Tether (“USDT”) was the first stable coin, launched in 2014 by a company called Tether Limited.⁸⁹ Buyers exchange one dollar for one Tether coin, with Tether Limited allegedly storing each dollar in a bank reserve.⁹⁰ Tether Limited has often been accused of not holding enough dollars in reserve and of manipulating the price of Bitcoin.⁹¹ It has repeatedly dodged demands for public audits and faced fines from the U.S. Commodity Futures Trading Commission.⁹² Despite the controversy, Tether remains the favored stable coin by crypto traders as of December 2022.⁹³

Since Tether, other notable stable coins were launched that were also pegged to the dollar. These include USD Coin and Gemini, launched in 2018;⁹⁴ JPM Coin in 2019;⁹⁵ and Binance USD in 2019.⁹⁶ While most stable coins are available to the public, JPM Coin is not, as it is only for JPMorgan’s institutional customers.⁹⁷ JPMorgan uses its JPM Coin to facilitate institution-to-institution transfers.⁹⁸ When one JPMorgan client sends money to another over the blockchain, it uses the digital coin to speed settlement times, which are immediately redeemed for dollars.⁹⁹

89. *What Is Tether? An In-Depth Guide for Beginners*, WORLDCOIN (Nov. 29, 2022), [<https://perma.cc/9PP7-RUK6>].

90. *Id.*

91. Elizabeth Lopatto, *The Tether Controversy, Explained*, THE VERGE (Aug. 16, 2021, 7:00 AM), [<https://perma.cc/V4GL-QGUA>].

92. Sebastian Sinclair, *Tether Pushes Back Timeline on Audit: Report*, BLOCKWORKS (Aug. 29, 2022, 5:10 AM), [<https://perma.cc/6Z8X-KMMR>]; Royal, *supra* note 86.

93. Prathap, *supra* note 85.

94. *Id.*; *What Is Gemini Dollar (GUSD)?*, COINDESK (Jan. 18, 2023, 12:30 PM), [<https://perma.cc/GW8P-NA3U>].

95. Eddie Mitchell, *What Is JPM Coin and How Do You Buy It?*, BITCOIN MKT. J. (Jan. 10, 2021, 8:00 AM), [<https://perma.cc/W3Y5-GK9B>].

96. Prathap, *supra* note 85.

97. Mitchell, *supra* note 95.

98. *Coin Systems*, ONYX BY J.P. MORGAN, [<https://perma.cc/F4ZE-WGK4>] (last visited Feb. 27, 2023).

99. *Id.*

B. Non-Fungible Tokens (“NFTs”)

Crypto tokens can be used to represent *non-fungible* (unique) assets where the token represents a particular asset.¹⁰⁰ For example, a unique token could be created to represent a particular diamond, concert ticket, or work of art. Smart contracts facilitate the creation, buying, and selling of NFTs on a blockchain network.¹⁰¹

CryptoKitties was the first NFT smart contract to gain widespread adoption.¹⁰² It runs on Ethereum.¹⁰³ Launched by Dapper Labs in 2017, it allows users to buy, trade, and breed virtual cats, each of which is unique and secured with an NFT.¹⁰⁴ If you buy two CryptoKitties on the marketplace,¹⁰⁵ you can breed them to produce a new CryptoKitty with its own “cattrIBUTES” and secured with its own NFT.¹⁰⁶ Cryptokitties became so popular in 2017 that the game created a backlog of tens of thousands of transactions on the Ethereum network.¹⁰⁷

NFTs made headlines in 2021 when some sold for millions of dollars. Jack Dorsey, founder of Twitter, sold his first tweet as an NFT for \$2.9 million in 2021.¹⁰⁸ He launched the NFT on the Valuables platform.¹⁰⁹ To date, Mike Winkelmann—the artist

100. Mitchell Clark, *NFTs, Explained*, THE VERGE (June 6, 2022), [https://perma.cc/MUE4-K5H9].

101. *All You Need to Know About NFT Smart Contracts*, BINANCE: BINANCE BLOG (Aug. 4, 2022), [https://perma.cc/M7KP-HGWN].

102. *Ethereum—The Blockchain That Changed It All*, CLAYSTACK (Aug. 6, 2021), [https://perma.cc/6WAZ-4KX9].

103. *Id.*

104. Fitz Tepper, *People Have Spent Over \$1M Buying Virtual Cats on the Ethereum Blockchain*, TECHCRUNCH (Dec. 3, 2017, 5:48 PM), [https://perma.cc/2Q4R-HDP8].

105. The CryptoKitties marketplace is here: CRYPTOKITTIES, [https://perma.cc/83JA-PELJ] (last visited Feb. 27, 2023).

106. *What Are CryptoKitties?*, KRAKEN, [https://perma.cc/XWB7-K47E] (last visited Feb. 27, 2023).

107. *CryptoKitties Craze Slows Down Transactions on Ethereum*, BBC NEWS (Dec. 5, 2017), [https://perma.cc/L9BZ-USVZ]; Joon Ian Wong, *The Ethereum Network Is Getting Jammed Up Because People Are Rushing To Buy Cartoon Cats on Its Blockchain*, QUARTZ (Dec. 4, 2017), [https://perma.cc/YAY9-MUNA].

108. Sandali Handagama, *‘Jack Dorsey’s First Tweet’ NFT Went on Sale for \$48M. It Ended with a Top Bid of Just \$280*, COINDESK (Apr. 16, 2022), [https://perma.cc/8BKK-4J7H].

109. Taylor Locke, *Jack Dorsey Sells His First Tweet Ever as an NFT for Over \$2.9 Million*, CNBC (Mar. 24, 2021), [https://perma.cc/QP94-QZE6].

known as Beeple—has the highest price paid for an NFT at \$69 million for a digital collage of his work that included more than 5,000 images.¹¹⁰ According to Bloomberg, the NFT market on Ethereum was \$41 billion in 2021.¹¹¹

While most NFTs are transferable, some are not, such as using an NFT to issue a credential to a particular person; these are called “Soulbound Tokens.”¹¹²

It’s important for NFT buyers to understand what they are purchasing. NFTs are programable, so the terms may vary from ownership of an asset to limited uses, such as the right to display the asset on social media, but the creator keeps copyright/ownership.¹¹³ So, in the NFT world, we must be careful to separate technical functionality (control over an NFT by possessing the private key) from legal ownership as defined by law and which varies by jurisdiction.

Most users buy NFTs from marketplaces like popular NFT platforms OpenSea, Axie Infinity, Rarible, Nifty Gateway, SuperRare, and Flow.¹¹⁴ NFT platforms are just one of the many threats to decentralization.

IV. THREATS TO DECENTRALIZATION

The first blockchain networks like Bitcoin and Ethereum aim to remedy the global crisis of distrust in our governments and institutions by decentralizing the architecture and governance of economic transactions.¹¹⁵ No matter the promised benefits of decentralization, the pull towards centralization is strong. Crypto technology is still evolving and confusing, so many people choose to rely on an exchange, called Centralized Finance (“CeFi”). Exchanges collect transaction fees and take custody of customers’

110. *Beeple: Digital Art Disruptor*, MASTERWORKS (Jan. 3, 2022), [<https://perma.cc/8QK6-GRH8>].

111. Allyson Versprille, *NFT Market Surpassed \$40 Billion in 2021, New Estimate Shows*, BLOOMBERG (Jan. 6, 2022), [<https://perma.cc/JPD6-2MNV>].

112. ERIC GLEN WEYL ET AL., *DECENTRALIZED SOCIETY: FINDING WEB3’S SOUL 2* (2022), [<https://perma.cc/8KX8-6ZZQ>].

113. Clark, *supra* note 100.

114. Trinetra Paul, *The Most Popular NFT Marketplaces You Should Know About*, PRESTIGE (Feb. 2, 2022), [<https://perma.cc/CE3S-XGLU>].

115. *See supra* Part I.

private keys¹¹⁶—the situation Nakamoto was trying to avoid. Low voter turnout in some blockchain networks threatens the effectiveness of decentralized governance.¹¹⁷ Additionally, powerful parties dominate some networks by controlling most nodes, assets, or governance. Let’s examine some of the major threats more closely.

A. Centralized Finance (“CeFi”)

Many consumers find the convenience of exchanges a better option than managing their own crypto wallets. The use of an exchange is called centralized-decentralized finance, meaning that a centralized exchange sits between customers and decentralized blockchain networks.¹¹⁸

The first Bitcoin exchange was Bitcoin Market, launched in March 2010 by a Bitcoin Talk member using the pseudonym “dwdollar.”¹¹⁹ Jed McCaleb soon after launched the most infamous Bitcoin exchange called Mt. Gox in 2010.¹²⁰ When his “hobby” began taking all his time in 2011, McCaleb sold the site to Mark Karpelès.¹²¹ Early exchanges operated under the radar of regulatory bodies, and many consumers were at risk for heists. Mt. Gox—and other exchanges that followed—were lucrative targets for hackers because exchanges controlled the users’ private keys.¹²² One of the largest heists occurred in August 2014 when 850,000 bitcoins, worth \$450 million at the time, were stolen from wallets managed by Mt. Gox.¹²³

116. Krisztian Sandor, *What Is Crypto Custody?*, COINDESK, [https://perma.cc/885B-LV9J] (last visited Feb. 27, 2023).

117. *Decentralisation, Governance and EOS—a Lost Case?*, BINANCE RSCH. (Feb. 18, 2020), [https://perma.cc/66MK-QZLF].

118. LACITY ET AL., *supra* note 44, at 14.

119. Nathaniel Whitemore & Clay Collins, *A History of Crypto Exchanges: A Look at Our Industry’s Most Powerful Institutions*, NOMICS (Nov. 14, 2019), [https://perma.cc/ZH3N-LXTH].

120. *Id.*

121. Wolfie Zhao, *Mt Gox Founder Hit with Lawsuit over Alleged Fraudulent Misrepresentation*, COINDESK (June 26, 2019, 4:10 AM), [https://perma.cc/GUR5-QQBJ]. See generally NATHANIEL POPPER, *DIGITAL GOLD* (2015).

122. LACITY & LUPIEN, *supra* note 1, at 162.

123. *Id.*; *Japan Arrests MtGox Bitcoin Head over Missing \$387m*, AL JAZEERA (Aug. 1, 2015), [https://perma.cc/9TJ4-YY4Z].

More recently, in November 2022, Sam Bankman-Fried, founder of the crypto exchange FTX, declared bankruptcy after a run on the bank when customers learned he had used their crypto to prop up his investment company.¹²⁴ At least \$1 billion in customer funds vanished in a matter of days.¹²⁵

Today, there are more than 500 cryptocurrency exchanges, including Coinbase (founded in 2012 in the United States), Huobi (founded in China in 2013), Kraken (founded in 2013 in the United States), and Binance (founded in China in 2017 but has since moved to Malta).¹²⁶ Although exchanges are based in one country, many exchanges serve customers worldwide. Kraken, for example, is available in 48 U.S. states and 176 countries.¹²⁷ Many exchanges now comply with regulations, including Know Your Customer (“KYC”) and Anti-Money Laundering (“AML”) requirements.¹²⁸ For example, Coinbase had money transmitter licenses from 45 U.S. states and a New York State Virtual Currency License by 2019.¹²⁹ Coinbase also has commercial criminal insurance that is greater than the value of digital currency maintained in online storage (98% of the private keys are stored offline).¹³⁰ Increased compliance means a loss of user anonymity, a consequence counter to the values of the initial Bitcoin adopters.

B. Fifty-One Percent Attacks

Blockchain networks need to be decentralized to prevent someone from overtaking and thus controlling 51% of the network.¹³¹

124. See Angus Berwick, *Exclusive: At Least \$1 Billion of Client Funds Missing at Failed Crypto Firm FTX*, REUTERS (Nov. 13, 2022, 4:00 PM), [<https://perma.cc/Z6KG-6YER>].

125. *Id.*

126. LACITY & LUPIEN, *supra* note 1, at 162. CoinMarketCap tracks cryptocurrency exchanges on its website at *Top Cryptocurrency Spot Exchanges*, COINMARKETCAP, [<https://perma.cc/2BEJ-YN8D>] (last visited Feb. 10, 2023).

127. LACITY & LUPIEN, *supra* note 1, at 162.

128. *Id.*

129. *Id.*

130. *Id.* at 162-63.

131. See *What Is a 51% Attack on the Blockchain?*, ORIGINSTAMP, [<https://perma.cc/FRV7-RAFX>] (last visited Feb. 10, 2023).

For large public blockchains, the threat comes from the concentration of power by mining or staking pools.¹³² On the day of this writing, five mining pools were creating 80% of the new Bitcoin blocks.¹³³ Ethereum had only moved to proof-of-stake four months ago, so it's hard to assess the risk of a 51% attack. Ethereum.org monitors the network closely.¹³⁴

Although Bitcoin and Ethereum have not suffered a 51% takeover, other blockchain networks have, including Ronen Network, Verge, ZenCash, Bitcoin Gold, and Ethereum Classic.¹³⁵

C. Centralized Asset Ownership

“Whoever has the gold, makes the rules!”¹³⁶ That's a caption from a 1964 comic strip that we can update as, “Whoever has the crypto makes the rules.” In some blockchain networks, a small percentage of people own the majority of crypto. For example, Ripple Labs owns about 60% of the supply of the Ripple network's crypto called XRP.¹³⁷ In 2020, the SEC charged Ripple Labs' co-founder and its current CEO with violating investor protection laws by raising \$1.3 billion through an unregistered securities offering.¹³⁸

In another example, one “whale” account in the Solend lending application owned 95% of one of its liquidity pools and nearly wiped out the value of the crypto SOL when he or she came

132. **Mining or staking pool:** Individuals who pool their resources and agree to share block rewards and transaction fees in proportion to their contributed mining hash power in the case of mining or stake in the case of staking. Mining pools are desirable to the average miner because they smooth out rewards and make them more predictable.

133. To see the dominant mining pools in real time, go to *Hashrate Distribution*, BLOCKCHAIN.COM, [https://perma.cc/TWS6-9FBJ] (last visited Feb. 27, 2023).

134. To see Ethereum's network charts and statistics, go to ETHSCAN, [https://perma.cc/JT6T-JZ4Y] (last visited Mar. 9, 2023).

135. LACITY & LUPIEN, *supra* note 1, at 403.

136. BRANT PARKER & JOHNNY HART, *Remember the Golden Rule!*, in THE WIZARD OF ID (1971).

137. See John Bogna, *Ripple's XRP: What It Is, What It's Worth and Should You Be Investing?*, NASDAQ (Sept. 26, 2022, 6:11 PM), [https://perma.cc/8SGR-5VNU].

138. See Press Release, Sec. & Exch. Comm'n, SEC Charges Ripple and Two Executives with Conducting \$1.3 Billion Unregistered Securities Offering (Dec. 22, 2020), [https://perma.cc/97Z4-9R94].

“dangerously close to a massive margin call.”¹³⁹ When the community called for a vote to stop the wallet, the “whale” had more than 1 million of the 1.48 million governance tokens.¹⁴⁰

D. Centralized Governance

While a blockchain architecture is decentralized, the same isn’t always true for the governance of a blockchain. Centralized governance runs aground when leaders abuse power, pursue their own interests at the expense of others, exclude participation from individuals who do not agree with them (no inclusivity), stifle opinions (no unity around decision), crush the will and actions of others (lack of freedom), and invade their privacy through over-monitoring. These are the major concerns expressed by the global blockchain community, as well as why, on the balance, many open-source communities favor decentralization—not only of the network architecture, but of the governance, as well.¹⁴¹

V. SAVING DECENTRALIZATION

Trust is the foundation for well-functioning societies; yet global surveys show high levels of distrust for governments and institutions.¹⁴² We have argued that the decentralization of economic (and social) activities is a way to restore global trust, and that blockchains can serve as the digital infrastructure and crypto serves as digital assets. We’ve made a crucial distinction between technology decentralization and governance decentralization.

While blockchains are designed to automate crypto transactions without relying on a trusted third party, many people

139. See Danny Nelson, *Solend’s Whale Liquidation Crisis Prompts Second Vote to Reverse ‘Emergency Powers,’* COINDESK (June 19, 2022 11:20 PM), [https://perma.cc/6PC2-NSZT].

140. See Kris Holt, *Cryptocurrency Is More Centralized Than Many Advocates Claim, According to Report,* ENGADGET (June 21, 2022, 1:46 PM), [https://perma.cc/9B8N-FGCP].

141. LACITY & LUPIEN, *supra* note 1, at 63.

142. For example, the 2022 Edelman Trust Barometer found that most of 33,000 global respondents do not trust government leaders (58%), business leaders (51%), or journalists (54%). See EDELMAN, EDELMAN TRUST BAROMETER 2022, at 1-2, 14 (2022), [https://perma.cc/97PX-9KWV].

choose to use exchanges and NFT platforms at this stage of development. To decentralize the exchange of value, a larger percentage of the population needs to understand these technologies, including their risks and benefits. While this Article aims to help educate legal professionals, the learning journey can continue with recommended readings,¹⁴³ online courses for professionals,¹⁴⁴ or university classes.¹⁴⁵

As readers learn more about blockchains, it's important to make one thing clear: readers should not trust a blockchain application just because it uses blockchain technologies. Scammers leave inventors rich and investors broke, as we saw with the FTX example. Bad actors try to take centralized control, which is counter to the aims of decentralized power. It's vital to investigate each crypto's history, network operations, and governance.

143. I highly recommend this book to legal professionals: CAROL GOFORTH, *REGULATION OF CRYPTOTRANSACTIONS* (2020).

144. Coursera offers a number of online specializations, such as Web3 and Blockchain in Global Commerce Specialization. *See* COURSEERA, [<https://perma.cc/X7UN-NU9A>] (last visited Feb. 27, 2023).

145. The Walton College of Business at the University of Arkansas offers blockchain courses, minors, concentrations, and certificates. *See U of A Courses*, UNIV. OF ARK. SAM M. WALTON COLL. OF BUS., [<https://perma.cc/Q3E5-HDB7>] (last visited Feb. 27, 2023).