Congressional Research Service
Informing the legislative debate since 1914

Blockchain: Novel Provenance Applications

April 12, 2022

Congressional Research Service
https://crsreports.congress.gov
R47064

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47064

April 12, 2022

Kristen E. Busch
Analyst in Science and Technology Policy

Blockchain: Novel Provenance Applications

Blockchain, generally, is a database technology that records and stores information in blocks of data that are linked, or "chained," together. Data stored on a blockchain are continually shared, replicated, and synchronized across the nodes in a network—individual computer systems or specialized hardware that communicate with each other and store and process information. This system enables tamper-resistant recordkeeping without a centralized authority or intermediary.

There are multiple types of blockchains, and, depending on the type, recorded data may be accessible to all users or only a designated subset. All blockchains share common characteristics, including decentralization (i.e., no centralized authority), immutability (i.e., the blockchain records are unalterable), and pseudonymity (i.e., how users' real-world identities are handled). Certain blockchain types may offer greater levels of decentralization and pseudonymity than others. New blockchain applications, such as smart contracts, non-fungible tokens, and decentralization autonomous organizations, may automate processes or replace intermediaries in a variety of fields. Recent developments in blockchain governance protocols and consensus mechanisms have raised concerns about the environmental impact, oversight, and accountability of blockchain networks.

Since its creation in 2008, blockchain has been most commonly associated with cryptocurrencies—digital currencies that users exchange through decentralized computer networks. More recently, public and private sector actors have used blockchain applications in fields such as supply chain management, identity management, and asset registration. Blockchain technologies may enable establishing the provenance of goods and tracking their progression through a supply chain; identity-management with digital credentials; recording the ownership of digital and physical objects; and the transfer of property, rights, or goods without a third-party intermediary. The United States is a hub for private-sector blockchain development, and many states and federal agencies are experimenting with novel blockchain provenance applications, including the Food and Drug Administration and Department of the Treasury.

Proponents claim that blockchain can increase transparency and efficiency in many fields by enabling auditable and immutable recordkeeping. However, opponents have significant concerns. Blockchain technologies are maturing and fully developed use cases outside of the financial sector are relatively limited. In some applications, blockchain technologies can add unnecessary complexity compared with using conventional databases or other alternatives. The technology may also pose security and privacy risks if sensitive information is permanently recorded on a blockchain, encryption algorithms are broken, smart contracts malfunction, or digital wallets and other blockchain applications are hacked. Some blockchains also use energy-intensive processes to validate transactions, which can consume as much energy as small nations.

Individual states have passed legislation or established initiatives to develop, incentivize, and regulate blockchain technologies. Some states have taken vastly different approaches to blockchain technologies, so the state-level regulations that do exist vary widely. A handful of federal agencies have released guidance on blockchain technologies in specific sectors, such as finance, but there is little guidance for blockchain applications in other fields, such supply chain logistics, identity credentialing, or intellectual property and asset registration. In the meantime, China and the European Union have invested heavily in blockchain technologies and developed their own respective regulatory frameworks, so international regulations may also conflict with one another.

Congress may consider the appropriate role, if any, the U.S. government may play in the development or regulation of blockchain technologies and applications. Congress could consider funding research into blockchain technologies, supporting standards development, or directing federal agencies to create guidance on certain blockchain applications, among other options. Congress may also consider the roles of the public and private sectors in addressing the potential risks associated with blockchain technologies generally, as well as within specific sectors and with specific applications. For example, Congress might consider whether existing privacy regulations are adequate to address potential concerns arising from the use of blockchain technologies and blockchain-enabled provenance applications.

Contents

Figures

Tables

Appendixes

Contacts

Introduction

Blockchain is a database technology that records and stores information in blocks of data that are linked, or "chained," together. Data stored on a blockchain are continually shared, replicated, and synchronized across the nodes in a network—individual computer systems or specialized hardware that communicate with each other and store and process information. This system enables tamper-resistant recordkeeping without a centralized authority or intermediary. All blockchains share common characteristics, including a level of decentralization (i.e., no centralized authority), immutability (i.e., the blockchain records are unalterable), and pseudonymity (i.e., how users' real-world identities are handled).

Since its creation in 2008, blockchain has been most commonly associated with cryptocurrencies—digital currencies that users exchange through decentralized computer networks. Proponents of blockchain technologies have identified applications that help establish the provenance of physical and digital items. Provenance is the ability to know the origin and history of a physical or digital item. Blockchain technologies may enable establishing the provenance of goods and tracking their progression through a supply chain; identity-management with digital credentials; recording the ownership of digital and physical objects; and the transfer of property, rights, or goods without a third-party intermediary.

Congress may consider the appropriate role, if any, the U.S. government may play in the development or regulation of blockchain technologies and applications. Congress could consider funding research into blockchain technologies, supporting standards development, or directing federal agencies to create guidance on certain blockchain applications, among other options. Congress may also consider the roles of the public and private sectors in addressing the potential risks associated with blockchain technologies generally, as well as within specific sectors and applications.

This report focuses on blockchain provenance applications in supply chain management, identity management, and registry and asset tracking. It provides an overview of blockchain technologies and recent technical developments. This report discusses examples of international and domestic regulatory frameworks and congressional considerations for blockchain technologies. For more information on cryptocurrencies and other blockchain applications, see the following list of existing CRS products.

CRS Products on Blockchain Technologies and Applications

Blockchain Technologies

CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

CRS Testimony TE10025, *Beyond Bitcoin: Emerging Applications for Blockchain Technology*, by Chris Jaikaran.

CRS Video WVB00200, *Understanding Blockchain Technology and Its Policy Implications*, by Chris Jaikaran.

Non-Financial Blockchain Applications

CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*, by Corrie E. Clark and Heather L. Greenley.

CRS In Focus IF11829, *Blockchain Technology and Agriculture*, by Genevieve K. Croft.

CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

Financial Blockchain Applications

CRS Report R46208, *Digital Assets and SEC Regulation*, by Eva Su.

CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, by David W. Perkins.

CRS Report R45440, *International Approaches to Digital Currencies*, by Rebecca M. Nelson.

CRS Report R46486, *Telegraphs, Steamships, and Virtual Currency: An Analysis of Money Transmitter Regulation*, by Andrew P. Scott.

CRS Report R45664, *Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals*, by Jay B. Sykes and Nicole Vanatko.

CRS Report R46843, *International Financial Messaging Systems*, by Liana Wong and Rebecca M. Nelson.

CRS Report R43339, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, by Edward V. Murphy and M. Maureen Murphy.

CRS In Focus IF10824, *Financial Innovation: "Cryptocurrencies"*, by David W. Perkins.

CRS In Focus IF10825, *Digital Currencies: Sanctions Evasion Risks*, by Rebecca M. Nelson and Liana W. Rosen.

CRS In Focus IF11004, *Financial Innovation: Digital Assets and Initial Coin Offerings*, by Eva Su.

CRS In Focus IF11910, *Cryptocurrency Transfers and Data Collection*, by Mark P. Keightley and Andrew P. Scott.

CRS In Focus IF11471, *Financial Innovation: Central Bank Digital Currencies*, by Marc Labonte, Rebecca M. Nelson, and David W. Perkins.

CRS In Focus IF10513, *Financial Innovation: "Fintech"*, by David W. Perkins.

CRS In Focus IF11195, *Financial Innovation: Reducing Fintech Regulatory Uncertainty*, by David W. Perkins, Cheryl R. Cooper, and Eva Su.

CRS Insight IN11709, *Decentralized Finance (DeFi) and Financial Services Disintermediation: Policy Challenges*, by Eva Su.

CRS Insight IN11632, *Pandemics, Payments, and (Digital) Property*, by Andrew P. Scott.

CRS Insight IN11183, *Libra: A Facebook-led Cryptocurrency Initiative*, by Rebecca M. Nelson and David W. Perkins.

CRS Legal Sidebar WSLG1856, *For First Time, FinCEN Imposes Penalty on Foreign-Based Virtual Currency Exchange for Violations of Anti-Money Laundering Laws*, by M. Maureen Murphy.

CRS Legal Sidebar LSB10227, *CFTC and Virtual Currencies: New Court Rulings and Implications for Congress*, by Nicole Vanatko.

Overview of Blockchain

Blocks of Data

Blockchain is a system to keep track of information and store data.[1] In many cases, blockchains record transactional data (e.g., assets sent and received between parties). Transactions occurring at around the same time on a network are grouped together and recorded as blocks of data on the blockchain. A typical block on the blockchain might include thousands of transactions, each with its own transaction data, list of senders and recipients, and timestamp.[2] However, the exact type of information stored in a block depends on the specific case, such as the exchange of digital currency, sale and transfer of land titles, records of intellectual property rights, or identity information.

For this report, the term "blockchain" refers to the digital ledger (i.e., record) of transactions. A "blockchain network" refers to the collection of nodes (i.e., computer or hardware systems) within a distributed network, for a specific blockchain. Each network has its own blockchain ledger. A "blockchain platform" is a technical infrastructure that supports blockchain operations and development, such as Ethereum or Solana, on which other features or blockchain-based applications can be built. Finally, "blockchain technologies" refers to the many different

[1] For an overview of blockchain, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

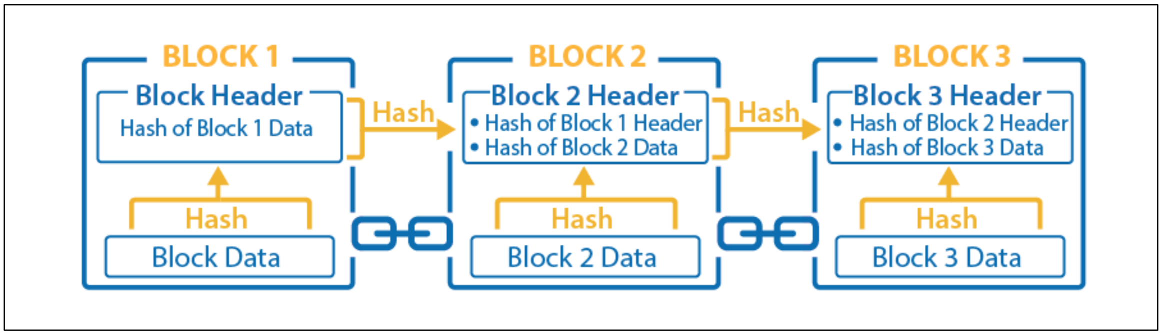
[2] For an in-depth technical explanation of blockchain, see Dylan J. Yaga, Peter M. Mell, and Nik Roby, et al., *Blockchain Technology Overview*, National Institute of Standards and Technology, NIST Interagency/Internal Report (NISTIR) 8202, Gaithersburg, MD, October 3, 2018, https://doi.org/10.6028/NIST.IR.8202.

implementations and applications of blockchains, such as decentralized apps (DApps), decentralized autonomous organizations (DAO), non-fungible tokens (NFT), and smart contracts, which are explored in the "DApps, DAOs, and NFTs" section of this report.

Chaining Blocks

In a blockchain, the blocks of data are cryptographically chained together through a hash function,[3] which refers to how each block contains unique data from the previous block. A hash function produces a string of characters as an output given some data as input. This is a one-way function, meaning a hash value may be created from an input, but the input cannot be recreated from the hash.[4] A number of blockchain transactions are grouped together to make a single block, which is then hashed. Any changes to one block would change the hash and immediately show in the subsequent block, thereby creating an immutable and tamper-resistant record of transactions.[5] As shown in **Figure 1**, each block contains a hash of the previous block's data and the main transaction data. The constant addition of new blocks is critical to maintaining a blockchain's security.[6]

Figure 1. Diagram of Blockchain and Cryptographic Linking



Source: CRS, adapted from Dylan J. Yaga, Peter M. Mell, and Nik Roby, et al., *Blockchain Technology Overview*, National Institute of Standards and Technology, NIST Interagency/Internal Report (NISTIR) 8202, Gaithersburg, MD, October 3, 2018, https://doi.org/10.6028/NIST.IR.8202.

Notes: Starting from the leftmost block in the diagram, the main block data (such as a transaction list, etc.) is hashed and stored in the current block header (along with other data such as a timestamp) (Block 1). The entire block header is hashed and stored in the next block's header (Block 2). The process repeats for each block (Block 3). Thus, each block will contain a hash from the previous block, which creates a chain of blocks that "reference" or "point" to one another. If a block's data was retroactively altered, it would automatically result in a different hash.

[3] There are various kinds of hash functions, such as SHA-256, Scrypt, and X11. Each hashing function has its own advantages and disadvantages for the blockchain's speed, energy-efficiency, and throughput.

[4] For more information on hash functions, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

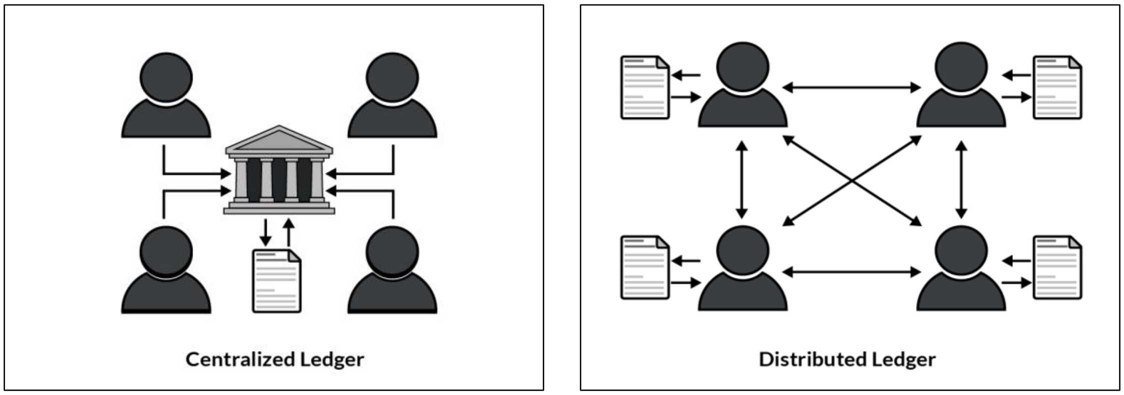
[5] If any data in a previous block is changed, it will result in a different hash, which alerts the blockchain network. This makes the blockchain immutable and tamper-resistant.

[6] In order to change the data in a particular block, the user must also change all subsequent blocks. In a "51% attack," a bad actor attempts to gain 51% of the computing power needed to generate blocks in a public, permissionless network. This type of attack is very difficult because the attacker must outpace the block creation rate of the rest of the network while new blocks are being continuously added.

Distributed Networks

The chained blocks of transaction data form a digital ledger that is stored and maintained by multiple parties in a distributed, peer-to-peer computer network (i.e., without centralized administration or use of an intermediary's repository).[7] The term ledger refers to a record or collection of transactions, which track the movement of money or goods from one entity to another. Conventionally, most records are digital and stored on servers maintained by a single entity or organization. Blockchain, however, creates multiple identical ledgers on individual computer systems or specialized hardware called nodes.[8] Through combining pre-existing technologies,[9] blockchain technologies enable peer-to-peer transactions and recordkeeping by sharing each update with participating nodes in the network as a record of activity for verification. The "safety in numbers" approach reduces the likelihood of fraud. Blockchain is one example of the larger category of distributed ledger technologies (DLTs).[10] **Figure 2** demonstrates the differences between centralized and distributed ledgers.

Figure 2. Centralized vs. Distributed Ledger Systems



Source: CRS, adapted from U.S. Government Accountability Office, *Blockchain & Distributed Ledger Technologies*, GAO-19-704SP, September 16, 2019, https://www.gao.gov/products/gao-19-704sp.

By publishing all blockchain transactions to all participating nodes, which node operators maintain and can constantly verify, proponents believe blockchain may enable more secure and transparent recordkeeping compared to traditional data management systems that use centralized

[7] Blockchain was created by an individual or group of people operating under the pseudonym "Satoshi Nakamoto." Satoshi Nakamoto published a white paper outlining a peer-to-peer digital payments system, which was the foundation for Bitcoin, the first application of blockchain. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008, http://satoshinakamoto.me/bitcoin.pdf.

[8] A "full" node stores the full blockchain data and verifies blocks; a "light" node only stores some of the blockchain data; a "publishing node" is a full node that also publishes new blocks.

[9] Blockchains combine many pre-existing technologies, including asymmetric key encryption, hash values, Merkle trees, and peer-to-peer networks. For more information on the technologies underlying blockchain, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

[10] Although definitions may differ, distributed ledger technologies (DLT) are often referred to as "a multi-party system in which participants reach agreement over a set of shared data and its validity, in the absence of a central coordinator. What separates DLT systems from traditional distributed databases are features rooted in designs capable of supporting data and maintaining data integrity in an adversarial environment." Michel Rauchs, Andrew Glidden, and Brian Gordon, et al., *Distributed Ledger Technology Systems: A Conceptual Framework*, University of Cambridge Centre for Alternative Finance, August 2018, pp. 19-20, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf.

databases maintained by a single organization. A fundamental idea behind blockchain is that an individual can trust the system as a whole without necessarily trusting any of the participants since there is a shared record of all transactions.

Types of Blockchains

There are many different types of blockchains, each with unique characteristics and applications. The four major types of blockchains—public, private, hybrid, and consortium blockchains—are shown in **Table 1**. However, all blockchain types share common characteristics, including immutability and a level of decentralization and pseudonymity. These characteristics are not prerequisites for a blockchain, but varying features. The balance among these characteristics may vary depending on the type of blockchain and specific implementation.

Public, Private, Hybrid, and Consortium Blockchains

Public blockchains allow anyone with an internet connection to access and "read" the blockchain ledger. Public blockchains feature a degree of pseudonymity by allowing participants to use verifiable aliases through public-private key cryptography.[11] Participants can use a public key to encrypt data, and a private key to decrypt the data.[12] Participants can also sign a transaction with their private key, and the recipient can verify the signature with the public key.[13] In such systems, linking identities to pseudonyms is computationally and data intensive. Access to private blockchains, typically run by a company for the benefit of that company or clients, is generally controlled. Unlike public blockchains, private blockchains require some level of identity verification before access is authorized. Private blockchains run by a group of entities are called consortium blockchains.

Hybrid blockchains combine elements of both public and private networks. Hybrid blockchains, or *side chains*, are controlled-access blockchains attached to a larger, public blockchain. Side chains may enable specific, authorized users to exchange sensitive information off the main blockchain. For example, the popular blockchain platform Ethereum enables developers to build private side chains.

Permissionless vs. Permissioned

Blockchain networks are either *permissionless* or *permissioned*, which is independent of whether the blockchain is *public* or *private*.

On *permissionless* blockchains, all nodes have equal rights, with any node able to view the full blockchain and potentially add additional blocks. *Permissioned* blockchains allow only authorized nodes to view the blockchain and validate blocks. Permissions may also be variable, with some nodes only able to view a portion of the blockchain, others able to view the whole

[11] Each key is a generated through a cryptographic algorithm. For more information on public-private key cryptography and blockchain, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

[12] "Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key." Cloudflare, *How Does Public Key Encryption Work? Public Jey Cryptography and SSL*, https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6 (1976), pp. 644-654, https://ieeexplore.ieee.org/iel5/18/22693/01055638.pdf.

[13] For more information on public and private keys, as well as encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran.

blockchain, and still others able to add and validate blocks. In a permissioned system, administrators control the rights of nodes on the blockchain, how many nodes are needed to validate a new block, and by what consensus mechanism. Different types of blockchains may offer varying levels of anonymity, speed, and efficiency.

Table 1. Types of Blockchains

	Ability to Validate Transactions	
Ability to Read and Submit Transactions	**Permissioned**	**Permissionless**
Public Blockchain	All nodes can read and submit transactions. Only authorized nodes can validate transactions. Examples: Sovrin	All nodes can read, submit, and validate transactions. No central entity manages blockchain membership. Examples: Ethereum, Bitcoin
Private Blockchain	Only authorized nodes can read, submit, and validate transactions.	NA (all private blockchains are permissioned by definition)
Hybrid Blockchain	Only authorized nodes can access the private chain, but all nodes can read, submit, and validate transactions on the public chain. All hybrid blockchains are in permissioned and permissionless categories.	
Consortium Blockchain	Only nodes authorized by the consortium can access the chain, and submit and validate transactions. Examples: Hyperledger Fabric	NA (all consortium blockchains are permissioned by definition)

Source: CRS, adapted from Roman Beck, Christoph Müller-Bloch, and John Leslie King, "Governance in the Blockchain Economy: A Framework and Research Agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10 (2018).

Blockchain technologies are often described as decentralized because of the use of distributed ledgers and lack of centralized servers. Decentralization, however, is not a condition of blockchain, but a varying feature, dependent on the type of blockchain and implementation. Many cloud service providers (CSP), such as Oracle and Amazon Web Services (AWS), offer cloud services for blockchain platforms.[14] Currently, AWS reports that 25% of all Ethereum nodes run on their services.[15] While a CSP might not act as a central validating authority, it becomes a third party to transactions on hosted blockchains.[16] However, in other services, a CSP may become a kind of central authority. For example, various companies have hired IBM, a CSP, to build their blockchains and host them in the IBM Cloud, rather than each individual company developing the necessary blockchain infrastructure internally.[17]

Different blockchain permission frameworks prioritize and balance factors such as transparency, speed, and security. For example, many cryptocurrencies, NFTs, and decentralized finance applications use public, permissionless, or hybrid blockchain networks. However, companies that adopt blockchain for their internal services typically use private or consortium blockchain

[14] For more information on Oracle's blockchain services, see "Oracle Blockchain," https://www.oracle.com/blockchain/.

[15] For more information on Amazon's blockchain services, see "Blockchain on AWS," https://aws.amazon.com/blockchain/.

[16] For information on peer-to-peer networks and CSPs, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

[17] For more information on IBM's blockchain services, see IBM, "IBM Blockchain Platform," https://www.ibm.com/cloud/blockchain-platform.

networks due to their increased efficiency. The various types of blockchain technologies may be of interest to Congress due to their varying levels of decentralization, security, and anonymity. For example, H.R. 6607 would have directed the Department of Health and Human Services to create a National Emergency Biodefense Network that tracks emergency health security supplies on a private blockchain. On the other hand, H.R. 2858 would have directed the National Institutes of Health to create a public, unalterable blockchain pilot project for endemic fungal disease research, most likely through using a public blockchain.

Consensus Mechanisms

In order for a block of data to be added to the blockchain, participating nodes must reach a consensus and agree to validate and verify the legitimacy of the block (i.e., verify that transactions follow the rules of a specific blockchain and properly reference the previous block).[18] There are various methods to validate blockchain transactions, known as a blockchain's consensus mechanism or consensus algorithm. Depending on the consensus mechanism, there are also different terms for the validation of a block, such as "mining," "forging," "minting," "earning," "harvesting," "staking," "creating," or "manufacturing."[19]

Blockchains use different consensus mechanisms depending on whether the blockchain is on a public or private and permissioned or permissionless network. Each type of consensus mechanism has implications for the security, sustainability, and concentrated ownership of the overall blockchain network.

The most common consensus mechanism for public blockchains is called Proof of Work (PoW), used by large networks such as Bitcoin and Ethereum. In a PoW blockchain network, miners compete against each other to solve the same task—a complex computational math problem.[20] The first miner to solve the problem validates the new block, adds it to the blockchain, and announces the addition to other nodes using peer-to-peer networking.[21] Other nodes operators verify the miner's solution and express their acceptance by using the hash of the newly-added block when validating the next block. Blockchain platforms, such as Bitcoin or Ethereum, typically award the successful miner a predetermined amount of cryptocurrency.

[18] For example, a Bitcoin transaction would need to follow the Bitcoin network protocol. For more information on the Bitcoin transaction validation process and requirements under the Bitcoin protocol, see "How Do Bitcoin Transactions Work?" https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/.

[19] In 2014, the Financial Crimes Enforcement Network (FinCEN) issued guidance on the regulation of cryptocurrency mining and other forms of transaction validation. Department of the Treasury Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf; Jamal El-Hindi, *Application of FinCEN's Regulations to Virtual Currency Mining*, Department of the Treasury Financial Crimes Enforcement Network, FIN-2014-R001, January 30, 2014, https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf.

[20] For most PoW blockchains, miners compete in a "hashing race" to find a nonce (an arbitrary random number) that will produce a certain hash value once put through a hashing function. The miners increment through nonce values until finding a hash value that meets the target criteria, which may change depending on the difficulty level. For more information on hashing and nonces, see Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, "Blockchain Technology Overview," NISTIR 8202, October 2018; and CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*, by Corrie E. Clark and Heather L. Greenley.

[21] The first miner is determined by whoever first broadcasts the "solved" block and proof-of-work solution. If two miners broadcast the block at the same time, nodes will work on both broadcasted blocks (creating two "branches" of the blockchain) until the next proof-of-work solution is found and one "branch" of the chain becomes longer.

The mining process is computationally intensive, by design, to deter bad actors. It is also energy intensive, since all competing miners simultaneously operate devices to solve the same math problem.[22] PoW networks automatically adjust problem difficulty in relationship to the average amount of time it takes to mine a new block.[23] Early miners on most public blockchain networks were able to use a desktop computer, but the increase in computational complexity and commensurate energy requirements needed to validate new blocks has shifted operations to computers with special mining hardware called application-specific integrated circuits. Some PoW miners have also joined "mining pools" to combine processing power with other miners and split rewards. As of January 2022, Bitcoin—the largest blockchain network in the world—consumes roughly the same amount of energy annually as nations such as Argentina, Sweden, and the United Arab Emirates.[24]

Some public blockchain networks have adopted alternative consensus mechanisms, such as Proof of Stake (PoS).[25] On a blockchain using a PoS consensus mechanism, users with a certain stake in the network can validate and add blocks in proportion to their stake.[26] For example, if a user owns 10% of a cryptocurrency blockchain network's total cryptocurrency, the user will be able to validate 10% of new blocks and receive the commensurate reward. This reduces the energy consumption relative to a PoW network. The second largest public blockchain network, Ethereum, announced in 2018 that it planned to transition from a PoW to a PoS consensus mechanism in order to improve transaction speed, network scalability,[27] and environmental sustainability. However, Ethereum has delayed its full move for years due to technical obstacles.[28]

Although blockchain is commonly associated with decentralization, a small number of major players or network operators dominate consensus mechanisms on most existing networks.[29] Seven mining pools account for nearly 80% of computing power on the Bitcoin network.[30] A

[22] For more information on the mining process and energy consumption of Proof of Work and cryptocurrency mining, see CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*, by Corrie E. Clark and Heather L. Greenley.

[23] According to Satoshi Nakamoto, the creator of Bitcoin, "To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases." See Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," paper, October 2008, https://bitcoin.org/bitcoin.pdf. Each block network has a different block time. Bitcoin's block time is 10 minutes, while Ethereum's block time is 12-14 seconds.

[24] "University of Cambridge Bitcoin Electricity Consumption Index," https://ccaf.io/cbeci/index.

[25] Paolo Tasca and Claudio J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," *Ledger*, vol. 4 (2019), pp. 1-39. For more information on specific consensus mechanisms, see Du Mingxiao, Ma Xiaofeng, and Zhang Zhe, et al., "A Review on Consensus Algorithm of Blockchain," *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, October 2017, https://doi.org/10.1109/SMC.2017.8123011.

[26] For example, after Ethereum moves to PoS, users must stake 32 ETH to become a validator. Similar to PoW mining pools, validators can combine their individual ownership stakes to form a "staking pool."

[27] Scalability refers to a blockchain network's ability to accommodate growth such as increased number of transactions, number of users, and number of validating users. Paolo Tasca and Claudio J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," *Ledger*, vol. 4 (2019), pp. 1-39, https://doi.org/10.5195/ledger.2019.140.

[28] Chris Morris, "Ethereum Update Defuses 'Difficulty Bomb' That Could Have Stopped Ether Crypto Mining," *Fortune*, December 8, 2021; Carl Beekhuizen, *Ethereum's Energy Usage Will Soon Decrease by ~99.95%*, Ethereum Foundation Blog, May 18, 2021, https://blog.ethereum.org/2021/05/18/country-power-no-more/.

[29] U.K. Office for Product Safety and Standards and Department for Business, Energy, & Industrial Strategy, *The Use of Distributed Ledgers to Verify the Provenance of Goods*, BEIS Research Paper Number 2020/036, September 2020, https://www.gov.uk/government/publications/use-of-distributed-ledger-technologies-to-verify-the-provenance-of-goods.

[30] See the pool distribution of Bitcoin and other large cryptocurrency networks, https://btc.com/stats/pool.

National Bureau of Economic Research study found that the top 50% of Bitcoin miners control nearly all Bitcoin mining capacity, the top 10% control 90%, and the top-most 0.1% of miners control close to 50% of Bitcoin mining.[31] If mining pools collaborate to own the majority of nodes on a public blockchain network, members could implement their own preferred rules or protocols. Hypothetically, these mining pools could forbid specific transactions.

Private and permissioned blockchain networks typically use less computationally and energy intensive consensus mechanisms than public blockchain networks.[32] Since only authorized users can see or add blocks to private, permissioned blockchains, there is an established level of trust between participants.

Governance and Protocols

Blockchain governance refers to the development and maintenance of a blockchain and its protocols, which govern the operation of a blockchain network. Protocols may specify how to execute transactions, how quickly new blocks of data may be added, and block size.[33] Node operators coordinate public blockchain network operations and the implementation of protocols. Assigned administrators oversee private blockchain operations and protocol implementation.

Some solutions to improve a blockchain's privacy, security, scalability, or other issues require protocol changes. In public blockchain networks, nodes can amend or change a blockchain's underlying protocol embedded in a blockchain's source code. These changes are called forks; categorized into *hard* or *soft* forks.[34] A *hard* fork refers to a change in the underlying blockchain protocol that requires all participating nodes to accept it, forcing network members to choose whether to follow the new or old protocol, thereby splitting the network. A *soft* fork changes a protocol by adding conditions to it and is backward compatible, since all of the features of the previous protocol remain in place. While nodes using the old protocol will recognize blocks using the new protocol, the reverse is not true. Soft forks do not split the blockchain and typically only require a majority of network members to accept the new protocol.

Many public blockchain networks have had to address governance issues. For example, following a $50 million hack, Ethereum underwent a hard fork after members of its community disagreed on the restoration of the stolen funds.[35] Ultimately, the core developers of Ethereum and the majority of participants agreed to implement a protocol change by forking the blockchain, fixing a bug in the source code, and moving funds back to the hacked account. Some blockchain applications, such as decentralized finance services, have introduced "governance tokens" to

[31] Igor Makarov and Antoinette Schoar, "Blockchain Analysis of the Bitcoin Market," *National Bureau of Economic Research Working Paper Series*, October 2021, http://www.nber.org/papers/w29396.

[32] Some private, permissioned blockchains use alternative consensus mechanisms, which are typically faster and less computationally intensive. Julien Polge, Jeremy Robert, and Yves Le Traon, "Permissioned Blockchain Frameworks in the Industry: A Comparison," *ICT Express*, vol. 7, no. 2 (June 2021), pp. 229-233, https://doi.org/10.1016/j.icte.2020.09.002; Wenbo Wang, Dinh Thai Hoang, and Peizhao Hu, et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, January 30, 2019, https://doi.org/10.1109/ACCESS.2019.2896108.

[33] Rowan van Pelt, Slinger Jansen, and Djuri Baars, et al., "Defining Blockchain Governance: A Framework for Analysis and Comparison," *Information Systems Management*, vol. 38, no. 1 (2021), pp. 21-41, https://doi.org/10.1080/10580530.2020.1720046.

[34] Dylan J. Yaga, Peter M. Mell, and Nik Roby, et al., *Blockchain Technology Overview*, National Institute of Standards and Technology, NIST Interagency/Internal Report (NISTIR) 8202, Gaithersburg, MD, October 3, 2018, https://doi.org/10.6028/NIST.IR.8202.

[35] "What Was the DAO?" Cryptopedia, https://www.gemini.com/cryptopedia/the-dao-hack-makerdao.

address governance issues and vote on decisions that guide and maintain the blockchain.[36] Users can buy governance tokens, which provide the holder with the right to vote on how the blockchain is maintained, upgraded, and managed.

Smart Contracts

Smart contracts on blockchain networks are collections of code that are automatically executed by network nodes if a specific set of conditions are met[37]—similar to "if A then B" statements in computer programming. The results of executing each contract provision are recorded as a transaction on the blockchain. For example, when certain criteria are met, a smart contract could transfer the ownership of an asset from one party's account—often referred to as a wallet—to another account for a set transaction cost. Often the more complex a smart contract's criteria, the higher the transaction costs for execution.

Although governments enforce contractual obligations and property rights, proponents argue smart contracts could complement or replace the services of some intermediaries, such as bankers, accountants, and lawyers.[38] However, disintermediation through smart contracts may face technical and legal obstacles, such as enforceability, among other issues.[39] Individual states such as Arizona, Nevada, and Tennessee have amended their state versions of the Uniform Electronic Transactions Act (UETA), which establishes the legal equivalence of electronic records to paper documents and signatures, to incorporate blockchains and smart contracts.[40]

NFTs, dApps, and DAOs

Smart contracts have enabled new blockchain applications. Some public blockchains that support smart contracts, such as Ethereum, enable developers to build and deploy NFTs, dApps, and Decentralized Autonomous Organizations (DAOs). NFTs have become popular as unique and non-interchangeable units of data (known as tokens), which can be used to represent the ownership of any unique item. NFTs are commonly used to represent the sole ownership of digital works, verify authenticity, and record ownership history.[41] dApps allow developers to build software applications that reside and operate on a blockchain network rather than the servers of a company that provides a web application. Open Sea, the largest NFT marketplace, is an example of a dApp built on the Ethereum blockchain. dApps can use smart contracts to enable transactions between anonymous parties without exchanging personal information. DAOs are

[36] Jake Ryan, "Who Writes the Rules of a Blockchain?" *Harvard Business Review*, July 23, 2021, https://hbr.org/2021/07/who-writes-the-rules-of-a-blockchain; Patrick Murck, "Who Controls the Blockchain?" *Harvard Business Review*, April 19, 2017, https://hbr.org/2017/04/who-controls-the-blockchain.

[37] Dylan Yaga, Peter Mell, and Nik Roby, et al., "Blockchain Technology Overview," NISTIR 8202, October 2018.

[38] "Could Blockchain-Based Smart Contracts Eventually Replace Lawyers?" Monash University Blockchain Technology Centre, https://www.monash.edu/blockchain/news/could-blockchain-based-smart-contracts-eventually-replace-lawyers.

[39] Eliza Mik, "Smart Contracts: Terminology, Technical Limitations," *Law, Innovation and Technology*, vol. 9, no. 2 (2017), pp. 269-300, https://doi.org/10.1080/17579961.2017.1378468.

[40] A.J. Bosco, "Blockchain and the Uniform Electronic Transactions Act," *The Business Lawyer*, vol. 74 (Winter 2018-2019), pp. 243-251, https://www.americanbar.org/content/dam/aba/publications/business_lawyer/2019/74_1/survey-cyberspace-blockchain-201902.pdf.

[41] For more information on the financial regulation and oversight of NFTs, see pages 19-20 of CRS Report R46208, *Digital Assets and SEC Regulation*, by Eva Su.

groups whose rules are encoded and transactions are executed using smart contracts, eliminating intermediaries. DAOs require member voting to make organizational changes.

Blockchain in Provenance Applications

Proponents assert that blockchain technologies can be used to ensure the provenance of physical and digital items without the need for a centralized authority or intermediary. For example, knowing the provenance of an item can prove its history, thereby ensuring the item's safety or legitimacy. Since transactions must be approved through a consensus mechanism and blocks are subsequently hashed, attempts to alter provenance records for digital or physical goods will leave an auditable trail, thereby alerting users to potential tampering. Blockchain provenance applications are likely to be most relevant for

1. transactions where there is not complete trust between parties;
2. markets characterized by error, delay, or fraud; or
3. contexts with existing digital infrastructure.[42]

Supply Chain Provenance

Supply chain traceability is important for highly-regulated industries with product contamination and counterfeit risks, such as the food and pharmaceutical industries. Some academics and companies have proposed using blockchain technologies to ensure product and process integrity and for tracking items—such as food products, vaccines, and prescription drugs—throughout their respective supply chains.[43]

The Food and Drug Administration (FDA) New Era of Smarter Food initiative builds upon the FDA's work to implement P.L. 111-353, also known as the FDA Food Safety Modernization Act (FSMA).[44] The initiative aims to prevent foodborne outbreaks by implementing digital traceability in food supply chains enabled by blockchain, artificial intelligence, and other emerging technologies.[45]

[42] Paul Nelson, *Primer on Blockchain: How to Assess the Relevance of Distributed Ledger*, United States Agency for International Development, April 27, 2018, https://www.usaid.gov/sites/default/files/documents/15396/USAID-Primer-Blockchain.pdf.

[43] Vishal Gaur and Abhinav Gaiha, "Building a Transparent Supply Chain," *Harvard Business Review Magazine*, May-June 2020, https://hbr.org/2020/05/building-a-transparent-supply-chain; "Continuous Interconnected Supply Chain: Using Blockchain & Internet-of-Things in Supply Chain Traceability," Deloitte, 2017, https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-internet-things-supply-chain-traceability.pdf.

[44] For more information on the FDA Food Safety Modernization Act, see CRS Report R43724, *Implementation of the FDA Food Safety Modernization Act (FSMA, P.L. 111-353)*, by Renée Johnson.

[45] U.S. Food and Drug Administration, *New Era of Smarter Food Safety: FDA's Blueprint for the Future*, July 2020, https://www.fda.gov/food/new-era-smarter-food-safety/new-era-smarter-food-safety-blueprint. Suman Bhattacharyya, "FDA Official Says New Rule Could Boost Blockchain-Based Food Tracking," *Wall Street Journal*, February 1, 2022, https://www.wsj.com/articles/fda-official-says-new-rule-could-boost-blockchain-based-food-tracking-11643711402.

In 2018, IBM launched the IBM Food Trust Program to provide companies a permissioned blockchain that records food system data.[46] Walmart's Food Traceability Initiative[47] uses the program to track over 500 food items.[48] In 2020, Walmart assisted the FDA with six investigations into food safety and provided investigators with detailed information on the original source of a potential contamination within an hour using blockchain ledgers, a task which previously took up to seven days.[49] In 2021, Walmart also worked with U.S. Customs and Border Protection to pilot a program to track imported foods.[50]

Pfizer, McKesson, and other pharmaceutical companies are testing the use of blockchain technologies to trace medicine from the factory to the patient, to help ensure authenticity and safety.[51] The Drug Supply Chain Security Act (DSCSA) established requirements to facilitate the tracing and verification of certain prescription drug products through the U.S. pharmaceutical distribution supply chain.[52] The FDA created a DSCA Pilot Project Program to assist drug supply chain stakeholders in developing an interoperable, electronic tracing system. IBM, KPMG, Merck, and Walmart were some of the selected program participants. Under the project title "DSCSA Blockchain Interoperability Pilot," the companies developed a shared, permissioned blockchain network to allow for real-time monitoring of drugs.[53] Based on similar models for global food supply chains, the DSCSA program uses new technologies like blockchain to trace prescription drugs and improve the security of drug supply chains.[54]

[46] IBM, "IBM Food Trust Expands Blockchain Network to Foster a Safer, More Transparent and Efficient Global Food System," press release, October 8, 2018, https://newsroom.ibm.com/2018-10-08-IBM-Food-Trust-Expands-Blockchain-Network-to-Foster-a-Safer-More-Transparent-and-Efficient-Global-Food-System-1. Aaron Stanley, "Ready to Rumble: IBM Launches Food Trust Blockchain for Commercial Use," *Forbes*, October 8, 2018, https://www.forbes.com/sites/astanley/2018/10/08/ready-to-rumble-ibm-launches-food-trust-blockchain-for-commercial-use.

[47] Walmart, "Food Traceability Initiative: Fresh Leafy Greens," press release, September 24, 2018, https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/_proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001.

[48] For more information on the Walmart Food Traceability Initiative, see CRS In Focus IF11829, *Blockchain Technology and Agriculture*, by Genevieve K. Croft; Michael del Castillo, "Blockchain 50 2021," *Forbes*, February 2021, https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/.

[49] Joanne Molinaro, Nathan Beaver, Kathleen Wegrzyn, Gary Solomon, and Eugenia Wang, "The Fast Track: Using Blockchain to Trace Products Through the Supply Chain," Foley & Lardner LLP, September 9, 2021.

[50] Michael del Castillo, "Blockchain 50 2021," *Forbes*, February 2021.

[51] Lucas Mearian, "How Pharma Will Soon Use Blockchain to Track Your Drugs," *ComputerWorld*, September 23, 2019, https://www.computerworld.com/article/3439843/how-pharma-will-soon-use-blockchain-to-track-your-drugs.html; Alison, McCauley, "Why Big Pharma Is Betting on Blockchain," *Harvard Business Review*, May 29, 2020, https://store.hbr.org/product/why-big-pharma-is-betting-on-blockchain/H05NDT.

[52] Food and Drug Administration, "Verification Systems Under the Drug Supply Chain Security Act for Certain Prescription Drugs; Draft Guidance for Industry; Availability," 87 *Federal Register* 47, March 10, 2022, https://www.fda.gov/media/117950/download.

[53] For more information on the Drug Supply Chain Security Act Pilot Project Program (DSCSA Pilot Project), see program details, https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program. "FDA DSCSA: Blockchain Interoperability Pilot Project Report," IBM, KPMG, Merck, Walmart, February 2020, https://institutes.kpmg.us/content/dam/institutes/en/healthcare-life-sciences/pdfs/2020/blockchain-interoperability-pilot-project-report.pdf.

[54] U.S. Food and Drug Administration, "FDA Takes New Steps to Adopt More Modern Technologies for Improving the Security of the Drug Supply Chain Through Innovations That Improve Tracking and Tracing of Medicines," press release, February 7, 2019, https://www.fda.gov/news-events/press-announcements/fda-takes-new-steps-adopt-more-modern-technologies-improving-security-drug-supply-chain-through.

Some companies and organizations have used blockchain technologies to collect and verify environmental, social, and corporate governance (ESG) data, including tracking product provenance and source materials to identify labor, human rights, and environmental violations. For example, in 2018, the State Department launched its first blockchain project with Coca-Cola to create a secure registry for workers to help prevent the use of forced labor, child labor, and other exploitative practices in countries where they procure sugarcane.[55] Other groups, such as the World Wildlife Fund[56] and Everledger,[57] use blockchain to track the provenance of products to help ensure they are not sourced from vulnerable ecosystems.

The use of blockchain technologies in supply chain management requires the necessary technical infrastructure to capture, verify, and upload data, which may be difficult for smaller-scale producers,[58] and would require standardization and coordination between actors throughout a particular supply chain. Additionally, the use of blockchain technologies does not ensure the accuracy of collected data. Producers could upload false data about their products or practices to circumvent or abuse traceability systems. Blockchain technologies can also add unnecessary complexity compared with using conventional databases or other alternatives.

Identity and Credential Provenance

Blockchain technologies have also been used for identity-management and credentialing systems, often using "digital wallet" technology to store digital credentials.[59] A digital wallet refers to software designed to store a user's private keys corresponding to anything from cryptocurrency to identifiers and credentials. There are generally two kinds of blockchain identity-management systems: top-down and self-sovereign.[60] In a top-down identity management system, a central authority still issues or has control over the origination of the credential or identifier, which a user may store in a digital wallet. For example, IBM created a blockchain-based "Digital Health Pass" to let organizations verify an individual's accurate health credentials such as vaccine records, COVID-19 test results, and temperature checks.[61] In 2021, New York launched its platform for COVID-19 test results and proof of vaccination on IBM's Digital Health Pass.[62]

[55] Gertrude Chavez-Dreyfuss, "Coca-Cola, U.S. State Dept to Use Blockchain to Combat Forced Labor," *Reuters*, March 16, 2018, https://www.reuters.com/article/us-blockchain-coca-cola-labor/coca-cola-u-s-state-dept-to-use-blockchain-to-combat-forced-labor-idUSKCN1GS2PY.

[56] Kate Whiting, "Blockchain Could Police the Fishing Industry—Here's How," World Economic Forum, February 12, 2020, https://www.weforum.org/agenda/2020/02/blockchain-tuna-sustainability-fisheries-food-security/.

[57] CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

[58] William Crumpler, Marti Flacks, and Amith Mandavilli, *The Human Rights Risks and Opportunities in Blockchain*, Center for Strategic and International Studies (CSIS), December 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211214_Crumpler_HumanRights_Blockchain.pdf.

[59] Wallets may take various forms, such as dedicated hardware wallets, mobile applications, or even paper wallets (i.e., private keys that are private and kept in a safe location). Wallet services called custodial wallets can also be provided by a third-party holder that controls a user's private keys.

[60] Loïc Lesavre, Priam Varin, and Peter Mell, et al., *A Taxonomic Approach to Understanding*, National Institute of Standards and Technology, NIST Cybersecurity White Paper, January 14, 2020, https://doi.org/10.6028/NIST.CSWP.01142020.

[61] For more information on the IBM Digital Health Pass, see https://www.ibm.com/products/digital-health-pass.

[62] New York State Governor's Press Office, "Governor Cuomo Announces Launch of Excelsior Pass to Help Fast-Track Reopening of Businesses and Entertainment Venues Statewide," press release, March 26, 2021, https://www.governor.ny.gov/news/governor-cuomo-announces-launch-excelsior-pass-help-fast-track-reopening-businesses-and.

In a self-sovereign identity system, there are no central authorities with control over identifiers or credential issuance.[63] Users may manage their own identifiers by storing them locally on their own devices or on a distributed network, and then grant selected parties access to their information.[64] A self-sovereign identity system typically uses a decentralized identifier (DID), which contains a uniform resource locator (URL) or uniform resource identifier (URI) that points to publicly identifying information about the user. The rules of the identity management system are often implemented through smart contracts.

Blockchain-based identity systems may be a core component of Web3, a proposed blockchain-based internet,[65] or be used for proving identity on the existing web. However, the storage of personally identifiable information, biometric data, or other information on blockchains could introduce new privacy and security risks. Additionally, users need access to a reliable internet connection and a smartphone or computer to download and use an identity management system's wallet application, which may exclude significant parts of the population.

Registries and Asset Provenance

Blockchain technologies could enable the transfer of rights to digital and physical assets, such as equipment, land titles, and intellectual property, and help maintain the timeliness and accuracy of public records. However, there are possible legal ramifications and security issues for asset transfers built on blockchains and smart contracts.

The Department of the Treasury's Bureau of the Fiscal Service's Office of Financial Innovation and Transformation (FIT) has begun to experiment with using blockchain technology in their services.[66] In 2017, FIT launched a pilot blockchain prototype to track and manage physical assets such as government-issued computers and cell phones. The pilot project tested whether the inventory of an agency's physical assets could be continuously monitored and reconciled in real time as the assets were transferred among employees. The pilot expanded to track software licenses, and as of 2020, the pilot was on its third iteration.[67] In collaboration with the National Science Foundation (NSF), FIT also conducted two proof-of-concept[68] tests using blockchain to facilitate federal grant payments. FIT identified benefits in using blockchain, but also legal, technical, and governance challenges to overcome in the next phase of the project.[69]

Transferring land titles or deeds can be time-consuming and expensive since multiple authorities may hold the information required to complete a transaction. Proponents argue using blockchain technologies makes recording and transferring titles easier and more efficient and records tamper-

[63] Ibid, p. 15.

[64] Fennie Wang and Primavera De Filippi, "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion," *Frontiers in Blockchain*, vol. 2 (January 23, 2020), https://doi.org/10.3389/fbloc.2019.00028.

[65] CRS In Focus IF12075, *Web3: A Proposed Blockchain-Based, Decentralized Web*, by Kristen E. Busch.

[66] Public-Private Analytic Exchange Program, *Blockchain and Suitability for Government*, U.S. Department of Homeland Security, 2018, https://www.hsdl.org/?abstract&did=825735; "Bureau of the Fiscal Service Launches Two Innovative Pilot Projects," Bureau of the Fiscal Service Financial Innovation & Transformation Blog, October 2, 2017, https://www.fiscal.treasury.gov/fit/blog/innovative-pilot-projects.html.

[67] Amelia Brust, "Bureau of Fiscal Service Sees Potential for Blockchain, AI in New Pilot Programs," *Federal News Network*, February 11, 2020, https://federalnewsnetwork.com/automation/2020/02/bureau-of-fiscal-service-sees-potential-for-blockchain-ai-in-new-pilot-programs/.

[68] A proof of concept is typically an early-stage prototype or pilot project.

[69] "Another Link in the Chain," Bureau of the Fiscal Service Financial Innovation & Transformation Blog, May 17, 2021, https://www.fiscal.treasury.gov/fit/blog/another-link-in-the-chain.html.

resistant and more easily auditable.[70] For example, smart contracts may enable the transfer of assets without the need for intermediaries or escrow services.

In 2016, Cook County, the largest county in Illinois, piloted putting its real estate title registration and land records on a blockchain, in part to decrease the number of steps where information had to be transferred from one party to another.[71] The pilot intended for all parties to record information on the blockchain, creating a single place to share and access data. At the end of the pilot, the Cook County Recorder of Deeds did not undertake large-scale conversions to blockchain due to office consolidations. Other countries such as Sweden and Georgia also use blockchain-based land titling systems to facilitate various services and help prevent against fraud and manipulation of property deeds.[72] Sweden's Lantmäteriet, the land mapping and registration authority, has also tested blockchain technology and smart contracts (requiring human approval) for recording property sales and managing land conveyance. The pilot, started in 2016, used smart contracts to require the buyer's bank to sign-off using a private key. The land registry also had to sign approval. The project decreased the numbers of steps in the process from 34 to 13 and significantly increased speed.[73]

Content creators and companies may use blockchain technologies to represent ownership of intellectual property, including digital items or the representation of goods in the physical world, enabling proof of ownership.[74] Some companies have filed trademark applications for their NFTs. For example, Nike filed a trademark application to sell NFTs of its sneakers and other goods. Most NFTs are automatically deployed and transferred between owners using smart contracts.

Although smart contracts may be able to automate the transfer of assets when specific conditions are met, they also pose new risks to legacy systems. Contract law is determined at the state level, but many states have not recognized the legal status or enforceability of smart contracts.[75] Additionally, bugs in smart contract code or errors in instructions may expose users to significant risk or mistaken loss of assets if an automated transfer executes automatically. Although smart contracts may be open source, meaning anyone can examine the code for potential weaknesses, many users may lack the technical knowledge necessary for inspection.

[70] "Blockchain in Commercial Real Estate: The future Is Here," Deloittee Center for Financial Services, December 1, 2016, https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html.

[71] Adrianne Jeffries, "Governments Explore Using Blockchains to Improve Service," *New York Times,* June 27, 2018, https://www.nytimes.com/2018/06/27/business/dealbook/governments-blockchains-services.html. Joanne Cleaver, "Could Blockchain Technology Transform Homebuying in Cook County—and Beyond?" *Chicago Tribune,* July 9, 2018, https://www.chicagotribune.com/real-estate/ct-re-0715-blockchain-homebuying-20180628-story.html.

[72] Georg Eder, "Digital Transformation: Blockchain and Land Titles," OECD Global Anti-Corruption & Integrity Forum, March 2019; Qiuyun Shang and Allison Price, "A Blockchain-Based Land Titling Project in The Republic of Georgia," *Innovations Technology Governance Globalization*, vol. 12, no. 3-4 (January 2019), pp. 72-78, https://doi.org/10.1162/inov_a_00276.

[73] Shefali Anand, "A Pioneer in Real Estate Blockchain Emerges in Europe," *Wall Street Journal*, March 6, 2018, at https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601. William Crumpler, Marti Flacks, and Amith Mandavilli, *The Human Rights Risks and Opportunities in Blockchain,* CSIS, p. 47.

[74] Massimo Franceschet, Giovanni Colavizza, and T'ai Smith, et al., "Crypto Art: A Decentralized View," *Leonardo*, vol. 54, no. 4 (September 9, 2021), pp. 402-405, https://doi.org/10.1162/leon_a_02003.

[75] Stuart D. Levi and Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, Harvard Law School Forum on Corporate Governance, May 26, 2018, https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

Other Blockchain Applications

As blockchain technologies continue to mature, experts predict they will find application in a variety of sectors and fields. For example, some have proposed blockchain technologies as a solution for electronic voting systems,[76] integration with the Internet of Things (IoT),[77] smart grids,[78] distribution of social welfare benefits,[79] and peer-to-peer carbon-credit trading and carbon tracking.[80] These applications may introduce new benefits and risks in each sector.

Domestic and International Initiatives and Regulatory Frameworks

This section discusses the state and international regulatory frameworks and other initiatives around blockchain technologies. Some states and countries have taken vastly different approaches to blockchain, so the regulations that do exist vary widely.

State Regulatory Frameworks

Individual states have passed legislation or established initiatives to develop, incentivize, and regulate blockchain technologies. For example, in 2021, Wyoming passed legislation allowing the state to recognize DAOs as limited liability companies, in addition to creating sales and property tax exemptions for cryptocurrency transactions.[81] This has been part of a larger effort by many

[76] In 2019, the United States Postal Service built a blockchain-based mobile voting system, but encountered multiple security and privacy issues. Joseph Marks and Aaron Schaffer, "The Postal Service Secretly Built a Risky Mobile Voting System," *Washington Post*, December 14, 2021; Joseph Marks and Jacob Bogage, "USPS Built and Secretly Tested a Mobile Voting System Before 2020," *Washington Post,* December 13, 2021. In the 2018 primary and general elections, West Virginia piloted a mobile voting application powered by blockchain for absentee ballots. Alaska has also introduced legislation to adopt blockchain technology statewide in its voting security system. However, some scholars have questioned the cybersecurity risks of blockchain-based voting. Sunoo Park, Michael Specter, et al., "Going from Bad to Worse: From Internet Voting to Blockchain Voting," *Journal of Cybersecurity*, vol. 7, no. 1, (Feburary 16, 2021), pp. 1-15.

[77] IoT is a system of interrelated devices connected to a network and/or to one another, exchanging data without necessarily requiring human-to-machine interaction. In other words, IoT is a collection of electronic devices that can share information among themselves. For more information on the integration of IoT and blockchain, see T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, (2018), pp. 32979-33001. For more information on IoT itself, see CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Patricia Moloney Figliola; and CRS In Focus IF11239, *The Internet of Things (IoT): An Overview*, by Patricia Moloney Figliola.

[78] For information on the integration of blockchain and smart grids, see Shen Wang, Ahmad F. Taha, and Jianhui Wang, et al., "Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8 (August 2019), pp. 1612-1623.

[79] Blockchain may enable the distribution of government benefits. For example, the U.N. World Food Programme provided blockchain-based cash transfers to Syrian refugees in Jordan, which avoided complications with banking fees, physical cash, vouchers, or electric cards. "How Blockchain Technology Is Helping Refugees Grocery Shop in Conflict Zones," World Food Program USA, December 23, 2020, at https://www.wfpusa.org/articles/blockchain-tech-helps-refugees-grocery-shop-in-conflict-zones/.

[80] Peter Howson, "Tackling Climate Change with Blockchain," *Nature Climate Change*, vol. 9 (August 19, 2019), p. 644–645. "The Good, the Bad and the Blockchain," United Nations Framework Convention on Climate Change (UNFCCC), May 17, 2021.

[81] Wyoming CH0162, https://www.wyoleg.gov/Legislation/2021/SF0038; Elena Botella, "Wyoming Wants to Be the Crypto Capital of the U.S." *Slate*, June 28, 2021, https://slate.com/technology/2021/06/wyoming-cryptocurrency-laws.html.

state governments to foster blockchain and cryptocurrency development, and attract companies to relocate to their states. Similarly, Texas has amended its Uniform Commercial Code to include a definition of virtual currency and clarify that certain business laws apply to cryptocurrencies.[82] Many states have amended their money service business (MSB) or money transmitter regulations to include cryptocurrency transactions.[83] Some state legislatures have introduced legislation to tax cryptocurrencies, prohibit cryptocurrency mining, study the environmental impacts of cryptocurrency, and investigate state government use of blockchain technologies.[84] Potential federal regulation of blockchain provenance applications may complement or interact with state-level blockchain regulations.

In 2016, Illinois established the Illinois Blockchain Initiative, which includes a consortium of state and county agencies, to collaborate on the integration of blockchain technologies into the delivery of state services.[85] The Cook County Recorder of Deeds, which piloted the aforementioned real estate blockchain project, also provided recommendations to the Illinois Blockchain Initiative. In 2016, the Delaware state government launched the Delaware Blockchain Initiative to provide a regulatory and legal environment for blockchain development, as well as testing blockchain within government services.[86] California created a Blockchain Working Group in 2019, which published policy recommendations to define blockchain, evaluate the legal implications of distributed ledger technologies, and recommend amendments to statutes that may be impacted by the application of blockchain technologies.[87] However, many state blockchain initiatives have struggled to implement the technology.[88] The Illinois Blockchain Initiative identified various limitations to government adoption, such as issues with scalability and smart contract security, and Delaware's project never launched due to potential cost concerns.[89] These state-level initiatives may present opportunities for Congress to consider the role of the federal government in blockchain development or regulation, as well as identify best practices and potential risks.

[82] Texas CH739, https://legiscan.com/TX/bill/HB4474/2021.

[83] CRS Report R46486, *Telegraphs, Steamships, and Virtual Currency: An Analysis of Money Transmitter Regulation*, by Andrew P. Scott.

[84] See "Blockchain 2021 Legislation" and "Cryptocurrency 2021 Legislation," maintained by the National Conference of State Legislatures (NCSL), https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2021-legislation.aspx.

[85] For more information on the Illinois Blockchain Initiative, see the Illinois Blockchain Task Force Final Report and general background, https://www2.illinois.gov/sites/doit/Pages/BlockChainInitiative.aspx.

[86] Delaware Office of the Governor, "Governor Markell Launches Delaware Blockchain Initiative," press release, April 2, 2016, https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html; Andrea Tinianow and Caitlin Long, "Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance," *Harvard Law School Forum on Corporate Governance*, March 16, 2017, https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/.

[87] See the California Blockchain Working Group webpage, https://www.govops.ca.gov/blockchain/.

[88] Colin Wood, "What Happened with Blockchain in State Government?" *StateScoop*, November 23, 2021, https://statescoop.com/what-happened-with-blockchain-in-state-government/.

[89] Karl Baker, "Delaware Eases off Early Blockchain Zeal After Concerns over Disruption to Business," *Delaware Online*, February 1, 2018, https://www.delawareonline.com/story/news/2018/02/02/delaware-eases-off-early-blockchain-zeal-after-concerns-over-disruption-business/1082536001/.

International Regulatory Frameworks

This section highlights the regulatory frameworks for blockchain technologies and their applications developed by China and the European Union.

China

China has supported the adoption of blockchain technologies[90] and leads the world in blockchain patent applications.[91] The Chinese government has facilitated the development of blockchain technologies through the Blockchain-based Service Network (BSN), which provides Chinese businesses a "global infrastructure network used to deploy and operate all types of blockchain applications."[92] In 2019, the Cyberspace Administration of China issued the "Administrative Provisions on Blockchain Information Services," a set of rules governing blockchain-based information services that required authentication of users' real identities.[93] In 2020, China also launched the National Blockchain and Distributed Accounting Technology Standardization Technical Committee to create national standards for the industry.[94]

While simultaneously supporting blockchain development, China has also banned cryptocurrencies in order to protect the dominance of its government-run digital currency, officially called the Digital Currency Electronic Payment (DCEP).[95] The DCEP is referred to as the digital renminbi (digital RMB) or digital yuan (e-CNY), but does not use blockchain. The DCEP is one of the most developed examples of a Central Bank Digital Currency (CBDC). Many other countries and central banks are exploring the option of CBDCs, which has raised issues about competition with the U.S. dollar, efficacy of monetary policy, and privacy concerns.[96]

In September 2021, China officially banned all cryptocurrency transactions and cryptocurrency mining.[97] These actions caused a global drop in the total amount of cryptocurrency mining and

[90] Alice Ekman, *China's Blockchain and Cryptocurrency Ambitions: The First-Mover Advantage*, European Union Institute for Security Studies, July 13, 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_15_2021.pdf.

[91] See Francis Gurry, "China Becomes Top Filer of International Patents in 2019 amid Robust Growth for WIPO's IP Services, Treaties and Finances," World Intellectual Property Organization, April 7, 2020, https://www.wipo.int/pressroom/en/articles/2020/article_0005.html.

[92] For more information on the Blockchain-based Service Network (BSN), see the BSN's "Introductory White Paper," https://bsnbase.io/static/tmpFile/BSNIntroductionWhitepaper.pdf.

[93] Laney Zhang, "China: Rules on Blockchain-Based Information Services Issued Requiring Authentication of Users' Real Identities," The Law Library of Congress, February 12, 2019, https://www.loc.gov/law/foreign-news/article/china-rules-on-blockchain-based-information-services-issued-requiring-authentication-of-users-real-identities/.

[94] Arjun Kharpal, "Chinese Giants Huawei and Tencent Join National Group on Blockchain After Xi's Backing for the Tech," *CNBC*, April 15, 2020, https://www.cnbc.com/2020/04/15/huawei-tencent-on-china-blockchain-national-committee.html.

[95] Ryan Browne, "Central Bank Digital Currencies Are a Long Way from Becoming Reality—Unless You're in China," *CNBC*, November 12, 2021, https://www.cnbc.com/2021/11/12/central-bank-digital-currencies-are-moving-slowly-but-not-in-china.html; Arjun Kharpal, "China Has Given Away Millions in Its Digital Yuan Trials. This Is How It Works," *CNBC*, March 4, 2021, https://www.cnbc.com/2021/03/05/chinas-digital-yuan-what-is-it-and-how-does-it-work.html.

[96] For more information on CBDCs and China's digital currency efforts, see CRS Report R46850, *Central Bank Digital Currencies: Policy Issues*, by Marc Labonte and Rebecca M. Nelson.

[97] Alun John, Samuel Shen, and Tom Wilson, "China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling," *Reuters*, September 24, 2021, https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/.

mining difficulty since 70-80% of mining previously occurred in China.[98] Since the ban, many Chinese companies have moved their mining equipment and operations to the United States and other countries, where cryptocurrencies are currently unregulated for the most part.[99] It remains to be seen how these policy changes will impact the distribution and growth of blockchain technologies across the world, and particularly in the United States.

European Union

In 2018, EU member states launched the European Blockchain Partnership (EBP), which stresses the potential of blockchain-based services for the benefit of citizens, society, and the economy.[100] The EBP currently includes all 27 EU member states, plus non-EU members Norway and Liechtenstein. As part of this commitment, the EBP is building a European Blockchain Services Infrastructure (EBSI), which will deliver public services (e.g., notarization, managing educational or identity credentials, data sharing among EU authorities) using blockchain technology.[101] In 2020, EBSI deployed a network of distributed blockchain nodes across Europe to support applications focused on selected use-cases, including digital credentials and identity management systems. Similar to a digital wallet for storing cryptocurrencies, the EBSI wallet could store a user's credentials and documentation, such as diplomas or verifiable IDs.

Due to the immutability of blockchain ledgers, there have been concerns in the EU about how to treat blockchain technologies within existing legal frameworks, particularly the EU's General Data Protection Regulation, which establishes rules for the protection of personal data and outlines individual rights, including a "right to be forgotten."[102] A 2018 European Parliament resolution underlined that the European Data Protection Supervisor (EDPS), the EU's independent data protection authority, should provide further clarification on how blockchain technologies may affect EU legislation on data protection.[103]

Considerations for Congress

There are a range of options, if Congress determines there is an appropriate role for the U.S. government, to support and incentivize the development of blockchain or regulate risks and potential adverse outcomes.

Regulatory Authority and Federal Agencies

Some federal entities, such as the Treasury Department, Securities and Exchange Commission (SEC), Commodity Futures Trading Commission and others, have applied existing regulatory

[98] Michel Rauchs, "Geographic Shift," *University of Cambridge Judge Business School*, October 13 2021, https://www.jbs.cam.ac.uk/insight/2021/geographic-shift/.

[99] Martha Muir, "China's Exiled Crypto Machines Fuel Global Mining Boom," *Financial Times*, November 22, 2021, https://www.ft.com/content/0dbe4f9f-a433-4288-858e-c4b852f4c340.

[100] "European Countries Join Blockchain Partnership," April 10, 2018, https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership.

[101] For more information on the EBSI, see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

[102] CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

[103] For more information on EDPS and blockchain, see https://edps.europa.eu/data-protection/our-work/subjects/technologies/blockchain_en. "Blockchain and the General Data Protection Regulation," Panel for the Future of Science and Technology, European Parliamentary Research Service, July 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

authorities to the use of blockchain technologies and released guidance addressing specific financial applications, such as cryptocurrencies and initial coin offerings (ICOs).[104]

The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Federal Reserve have established a Digital Assets Sprint Initiative to support agency collaboration on digital asset policies.[105] The Initiative intends to develop a common taxonomy for digital assets and a set of agreed upon definitions of basic terms. In 2021, the Department of Justice and Treasury Department jointly created a National Cryptocurrency Enforcement Team to conduct investigations and prosecutions of criminal misuses of cryptocurrency, including crimes committed by virtual currency exchanges and the use of cryptocurrencies and blockchain-based digital assets in money laundering.[106]

Similar collaborative initiatives in sectors such as healthcare, agriculture, transportation, and supply chain management, could be considered as the use of non-financial blockchain applications expands. Similar to the guidance released on cryptocurrencies and ICOs, Congress could direct federal agencies to create guidance on non-financial blockchain applications, such as the provenance uses discussed earlier in this report.

Policy Considerations and Risks

Blockchain technologies may be useful in certain applications but also may present new risks. For example, data recorded on a blockchain may have ramifications for user privacy and security. Any data added to a public, permissionless blockchain will be viewable by all participating nodes indefinitely. Because blockchain records are immutable, any error in a record associated with an individual may persist despite efforts to correct it,[107] with potential ramifications for authenticating identity or completing transactions. In order to comply with the EU's GDPR regulations and other privacy requirements, such as the right to be "forgotten," NIST has explored the possibility of an "editable blockchain."[108] NIST's proposed system could allow for the

[104] Strategic Hub for Innovation and Financial Technology, *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. Securities and Exchange Commission, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1. Commodity Futures Trading Commission, "Retail Commodity Transactions Involving Certain Digital Assets," 85 *Federal Register* 37734-37744, June 24, 2020. U.S. Treasury Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models*, FIN-2019-G001, May 9, 2019, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models. U.S. Department of the Treasury's Office of Foreign Assets Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, September 21, 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. Jonathan V. Gould, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers*, Office of the Comptroller of the Currency, Interpretive Letter #1170, July 22, 2020, https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf. 26 C.F.R. §§ 1.61-1.

[105] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, "Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps," press release, November 23, 2021, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211123a1.pdf.

[106] Department of Justice, "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team," press release, October 6, 2021, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

[107] Victoria L. Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework," *Future Technologies Conference (FTC) 2017*, 2017, https://www.researchgate.net/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework.

[108] "Enhanced Distributed Ledger Technology," NIST, https://csrc.nist.gov/Projects/enhanced-distributed-ledger-technology.

modification or deletion of specified records, which also removes the need for energy-intensive consensus mechanisms.

Additionally, if personal information is stored on a public blockchain, confidentiality for that data may be lost if the encryption algorithm is cracked.[109] For this reason, some organizations have argued personal information and biometric data should never be recorded on a blockchain.[110] Additionally, as more personal information is recorded and shared with a blockchain network's nodes and credential issuers, it may increase the possibility that it may be correlated with other data and on-chain activity to identify specific users and their behaviors.[111] Congress might consider whether existing privacy regulations are adequate to address potential concerns arising from the use of blockchain technologies and blockchain-enabled provenance applications.

Currently, the NSF America's Seed Fund, a congressionally mandated Small Business Innovation Research and Small Business Technology Transfer program, provides research and development funding to startups and small businesses in the United States.[112] The program has funded various distributed ledger companies.[113] Congress may consider options to address some of the potential risks associated with blockchain technologies. Congress could direct NIST to expand existing research on blockchain or direct the NSF to fund blockchain research as well as research that examines blockchain risks and failure modes and the social, ethical, legal, and environmental implications of blockchain technologies.

In P.L. 117-58, Congress extended Internal Revenue Service reporting requirements to cryptocurrency brokers, such as cryptocurrency exchanges.[114] Congress might consider a similar approach to extend regulation to cover blockchain platforms and network operators, depending on the particular application and intent of oversight. Alternatively, outside academics have proposed requiring all blockchain-based applications and associated smart contracts be required to register in a searchable database, which would create more transparency, but may face logistical obstacles.[115]

Standards Development

The International Organization for Standardization (ISO) has begun issuing some standards for blockchains.[116] Congress may consider similar approaches to develop standards for blockchain technologies or provide resources to agencies to be involved in similar international standard-setting bodies.

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the Department of Commerce. Among its key roles, NIST promotes coordination between the public and private sectors in the development of standards and in conformity assessment

[109] Loïc Lesavre, Priam Varin, and Peter Mell, *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*, NIST, pp. 35.

[110] William Crumpler, Marti Flacks, and Amith Mandavilli, *The Human Rights Risks and Opportunities in Blockchain*, CSIS, p. 57.

[111] See Section 5 for "Metadata Tracing" in Loïc Lesavre, Priam Varin, and Peter Mell, *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*, NIST, pp. 32.

[112] "Portfolio," National Science Foundation (NSF), https://seedfund.nsf.gov/portfolio/.

[113] "Distributed Ledger (DL)," NSF, https://seedfund.nsf.gov/topics/distributed-ledger/.

[114] CRS In Focus IF11910, *Cryptocurrency Transfers and Data Collection*, by Mark P. Keightley and Andrew P. Scott.

[115] Aaron Wright and Primavera De Filippi, *Blockchain and the Law: The Rule of Code*, April 2018.

[116] See ISO Technical Committee ISO/TC 307 or IEEE SA for information on developing blockchain standards.

activities, encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government-unique standards, and coordinating federal agency participation in the development of relevant standards.[117] Congress has previously directed NIST to advance collaborative frameworks, standards, and guidelines for artificial intelligence.[118] Executive orders have also required NIST to lead a public-private effort to develop a framework of cybersecurity standards and best practices for protecting critical infrastructure.[119] Congress might consider a similar approach for the development of frameworks and standards for blockchain technologies or particular blockchain applications.

Some scholars assert that a multi-stakeholder approach to standards development for blockchain technologies would be beneficial to address interoperability challenges, among others.[120] Many blockchain networks remain unable to communicate with each other directly. For example, thousands of blockchain-based cryptocurrencies exist in the financial sector, but SEC authorities have noted the potential lack of long-term viability for so many different private forms of money that are not interchangeable.[121] Standardization and interoperability could enable the movement of funds, NFTs, or other assets from one blockchain to another preferred blockchain. Consumers could have more choice in their ability to move tokens and other data to quicker, cheaper, and less-energy alternatives. For example, standards such as BIP-32 and ERC-20 facilitated the emergence of interoperable wallets for cryptocurrencies.[122]

Conclusion

Blockchain technologies are in a phase of rapid development and expanded application and adoption in a number of industries and economic sectors. New blockchain applications, such as smart contracts, non-fungible tokens, and decentralization autonomous organizations, may automate processes or replace intermediaries in a variety of fields. Public and private sector actors are using, or have proposed using, novel blockchain applications in fields such as supply chain management, identity management, and asset registration. These applications may prove beneficial, but may also be accompanied by privacy, security, and environmental risks. Congress may consider balancing support for the further technical development of blockchain technologies and accompanying standards with oversight, privacy and security risk mitigation measures, and further consideration of the social, ethical, legal, and environmental impacts of expanded blockchain use.

[117] CRS Report R46586, *Federal Law Enforcement Use of Facial Recognition Technology*, coordinated by Kristin Finklea.

[118] CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[119] For more information on Executive Order 13636 or the White House's legislative proposal to Congress, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[120] Ibid.

[121] Paul Kiernan, "SEC's Gensler Doesn't See Cryptocurrencies Lasting Long," *Wall Street Journal*, September 21, 2021, https://www.wsj.com/articles/secs-gensler-doesnt-see-cryptocurrencies-lasting-long-11632246355.

[122] Loïc Lesavre, Priam Varin, and Peter Mell, *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*, NIST, p. 39.

Appendix A. Selected Legislation and Hearings

This section provides a brief summary of legislative activities in the 115th, 116th, and117th Congresses, including descriptions of laws, selected bills, and hearings that focus on blockchain technologies.

Members of Congress have introduced legislation that could affect blockchain platforms. Some bills aim to provide regulatory clarity, while others bills and legislation focus on specific applications of blockchain, such as anti-money laundering enforcement or climate solutions.[123] During the 114th Congress, Members established a bipartisan blockchain caucus in the House of Representatives.[124]

Table A-1. Selected Blockchain Legislation Introduced in the 115th-117th Congresses

Legislation	Congress	Title	Section on Blockchain
H.R. 3612	117th Congress	Blockchain Promotion Act of 2021	Would direct the Secretary of Commerce to establish a working group to recommend to Congress a definition of blockchain technology and other purposes.
H.R. 3543	117th Congress	Blockchain Technology Coordination Act of 2021	Would establish a National Blockchain Technology Coordination Office within the Department of Commerce.
H.R. 5045	117th Congress	Blockchain Regulatory Certainty Act	Would exempt certain non-controlling blockchain developers and providers of blockchain services from licensing and registration.
H.R. 3639	117th Congress	Blockchain Innovation Act	Would require the Department of Commerce to consult with the Federal Trade Commission and other relevant agencies to study potential applications of blockchain technology (i.e., the technology that supports digital currencies such as Bitcoin), including the use of such technology to address fraud and other unfair or deceptive practices.

[123] P.L. 117-58 directs the Department of Energy to submit a Digital Climate Solutions report that assesses using technologies, like blockchain and artificial intelligence, as climate solutions. H.R. 3639 directs the Secretary of Commerce and Federal Trade Commission to study the benefits of blockchain for limiting fraud and unfair or deceptive practices.

[124] The Congressional Blockchain Caucus was founded during the 114th Congress, see https://congressionalblockchaincaucus-schweikert.house.gov/.

Legislation	Congress	Title	Section on Blockchain
H.R. 6607	116th Congress	Strategic National Stockpile Enhancement and Transparency Act	Would have required the Department of Health and Human Services (HHS) to establish, and award grants to states for the implementation of, the National Emergency Biodefense Network. The network would have consisted of state entities responsible for tracking and maintaining adequate supplies of drugs, medical devices, and other items necessary for the emergency health security of the United States. The network would have been developed and implemented using a private blockchain.
H.R. 6938	116th Congress	Advancing Blockchain Act	Would have required the Department of Commerce to study and report on the impact of blockchain technology on U.S. businesses conducting interstate commerce. Would have required Commerce to report to Congress the results of such study and any recommendations to promote the adoption of blockchain technology.
H.R. 2858	116th Congress	FORWARD Act of 2019	Would have required the National Institutes of Health to develop a publicly-accessible server using blockchain technology to securely facilitate the sharing of fungal disease clinical research data.
H.R. 7002	115th Congress	Blockchain Records and Transactions Act of 2018	Would have specified how provisions related to the preemption of federal laws regarding electronic signatures apply to electronic signatures created or stored by blockchain technology.

Source: CRS, using Congress.gov.

Various committees in both the House of Representatives and the Senate held hearings on blockchain issues during the 115th, 116th, and 117th Congresses, with some focused on specific blockchain applications, such as identity verification, supply chain management, and domestic agriculture supply chains.[125]

[125] U.S. Congress, House Committee on Agriculture, *21st Century Food Systems: Controlled Environment Agriculture's Role in Protecting Domestic Food Supply Chains and Infrastructure*, 117th Cong., 1st sess., July 29, 2021. U.S. Congress, House Committee on Financial Services, Task Force on Artificial Intelligence, *I Am Who I Say I Am: Verifying Identity while Preserving Privacy in the Digital Age*, 117th Cong., 1st sess., July 16, 2021. U.S. Congress, House Committee on Science, Space, and Technology, Subcommittee on Oversight and Subcommittee on Research and Technology, *Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods*, 115th Cong., 2nd sess., May 8, 2018.

Appendix B. Glossary

Term	Definition
Application-Specific Integrated Circuit (ASIC):	Technology designed to accomplish a specific computational purpose. For blockchain, ASICs are used to mine cryptocurrency in a Proof of Work consensus mechanism (ex. Bitcoin, Ethereum).
Blockchain:	A distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is linked to the previous block after validation. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across copies of the ledger within the network.
Consensus Mechanism:	A process to achieve agreement within a distributed system on the current state of the blockchain. Also called a consensus method or consensus algorithm.
Decentralized Autonomous Organization (DAO):	Groups whose rules are encoded and transactions are executed using smart contracts, eliminating intermediaries. DAOs require member voting to make organizational changes.
Decentralized Finance (DeFi):	Generally refers to the use of digital assets and blockchain technology to replicate and replace conventional delivery of financial services—such as loans, asset trading, insurance, and other services—through central financial intermediaries such as brokerages, exchanges, or banks.
Distributed Ledger:	A database shared across many nodes that is constantly shared, replicated, and synchronized.
Distributed Ledger Technology:	Blockchains are part of a larger family of distributed ledger technologies (DLTs), which refers to technologies based on distributed ledgers where the storage of data is not based on chains of blocks. In addition to blockchain, Directed Acyclic Graphs (DAGs) are another example of a DLT.
Fork:	A change to blockchain network's software. The changes may be backwards compatible (soft fork), or the changes may not be backwards compatible (hard fork).
Hash:	Digital equivalent of a fingerprint; unique and useful for detecting change in a file. A function that takes an input string, which can be of any length, and generates an output of fixed length. The output, or hash, is used to authenticate information. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.
Hashrate:	The number of calculations (or hash functions) performed on the network per second. Devices have different hashrates and therefore different power requirements. The network hashrate refers to the total computing power of the blockchain network.
Miners:	Participants who validate and add a block to the blockchain in exchange for a reward such as cryptocurrency or a transaction fee.
Mining Pool:	A group of miners who pool their computational resources via a shared server to mine cryptocurrency and validate transactions more efficiently. A pool operator distributes rewards between miners in the mining pool.
Non-Fungible Tokens (NFTs):	Unique and non-interchangeable units of data (tokens), which can be used to represent the sole ownership of any unique item. NFTs are commonly used to verify the authenticity of a digital item and record its ownership history.
Node:	Individual participant or computer system on the blockchain network. Some nodes can only view the blockchain ledger, while others can read and edit the ledger.
Private Key:	The secret complement to a public key used to conduct encrypted transactions.

Proof of Authority (PoA): A participant is chosen to validate the next block based on their reputation. PoA uses identity and reputation to prevent bad actors.

Proof of Stake (PoS): A participant is chosen to validate the next block based on the individual's proportion of staked coins or ownership of the blockchain network.

Proof of Work (PoW): Under PoW, miners—those seeking to add a block to a blockchain—are presented a difficult computational problem. Once the problem is solved, other users validate the solution and confirm the block, adding the next block to the chain.

Public Key: Publicly viewable complement to the private key. Sometimes tied to a public address on a ledger. The public address is a short, alphanumeric string derived from a user's public key using a hash function, with additional data to detect errors. Addresses are used to send and receive digital assets.

Smart Contract: Self-executing code that executes a contract with commands on a blockchain.

Author Information

Kristen E. Busch
Analyst in Science and Technology Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.