GAO

United States Government Accountability Office

Report to Congressional Requesters

March 2022

TECHNOLOGY ASSESSMENT

Blockchain

Emerging Technology Offers Benefits for Some Applications but Faces Challenges

GAO-22-104625

The cover image displays graphical examples of different use cases of blockchain technology, including for government, IDs, finance, supply chains, and medicine, connected by a series of chained blocks.

Cover source: GAO. | GAO-22-104625

TECHNOLOGY ASSESSMENT

Blockchain

Emerging Technology Offers Benefits for Some Applications but Faces Challenges

Highlights of GAO-22-104625, a report to congressional requesters

March 2022

Why GAO did this study

Economies rely on central authorities and trusted intermediaries to facilitate business transactions. Blockchain is a technology that could reduce the need for such entities while establishing a system of verification. It might therefore improve a variety of financial and non-financial applications. However, the use of blockchain technologies raises a variety of ethical, legal, economic, and social concerns.

GAO was asked to conduct a technology assessment on the use of blockchain, with an emphasis on foresight and policy implications. This report discusses (1) non-financial applications of blockchain, including potential benefits and challenges, (2) financial applications of blockchain, including potential benefits and challenges, and (3) policy options that could help enhance benefits or mitigate challenges of blockchain technologies.

GAO assessed blockchain applications developed for or used in finance, government, supply chain management, and organization management; interviewed a range of stakeholder groups including government, industry, academia, and a venture capital firm; convened a meeting of experts in collaboration with the National Academies of Sciences, Engineering, and Medicine; and reviewed key reports and scientific literature. GAO is identifying policy options in this report.

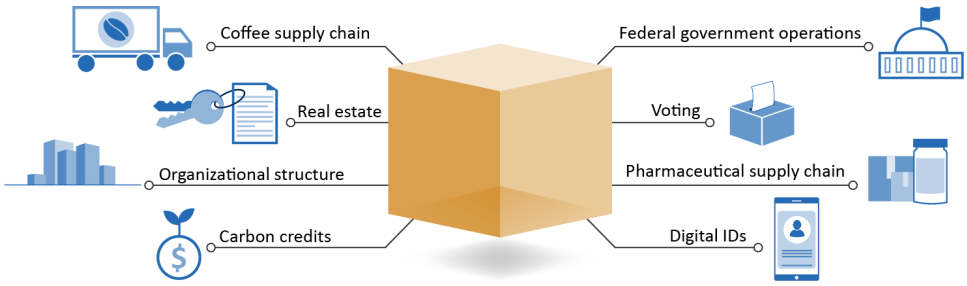
View GAO-22-104625. For more information, contact Karen L. Howard at (202) 512-6888, howardk@gao.gov.

What GAO found

Blockchain combines several technologies to provide a trusted, tamper-resistant record of transactions by multiple parties without a central authority such as a bank. Blockchain can be used for a variety of financial and non-financial applications, including cryptocurrency, supply chain management, and legal records. GAO found that blockchain is useful for some applications but limited or even problematic for others. For example, because of its tamper resistance, it may be useful for applications involving many participants who do not necessarily trust each other. But it may be overly complex for a few trusted users, where traditional spreadsheets and databases may be more helpful. Blockchain may also present security and privacy challenges and can be energy-intensive.

Blockchain has a wide range of potential non-financial uses (see figure).

Blockchain has many potential non-financial applications



Source: GAO. | GAO-22-104625

For example, it could be used to organize supply chains, create less hierarchical organizations, and document title registries for real estate. However, most such efforts are not yet beyond the pilot stage and face challenges. For example, most blockchain networks are not designed to be interoperable and cannot communicate with other blockchains. Organizations that want to use blockchain also face legal and regulatory uncertainties, and have found it difficult to find skilled workers to implement blockchain.

Financial applications of blockchain have the potential to reduce costs and improve access to the financial system, but they also face multiple challenges. Cryptocurrencies, likely the most widely known application, are a digital representation of value protected through cryptographic mechanisms, which facilitates payments. Some are known for volatility (i.e., frequent or rapid changes in value), but a type known as stablecoins may help reduce this risk. Similarly, an emerging area known as decentralized finance offers services such as blockchain-based lending and borrowing, which also face several challenges. For example, blockchain-based financial applications can facilitate illicit activity, may reduce consumer and investor protections compared to traditional finance, and, in some cases, are subject to unclear and complex rules.

GAO developed four policy options that could help enhance benefits or mitigate challenges of blockchain technologies. The policy options identify possible actions by policymakers, which may include Congress, federal agencies, state and local governments, academic and research institutions, and industry. In addition, policymakers could choose to maintain the status quo, whereby they would not take additional action beyond any current efforts. See below for details of the policy options and relevant opportunities and considerations.

Policy Options That Could Help Enhance Benefits or Mitigate Challenges of Blockchain Technologies

	Opportunities	Considerations
Standards (report p. 38) Policymakers could collaborate to unify standards that focus on the development, implementation, and use of blockchain technologies.	• Could simplify fragmented standards and help identify gaps and reduce overlap in standard-setting efforts. • Could identify the areas in which standards would be most beneficial across different sectors of the economy or applications of blockchain. • Could help address challenges around interoperability and data security.	• Could require consensus from many public- and private-sector stakeholders, which can be time- and resource-intensive. • May not be clear which entities should take the lead in establishing internationally recognized standards for different technologies and application areas. • May require new funding or reallocation of existing resources to support new efforts.
Oversight (report p. 39) Policymakers could clarify existing oversight mechanisms, including regulations, or create new mechanisms to ensure appropriate oversight of blockchain applications.	• Clear, industry-specific U.S. oversight frameworks could offer the clarity needed for individuals and firms to more successfully engage in blockchain-related commerce in the U.S. • Policymakers, including regulatory entities and developers, could use tools to create oversight mechanisms in addition to testing innovative products and services. • Could provide coordinated and timely clarity to promote safety and soundness, consumer protection, and compliance with applicable laws and regulations to combat illicit activity in blockchain-related commerce.	• Policymakers will need to determine the appropriate level of oversight. Aggressive oversight could hamper innovation and competition as the technology matures, whereas too little oversight could leave consumers and businesses unprotected. • Soliciting input across a range of stakeholders in various sectors may be time consuming and challenging. • May require new funding or reallocation of existing resources.
Educational materials (report p. 40) Policymakers could support the development of educational materials to help users and regulators better understand blockchain technologies beyond existing financial applications.	• Could enable instructors to train a workforce skilled in developing, implementing, and using blockchain-based products. • Could increase consumer literacy and help reduce negative public perceptions of blockchain. • Could stimulate critical thinking and innovation, as well as prompt innovative research and development. • Could help prepare policymakers to better use and regulate the latest technologies.	• Educational materials will likely need to be tailored to meet a wide variety of learning needs across multiple target audiences. • May be difficult to identify who could most effectively create educational materials for any particular target audience. • May require new funding or reallocation of existing resources, especially to address the need for education regarding innovative uses of blockchain beyond existing financial applications.
Appropriate uses (report p. 41) Policymakers could support activities designed to determine whether blockchain is appropriate for achieving specific missions and goals or to mitigate specific challenges.	• Actively investigating where and when blockchain would be the most useful could allow entities to capture the full benefits the technology might offer. • Supporting blockchain use, where appropriate, could enhance transparency and accountability of existing systems and services.	• Legal or regulatory uncertainty may hinder some potential users from benefitting from blockchain. • Could be difficult to revert to a non-blockchain technology once an entity has invested a significant amount of time and resources. • May require new funding or reallocation of existing resources.

Source: GAO. | GAO-22-104625

Table of Contents

Abbreviations

BFS	Bureau of the Fiscal Service
CBP	U.S. Customs and Border Protection
CFTC	Commodity Futures Trading Commission
DAO	decentralized autonomous organization
DeFi	decentralized finance
DHS	Department of Homeland Security
EU	European Union
FinCEN	Financial Crimes Enforcement Network
ICO	initial coin offering
IEEE	Institute of Electrical and Electronics Engineers
NASEM	National Academies of Sciences, Engineering, and Medicine
SEC	Securities and Exchange Commission

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 23, 2022

The Honorable Rodney Davis
Ranking Member
Committee on Administration
House of Representatives

The Honorable William Foster
Chairman
Subcommittee on Investigations and Oversight
Committee on Science, Space, and Technology
House of Representatives

Economies rely on central authorities and trusted intermediaries to facilitate business transactions. Perhaps the most familiar example is money: a medium backed by a central authority that can be exchanged for goods and services. In an average day in the United States, at least $245 billion changes hands.[1] Another example is an escrow account, in which a trusted intermediary holds onto an asset from one party, such as a homebuyer, and transfers it to another party that meets certain conditions, such as a seller who transfers title of a home.

Blockchain is a technology that could facilitate these and many other types of transactions without the need for a central authority. Cryptocurrency is one of the first and most well-known applications. Blockchain is the enabling technological infrastructure behind cryptocurrencies, but blockchain and cryptocurrencies are not the same. Blockchain has many other potential applications, both financial and nonfinancial. For example, it could be used to facilitate lower-cost loans, track items in a supply chain, document title registries for real estate, and create organizations without traditional hierarchies.

Blockchain helps accomplish these tasks by creating a virtual, consensus-driven, tamper-resistant ledger for recording transactions. The ledger is distributed rather than centralized, meaning all parties to the transaction can retain a copy and add data. Blockchain technology uses an agreed-upon protocol to add each transaction to a block, connects all the blocks in a chain, and distributes the results to all parties. The resulting record is secure (or "immutable") because the mathematical relationships among the blocks prevent the record from being changed without that change being obvious. There are two types of blockchain technology implementations: "permissionless" where anyone can add information and "permissioned" where only certain users are allowed to do so. Cryptocurrencies generally use permissionless blockchains whereas many other applications use permissioned blockchains.

However, blockchain and its applications have some drawbacks and challenges. For example,

[1]This money flows through a system known as the Automated Clearing House, or ACH Network, and is used for direct deposit of salaries and tax refunds, payments between business, and other transactions.

although privacy concerns apply to many technologies, some blockchain characteristics may make such concerns more severe. In addition, blockchain has no mechanism for detecting or preventing the entry of inaccurate data by an authorized user. Furthermore, even though there are many promising uses for permissioned blockchain technology, few we examined outside of permissionless financial applications have progressed beyond the proof-of-concept or pilot phases. Some applications of blockchain also raise ethical, legal, and other concerns. For example, because of cryptocurrencies' pseudoanonymity, some money-laundering organizations use it to transfer proceeds from illegal activities across borders.

You asked us to conduct a technology assessment in this area, with an emphasis on foresight and policy implications. This report discusses (1) non-financial applications of blockchain, including their potential benefits and challenges, (2) financial applications of blockchain, including their potential benefits and challenges, and (3) policy options that could help enhance benefits or mitigate challenges of blockchain technologies.[2] We focused our review on a wide range of blockchain applications. However, we did not include some applications, such as non-fungible tokens (NFTs). See appendix I for a full discussion of the objectives, scope, and methodology used in this report.

We conducted our work from November 2020 through March 2022 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

[2]In addition to this technology assessment, GAO's Innovation Lab is experimenting with possible uses for blockchain within the federal government, including use of blockchain to support GAO operations.

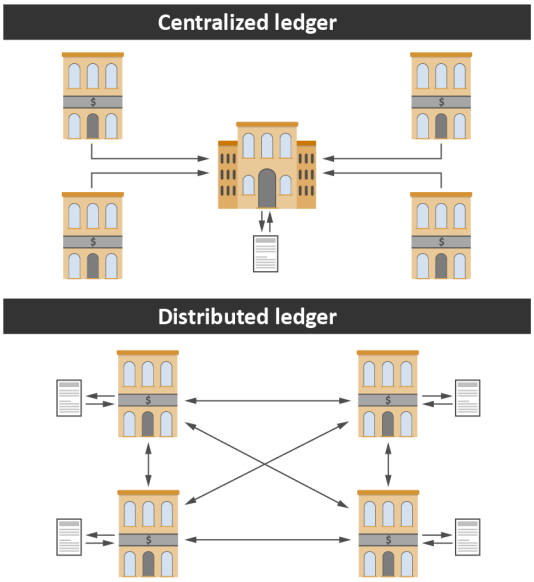
1 Fundamentals of Blockchain

1.1 What is blockchain?

Blockchain is not a new technology but rather an innovative way of using existing, mature technologies. Its core function is to create a tamper-resistant ledger for digital assets, such as cryptocurrency. The ledger is tamper-resistant because blockchain technology duplicates the data on ownership and transfer of these assets across many computers and users. This distribution reduces the likelihood that a single failure or dishonest user could compromise network integrity or tamper with the ledger.

Blockchain ledgers do not require a central authority, unlike centralized databases or other ledgers (see fig. 1). This decentralization is possible because blockchain (1) uses cryptographic techniques to computationally verify transactions and (2) builds an immutable ledger by cryptographically "chaining" a grouping of newly added data—known as a block—to past blocks (see below). This process prevents changes unless they are verified by other users.

Figure 1: Difference between centralized and distributed ledgers

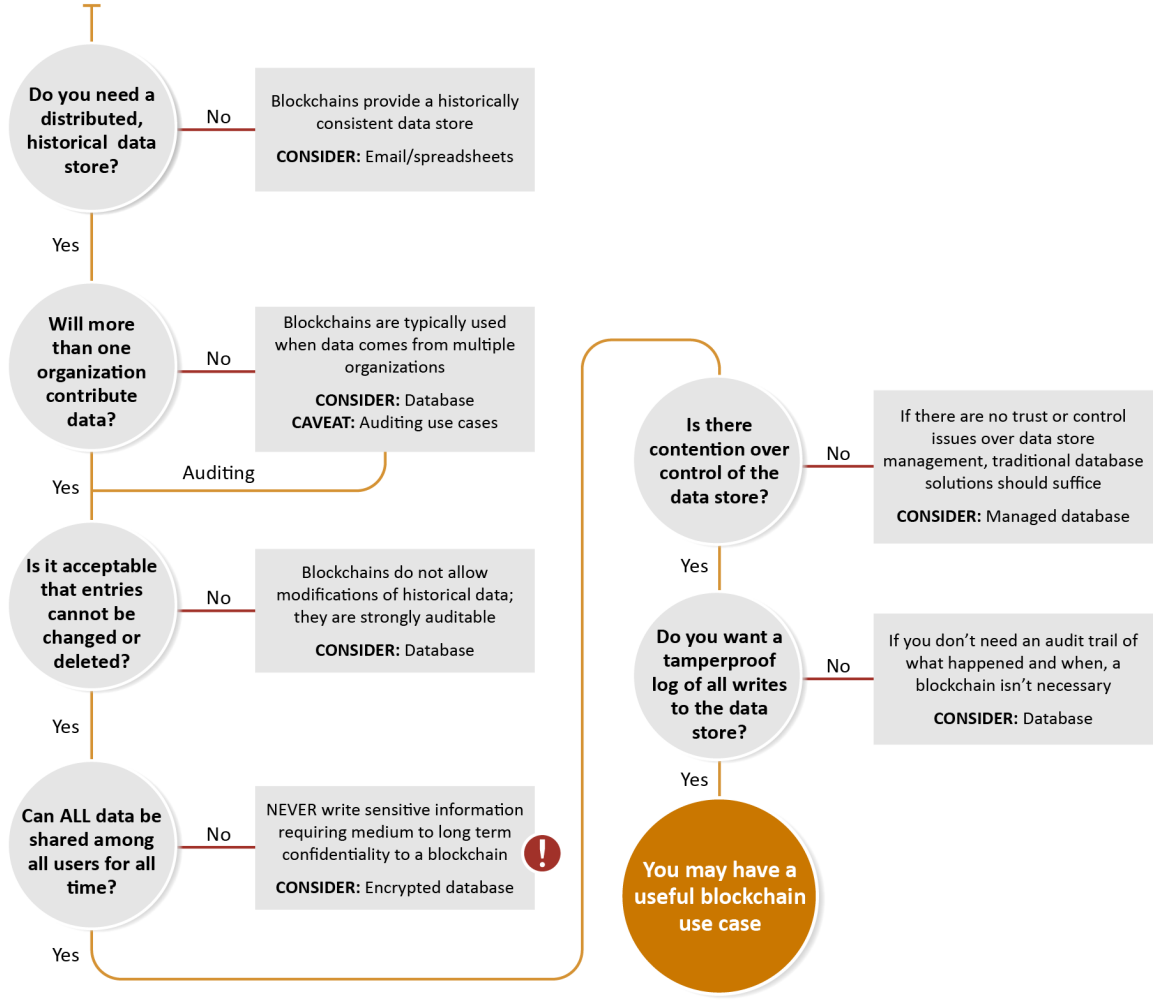


Source: GAO. | GAO-22-104625

1.2 How to determine whether a blockchain would be most useful

Blockchain is useful for some applications but limited or even problematic for others. For example, it may be useful for applications involving many distributed participants or transactional workflow such as management of a supply chain, or applications involving digital assets. But it may be overly complex if users are relatively few and they all trust each other, in which case techniques such as spreadsheets and databases may be more helpful. See chapter 3 for further discussion of potential blockchain use cases in specific sectors. Figure 2 illustrates in more detail some of the situations in which blockchain or its alternatives may be useful.

Figure 2: Flowchart for determining whether blockchain may be useful



Source: Department of Homeland Security Science & Technology Directorate. | GAO-22-104625

The following are additional important considerations in weighing the benefits and challenges of blockchain for a given application:

Privacy. Storing sensitive data on public blockchains may lead to privacy concerns because of blockchain's distributed nature. Specifically, numerous users store data separately due to the distributed nature of blockchain, giving multiple people access to the encrypted data. If it becomes feasible to decrypt the sensitive data, then unauthorized people could have access to sensitive data.

While privacy concerns apply to many technologies, the immutability and distributed nature of information on a blockchain may make such concerns more severe. According to one peer-reviewed study, if an individual's public blockchain address is matched to their true identity, all transactions associated with that address can

then be linked to an individual.[3] Although there are efforts underway to solve privacy concerns, one study found only a small number of the blockchain systems surveyed attempted to address these privacy issues.[4]

Data reliability. In some cases, external sources, such as freight shippers in a product supply chain, can add data to the blockchain. These sources are known as "oracles," and can be people or devices.[5] Similar to other data management systems, blockchains have no inherent mechanism to check the accuracy of oracle data, which creates the risk that information will be entered incorrectly onto a blockchain, whether intentionally or unintentionally. Incorrect data can compromise the integrity of a blockchain, leading to a variety of problems, sometimes including financial losses and incorrect tracking of information. Furthermore, parties involved in an automatic transaction triggered by a "smart contract" (see below) may have limited recourse, because the enforceability of such smart contracts varies among U.S. jurisdictions. Some efforts are underway to improve the reliability of data entered onto blockchains in certain circumstances.

Long-term data security and quantum computing. Advances in quantum computing may generate longer-term risks to the security of encrypted data, including such data stored on blockchains.[6] Specifically, some of the public key encryption algorithms that most blockchains (and many other technologies) use to guarantee the integrity and confidentiality of stored data could in the future be broken by quantum computers.[7] Federal agencies and academic researchers are involved in research and development of post-quantum cryptography systems that will be secure against decryption attempts using either quantum or classical computers. Further, the National Institute of Standards and Technology is developing standards to support deployment of new post-quantum cryptography infrastructure.

Energy consumption. Although data on energy use across industries are limited, there is some evidence from the research literature that blockchains use more energy than traditional centralized databases because a blockchain must store multiple copies across multiple computers. Further, while the specific energy usage is unknown, certain blockchains (in technical terms, those using a proof-of-work consensus protocol) generally require more energy than other blockchains. A 2019 study estimated that Bitcoin's annual carbon emissions range from 22.0 million to 22.9 million metric tons of carbon dioxide, about as much as the nations of Jordan and Sri Lanka combined.[8] A 2021 report estimated that Bitcoin networks consume around half

[3]William J. Gordon and Christian Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Computational and Structural Biotechnology Journal,* June 30, 2018, Vol. 16, p. 224-230.

[4]Taylor Hardin and David Kotz, "Blockchain in Health Data Systems: a Survey," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019.

[5]Oracles are people, devices, or software that add information to a blockchain. Oracle does not refer to the Oracle Corporation.

[6]Quantum computing uses the principles of quantum physics, the properties of nature at atomic scales, to accomplish some tasks that are not achievable with existing technologies. The development of an advanced quantum computer may be more than a decade away.

[7]For more details on quantum computers and the risks to current encryption technologies, see GAO, *Quantum Computing and Communications: Status and Prospects,* GAO-22-104422 (Washington, D.C.: Oct. 19, 2021).

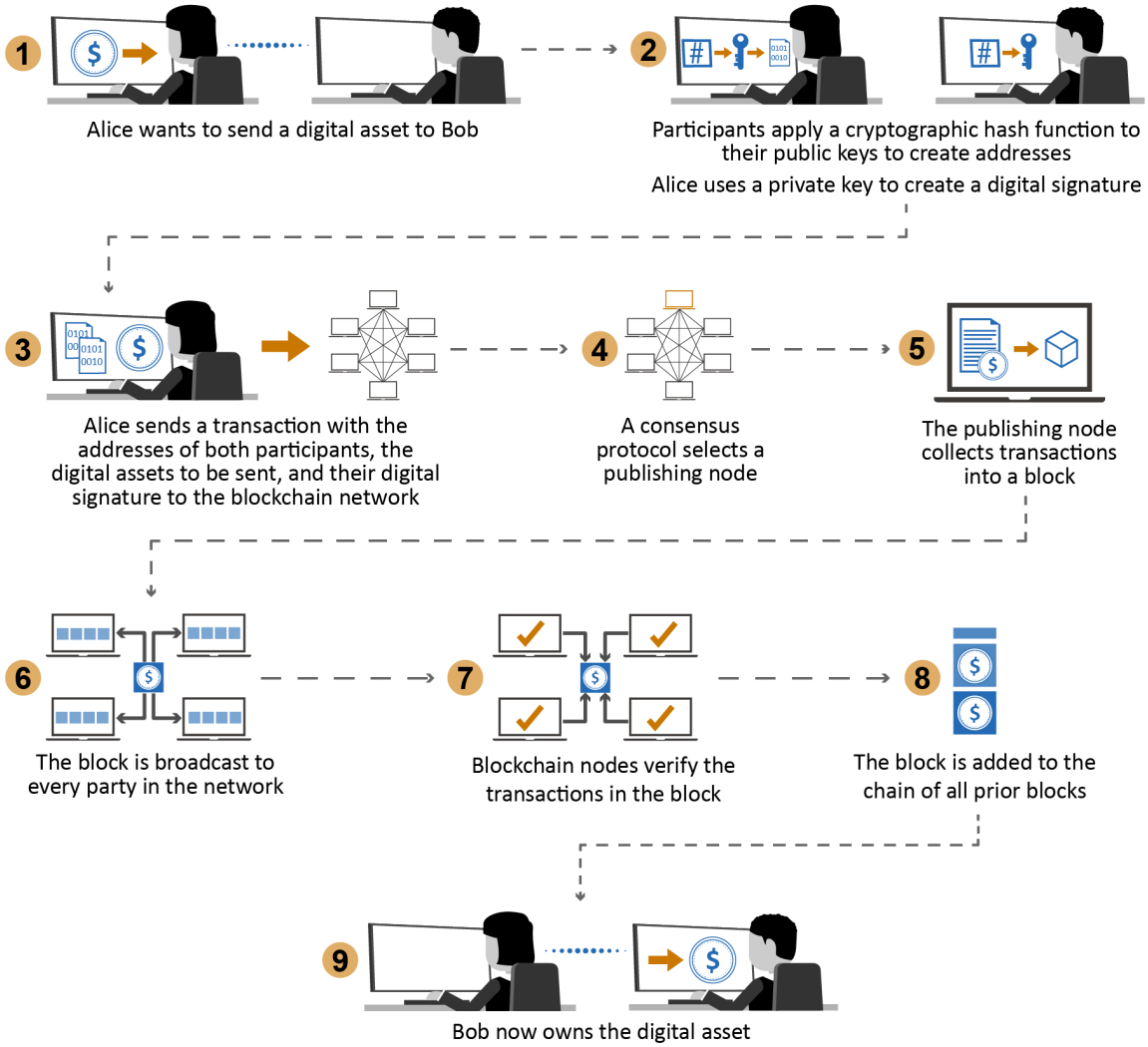
[8]Christian Stoll, Lena Klaaßen, and Ulrich Gallersdorfer "The Carbon Footprint of Bitcoin," Joule, Volume 3, Issue 7, pp. 1647-1661, July 17, 2019. Total greenhouse gas emissions in the U.S. were estimated at 6.6 billion metric tons of carbon dioxide equivalents in 2019.

the energy of the banking or gold industries.[9] Given the growth of Bitcoin (see chapter 3), emissions are likely higher as of 2022.

1.3 Blockchain operation

A blockchain functions through a series of computational steps (see fig. 3).

Figure 3: Simplified example of blockchain operation to send digital assets



Source: GAO and GAO analysis of report by the National Institute of Standards and Technology. | GAO-22-104625

[9]According to the following report, due to limitations in publicly available data from the banking, gold, and cryptocurrency industries, it is challenging to accurately compare energy usage across sectors. Rachel Rybarczyk, Drew Armstrong and Amanda Fabiano, *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question* (Galaxy Digital Mining, 2021).

Transactions are added to a blockchain's ledger in the form of blocks. First, a transaction is sent to the blockchain network. The members of the network (known as nodes) then validate and queue the transaction with other valid transactions. For example, one node (known as the publishing node) will group valid transactions onto a block and broadcast the block to the network. Other nodes will check the validity and authenticity of transactions and will only add the block if its values are valid.

When a new block is added to the blockchain, it includes a number known as the hash digest, which the blockchain mathematically derives from the data in the previous block. This has the effect of cryptographically "chaining" the blocks together. If a previous block is modified, it will change all subsequent blocks, making it easy to detect altered blocks. When this happens users can readily see that a change in the blockchain occurred by comparing the new blockchain to the blockchain stored on their node, making a blockchain ledger tamper-resistant.

Users can employ third-party software and services, sometimes described as blockchain-as-a-service, to handle the many complexities of blockchain, which can make it more accessible. For example, these services can maintain copies of the ledger as well as manage private and public keys, transactions, and account security. However, using such a service provider creates a source of centralization because a single provider may have control over many accounts.

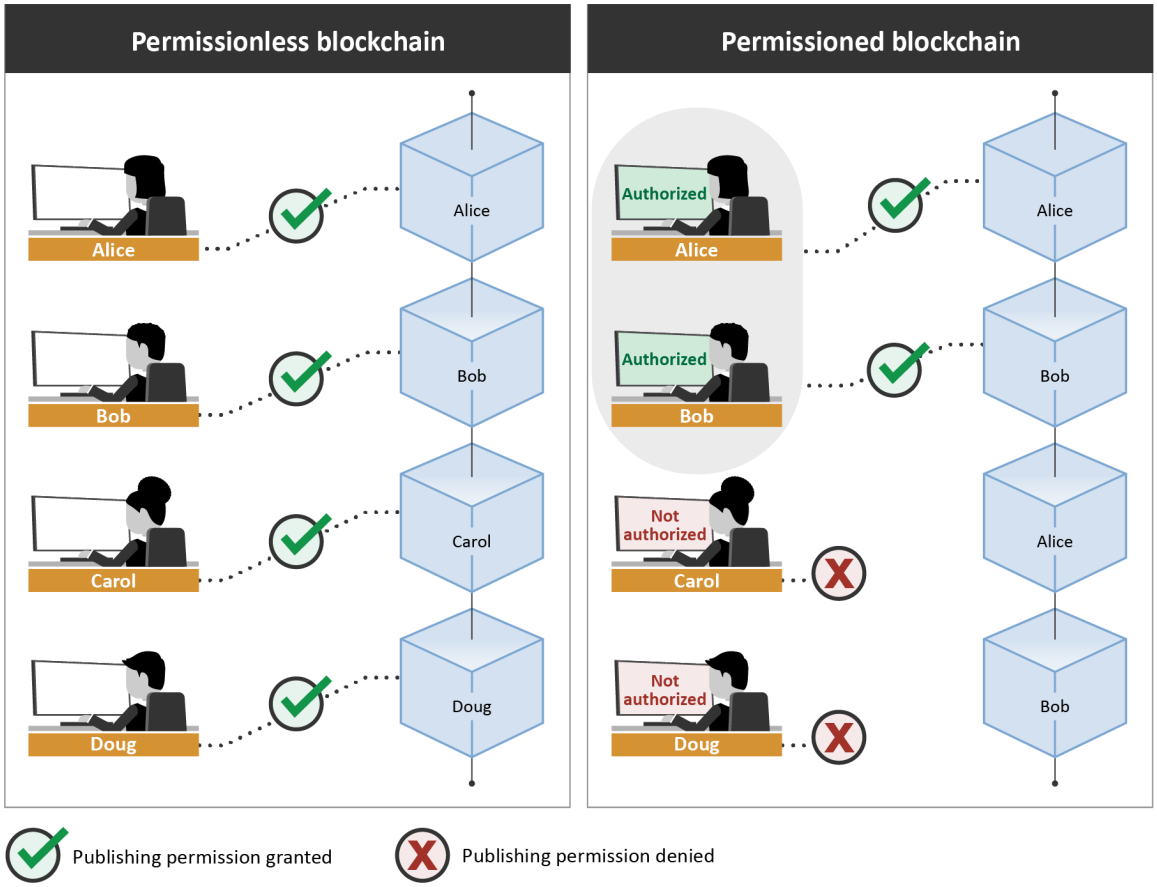
1.4 Types of blockchains

The two main categories of blockchains are *permissionless* and *permissioned* blockchains (see fig. 4). The permission setting for who can access, read, and write to a blockchain is a critical characteristic.

Permissionless blockchains are open to everyone to contribute data. Cryptocurrencies often use permissionless blockchains. Anyone has the right to publish blocks on a permissionless blockchain, so anyone can read and issue transactions on the blockchain. Because permissionless blockchain networks are open, malicious users may attempt to publish blocks in a way that subverts the system. To help prevent this, such networks often use a consensus protocol (see below) that requires users to expend or maintain resources when attempting to publish blocks. This requirement usually promotes non-malicious behavior by rewarding the successful publishers of blocks with the blockchain's cryptocurrency.

Permissioned blockchains are privately operated and only specified entities (i.e., authorized users) are allowed to access the network and make transactions. Permissioned blockchains may be beneficial when they store proprietary or sensitive information, such as blockchains for supply chains or health care (see vignettes in chapter 2 for specific examples of blockchain).

Figure 4: Comparing a permissionless blockchain to a permissioned blockchain



Source: GAO. | GAO-22-104625

1.5 Smart contracts

Smart contracts are a tool to extend the functionality of a blockchain beyond recording transactions, although not all blockchains support them. Smart contracts are not contracts in the traditional legal sense of the term; rather, they are used to automatically transfer digital assets on the blockchain if certain conditions are met.[10] These can include conditions such as addressing payment terms, liens, confidentiality, and enforcement. Smart contracts can provide services such as recording data from a sensor to the blockchain. Smart contracts consist of code and data that can automatically run on the blockchain using cryptographically signed transactions. Multiple nodes execute the code, and if all nodes derive the same answer, a node records the result to the blockchain. Smart contracts can collect input data from external sensors and external users, among

[10]U.S. jurisdictions vary on the recognition of smart contracts as legally binding contracts and the enforcement of smart contract terms.

other sources, and make decisions based on that information.

1.6 Consensus protocols

Consensus protocols are the steps a blockchain takes to ensure verified blocks are added to the blockchain and unverified blocks are ignored. Choosing the correct consensus protocol is critical because it controls who can publish information to the blockchain, affects the energy consumption, and can dictate the time it takes to publish a block. There are several types of protocols with different features; the choice of protocol depends on whether it is for a permissionless or permissioned blockchain and the level of trust between participants.[11] See appendix IV for more information on consensus protocols.

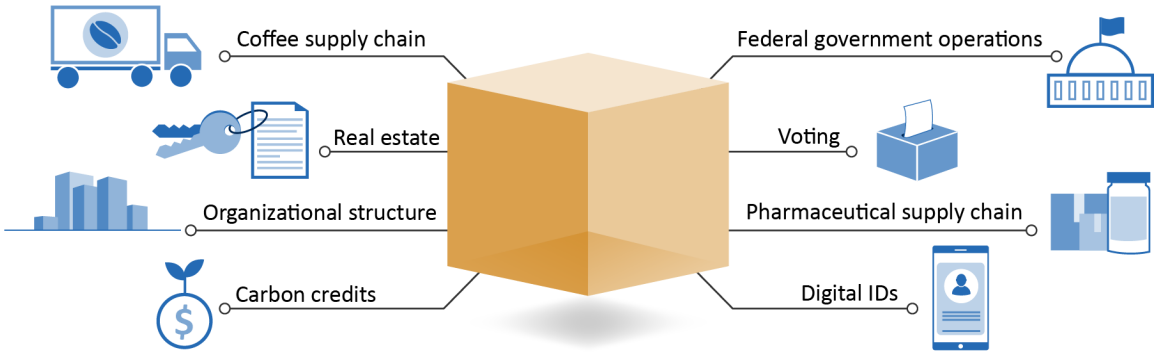
[11]For a more detailed description of consensus protocols see D. Yaga, P. Mell, N. Roby, and K. Scarfone. *Blockchain Technology Overview*. National Institute of Standards and Technology Internal Report 8202. (Gaithersburg, Md.: National Institute of Standards and Technology, Oct. 2018).

2 Blockchain Could Enable a Variety of Non-Financial Applications, but These Applications Face Challenges

Blockchain has many potential non-financial applications, which we highlight across a series of eight vignettes in this chapter (see fig. 5). For example, some businesses have explored using it to ensure the reliability of supply chains with numerous suppliers who do not necessarily trust one another. Existing instruments, such as escrow accounts, can already address that need; they allow a trusted third party to hold a payment and then convey it upon delivery of a good or service. But blockchain might reduce costs by replacing the escrow holder with a computationally enforced set of rules that enable trustless data sharing. In addition, companies are developing blockchain applications tailored to industries such as pharmaceuticals and food, to help combat counterfeit medicines, trace food-borne illnesses, and track food provenance. Potential public sector applications include maintaining property records, such as title transfer, or improving information sharing in federal agencies.

Blockchain developers have partnered with organizations to pilot these new applications. However, for most of the use cases we selected for review, blockchain did not resolve a majority of the critical challenges associated with each use case. Furthermore, blockchain can introduce new challenges such as exclusion of those people who do not have internet or computer access. Additionally, few of these blockchain systems have progressed beyond the pilot stage.

Figure 5: Examples of potential blockchain technology use cases



Source: GAO. | GAO-22-104625

Source: Yaruniv-Studio/stock.adobe.com. | GAO-22-104625

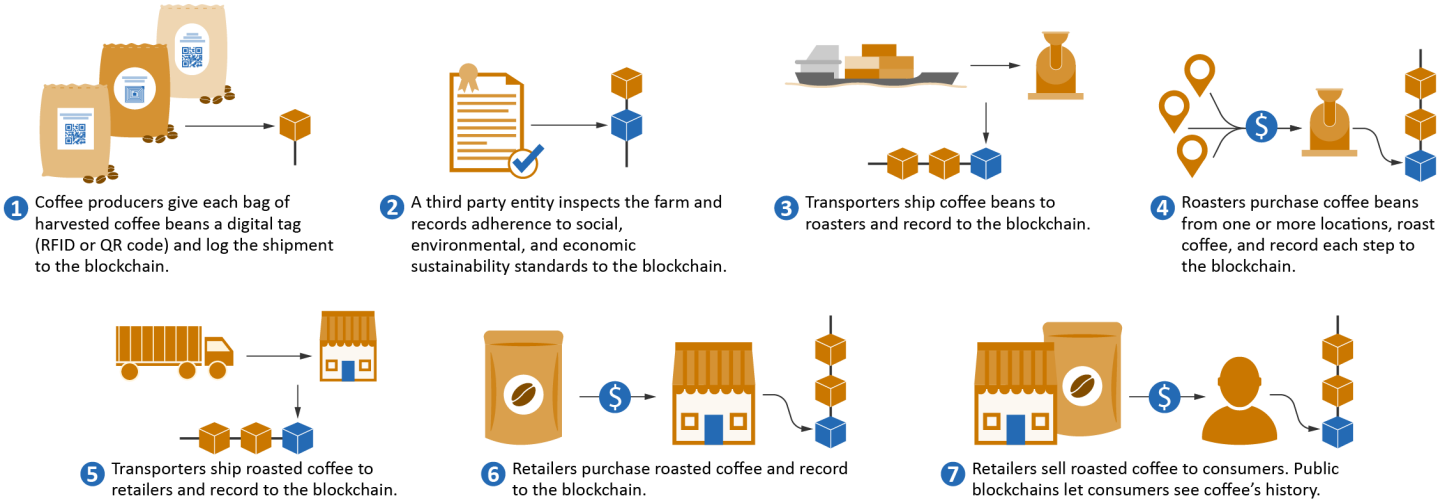
Vignette Coffee Supply Chain

Coffee beans change hands many times between a farmworker picking a coffee cherry off a coffee plant and a consumer purchasing an espresso, creating a complex international supply chain. The coffee supply chain faces challenges, including child and forced labor, poverty-level wages, and environmentally damaging farming practices. Consumers and organizations seek solutions to these problems; blockchain may help provide solutions.

Why blockchain?

By using blockchain to make transactions electronic and create an immutable record, blockchain may help increase the transparency of the coffee supply chain. However, it is unclear whether blockchain will address other critical issues as described above.

Simplified example blockchain for coffee bean supply chains



Note: This graphic represents a simplified supply chain.

Source: GAO analysis of literature. | GAO-22-104625

Potential challenges and limitations of a blockchain-based system

- **Labor conditions.** Reducing child and forced labor would require reliable monitoring by third-party industry inspectors, which some countries lack and would be conducted off the blockchain.
- **Data reliability.** A blockchain does not prevent users from entering faulty data. For example, the blockchain would not be able to identify whether incorrect data, which could affect actions of other supply chain participants, had been added to its ledger.
- **Digital exclusion.** As with other non-blockchain solutions, a lack of internet access may prevent participation. Internet access in the top 10 coffee-exporting countries has been reported to range from 19 to 70 percent of the population.

Examples of possible coffee supply chain challenges

Possible coffee supply chain challenge	Child and forced labor	Fair wages	Environmental impacts	Product traceability
Does blockchain help address challenge?	Unclear	Unclear	Unclear	Likely

Source: GAO analysis of literature. | GAO-22-104625

Source: James Thew/stock.adobe.com. | GAO-22-104625

Vignette: Pharmaceutical Supply Chain

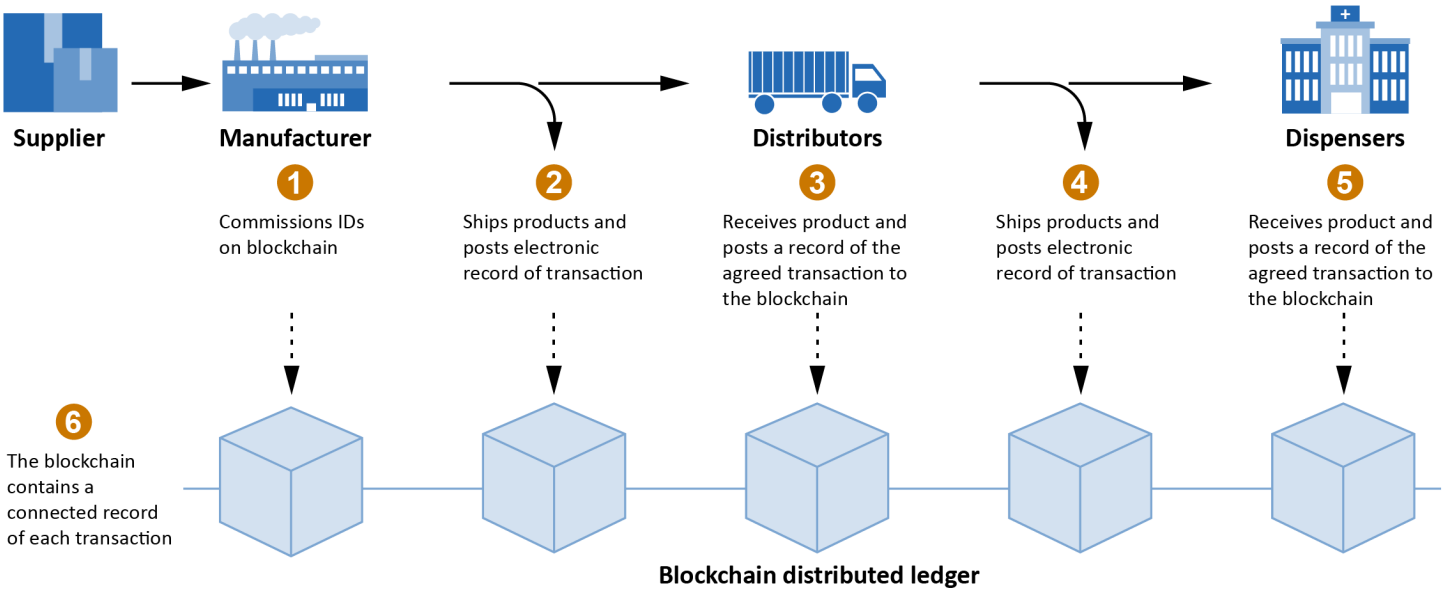
Counterfeit medicines in the pharmaceutical supply chain have threatened public health and patient safety for decades, and the globalization of the pharmaceutical supply chain has exacerbated the problem. Further, counterfeit medicines cost the pharmaceutical industry almost $40 billion annually. Addressing the growing prevalence of counterfeit medicines is a key challenge of the pharmaceutical supply chain.

Why blockchain?

Blockchain can provide transparency and traceability at every stage of the pharmaceutical supply chain with an immutable audit trail of transactions. With this audit trail, authorized stakeholders could verify the authenticity of the pharmaceuticals at any point in the supply chain by tracing the pharmaceutical to its origin.

The pharmaceutical supply chain is a complex network of multiple independent entities including manufacturers, pharmacies, and hospitals. This complexity makes it difficult to track products. Counterfeiters can take advantage of this to put their products on the market while providing little to no verifiable documentation.

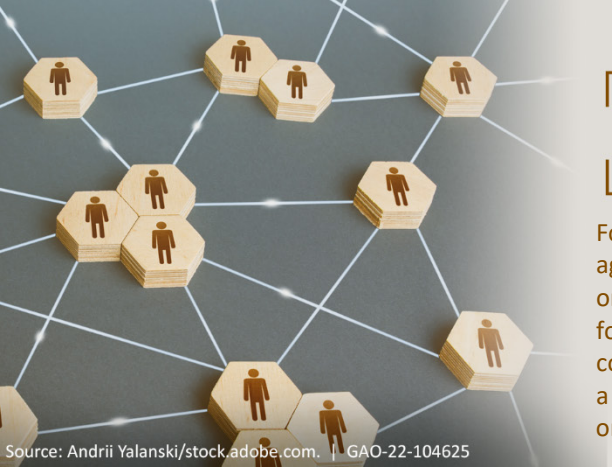
Potential Example of a Blockchain-based Pharmaceutical Supply Chain Ledger



Source: AmerisourceBergen and GAO review of literature. | GAO-22-104625

Potential challenges and limitations of a blockchain-based system

- **Interoperability.** Current pharmaceutical supply chains are complex structures. As with other non-blockchain solutions, any potential blockchain system will need to be interoperable with a vast, complex array of existing systems. However, today's available blockchain solutions are not interoperable despite their attempts to support the same industry and work with the same technology. This could mean that different firms that choose to use different blockchain solutions may not be able to conduct blockchain-enabled business with one another.
- **Regulatory Compliance.** As with other non-blockchain solutions, any blockchain system tracking the pharmaceutical supply chain must be capable of operating in multiple legal frameworks to function. As discussed above, pharmaceutical supply chains are global in nature, and these supply chains are also undergoing a period of increased oversight. More than 40 countries, such as the U.S. (Drug Supply Chain Security Act) and the European Union (Falsified Medicines Directive), have passed legislation to increase the safety of drug supply chains. The immutability of blockchain systems would make it difficult to remove consumer data despite regulations such as the EU General Data Protection Regulation that requires erasure of personal information upon request of an individual in certain circumstances.



Source: Andrii Yalanski/stock.adobe.com. | GAO-22-104625

Vignette

Organizational Structure

Formal organizations—including companies, nonprofits, and government agencies—are central to commerce and other critical activities in society. Such organizations provide a wide range of services, from utilities to consumer goods to foreign aid to community building. Hierarchical organizational structures are common across these types of organizations. Blockchain offers one way to enable a type of non-hierarchical structure known as a decentralized autonomous organization (DAO).

Why blockchain?

Blockchain technology has enabled a new form of organizational structure, known as a decentralized autonomous organization (DAO). DAOs are entities in which groups of people collaborate and govern themselves online using a blockchain-based system of smart contracts and tokens. They differ from traditional organizations in how they are created, designed, and managed. For example, token holders can vote on individual proposals, with votes weighted based on how many tokens members hold. These governance decisions would be executed as blockchain transactions and enforced through the consensus mechanisms of the blockchain. DAOs primarily make sense as an organizational tool when the core business proposition is blockchain-compatible and there is a need to use cryptocurrencies and other tokens, because users can gain efficiencies from using those programmable assets.

One of the earliest examples of a DAO was known as "The DAO," which created a virtual venture capital fund that initially raised approximately $150 million worth of Ether cryptocurrency. The DAO sold tokens to investors and used the proceeds to fund projects, which could pay profits to DAO token holders as a return on their investment.

DAOs offer a number of features that are different from traditional organizational structures, including reduced hierarchy and easier payments management. For example, if the members of a DAO want to make an organizational change, any of its members could propose a new structure and have it voted on by the other members—in contrast to the common top-down approach of traditional organizations. In addition, DAOs may have a wider variety of options to manage payments. Because smart contracts deployed to a blockchain self-execute, payments that are earmarked for specific purposes occur automatically without an intermediary. Literature we reviewed stated that this efficiency could be potentially be useful in multiple contexts, such as in foreign aid distribution or in charitable giving.

Potential challenges and limitations of a blockchain-based system

- DAOs use smart contracts to conduct monetary transactions; therefore money held in DAOs is only as secure as the code used to create those smart contracts. For example, "The DAO" was hacked and one-third of the cryptocurrency held by it stolen because of a security flaw.
- DAOs are susceptible to faulty data being recorded on a blockchain, which could cause negative consequences such as a smart contract that unintentionally triggers a payment to a vendor. This could be more problematic for DAOs than other solutions because of the self-executional nature of smart contracts.
- DAOs are generally not recognized legal entities and it may not be clear how they will be treated by the legal system. However, the state of Wyoming passed legislation that allowed certain DAOs to register as legal entities starting in July 2021. As of December 2021, over 100 entities had registered under this law, including a DAO investment firm.

Source: Golden Sikorka/stock.adobe.com. | GAO-22-104625

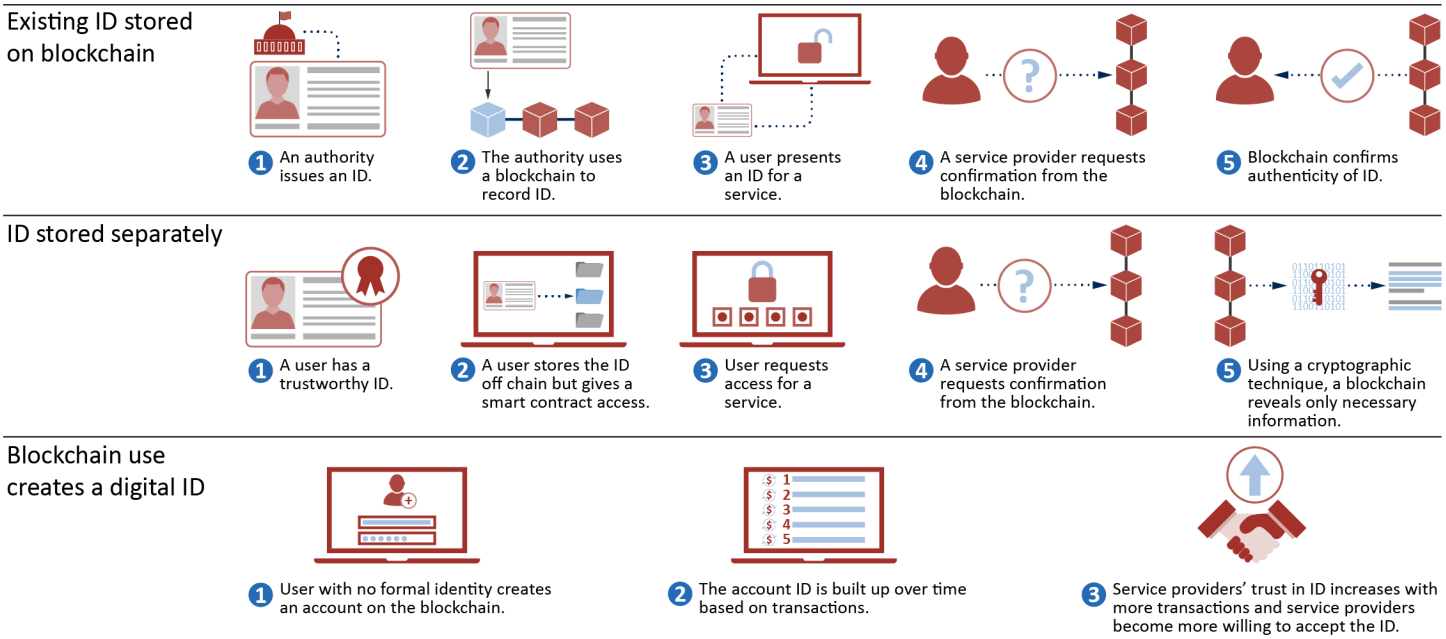
Vignette Digital IDs

Individuals need forms of ID because they allow people to interact in society and partake in transactions. Many transactions now occur electronically, and digital IDs provide trust in a digital interaction. However, digital IDs present challenges, such as maintaining privacy and interoperability. In addition, over 1 billion people do not have a formal ID, which further complicates assigning them a digital ID that could be used for government services.

Why blockchain?

Blockchain technologies may enhance digital IDs by adding transparency, traceability, and decentralization in certain situations, but some approaches may present challenges such as privacy concerns. A blockchain-based digital ID may give a user greater control over personal data than traditional ID systems. For example, specially-designed blockchains using smart contracts and advanced cryptographic techniques for digital IDs could provide proof of age without revealing any other information. In contrast, a driver's license includes personal information such as a birthday and driver's license number that may not be necessary for obtaining a specific service, unnecessarily exposing such personal information. However, blockchain technology is unproven in this area.

Potential examples of using a blockchain for digital ID management



Source: GAO analysis of federal agency documents and other literature. | GAO-22-104625

Potential challenges and limitations of a blockchain-based system

- **Data reliability.** Blockchain can only track the integrity of information once it is on the blockchain, and cannot verify that the original information was entered correctly. Because of this, ID issuers will still need to build, maintain, and manage their systems.
- **Privacy concerns.** While privacy concerns exist wherever there is data storage, because of the distributed and immutable nature of blockchain systems, these concerns are enhanced. For example, ID data stored on a public blockchain—even if encrypted—may result in a loss of privacy if encryption is broken at a future time.
- **Digital exclusion.** As with other non-blockchain solutions, user groups with lower rates of digital literacy or lack of internet access may be disadvantaged.

Source: Seventyfour/stock.adobe.com. | GAO-22-104625

Vignette Voting

Democracy depends on citizens being able to vote and having those votes accurately counted. Perceived and actual threats to voting equipment and computerized systems used to support the elections process—such as voter registration databases—may diminish public confidence and undermine the integrity of elections.

Why blockchain?

Some organizations and individuals have stated that switching to a blockchain-based voting system could offer several benefits, such as enhanced security of remote voting (e.g., using computers or smartphones) and enhanced auditability of an election. Some governments and companies have piloted blockchain voting systems, but it is unclear what advantages, if any, such systems would have over non-blockchain systems. In addition, they may not address all challenges and could introduce new vulnerabilities.

Table of possible voting challenges

Possible voting challenges	Authenticating valid votes	Maintaining ballot auditability	Preventing voter fraud	Allowing for voter anonymity	Providing voter access
Does blockchain help address challenge?	No	Unclear	No	No	Unclear

Source: GAO analysis of a state government document and other literature. | GAO-22-104625

How would a blockchain-based solution work?

Voting with blockchain could be a four-step process: (1) a jurisdiction generates the digital equivalent of unmarked ballot ovals; (2) the jurisdiction credits the potential votes to the registered voter's anonymous identification; (3) the voter makes a choice, which becomes a debit on the voter's account and a credit on an account belonging to the chosen candidate (or other ballot option); and (4) officials add the credits to the vote totals from other voting methods to determine the outcome.

According to one vendor of blockchain-based voting systems, such systems would likely need to be hosted on a permissioned blockchain network controlled by a certifying authority, such as a state's Chief Election Officer. This authority could control the number of blockchain nodes, the physical location of the servers that act as nodes, and the identity of the auditors of the system.

Potential challenges and limitations of a blockchain-based system

- In an election, observability and immutability—the main advantages of blockchain—might be achieved more simply by other means such as a centralized database to store election results and other information.
- Because blockchains are decentralized with many nodes, there might be added points of attack that could comprise elections.
- Existing blockchain-based voting systems do not appear to prevent voter fraud. Data are only tamper-resistant once on the blockchain. Therefore, blockchains cannot verify that an addition of external data, such as the casting of a vote, is correct.
- Blockchain networks rely on time stamping to create an unchangeable record of transactions, which could make it possible to link a vote to the voter's identity.
- Remote voting using a blockchain system—like electronic voting in general—requires access to specific hardware. Voters with lower rates of digital literacy or lack of internet access may be disadvantaged.


Source: Günter Albers/stock.adobe.com. | GAO-22-104625

Vignette

Carbon Credits

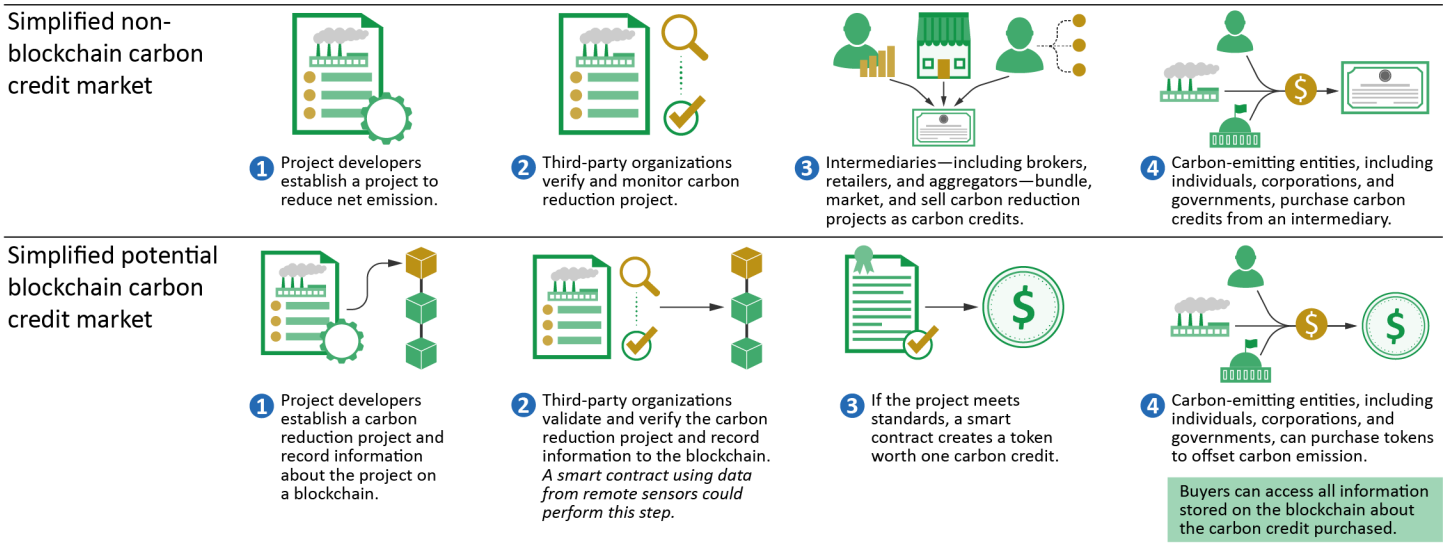
Carbon credits, also known as carbon offsets, are financial instruments that represent the reduction, avoidance, or removal of a certain amount of carbon dioxide or its equivalent. Individuals, businesses, and governments can purchase carbon credits to offset their own emissions and attempt to mitigate climate change. For example, a project developer can create a reforestation project. Challenges for carbon credits include verification, measurement, and equitable distribution of payments.

Why blockchain?

Blockchain may support a carbon credit market by minimizing the number of steps in the carbon credit supply chain, enhancing the auditability of these credits, and allowing more people to create and sell them. However, blockchain's ability to accomplish these goals is unknown, and challenges exist.

The use of blockchain may enhance the transparency of carbon credits compared to a non-blockchain system. The information on the creation, verification, and sales of a carbon credit can be made public on the blockchain, allowing a user to easily confirm its authenticity.

Comparison of a non-blockchain carbon credit market with a potential market using blockchain



Source: GAO and GAO analysis of literature. | GAO-22-104625

Potential challenges and limitations of a blockchain-based system

It is unclear whether a blockchain will solve key challenges associated with carbon credits (e.g., ensuring a reduction project generates additional offsets, measuring and managing offsets, verification, and equitable distribution of assets) and it may introduce new challenges. Using a blockchain for carbon credits presents the following limitations:

- **Data reliability.** A blockchain is limited by the accuracy of the data placed on the chain. Intermediaries, specifically, third-party inspectors, will still be needed to ensure the accuracy of the information. This continued need for inspectors limits blockchain's ability to remove intermediaries.
- **Limits for tasks beyond record keeping.** A blockchain does not directly address challenges such as measuring offsets because those tasks are done off the blockchain.
- **Adoption costs.** Blockchain may be more expensive compared to other technology solutions, which may discourage its adoption.
- **Inequitable distribution.** While blockchain aims to lower the costs associated with carbon credits by reducing the need for third-party regulators, it is unclear whether it would address the equitable distribution of the profit.

Source: Aldeca Productions/stock.adobe.com. | GAO-22-104625

Vignette Real Estate

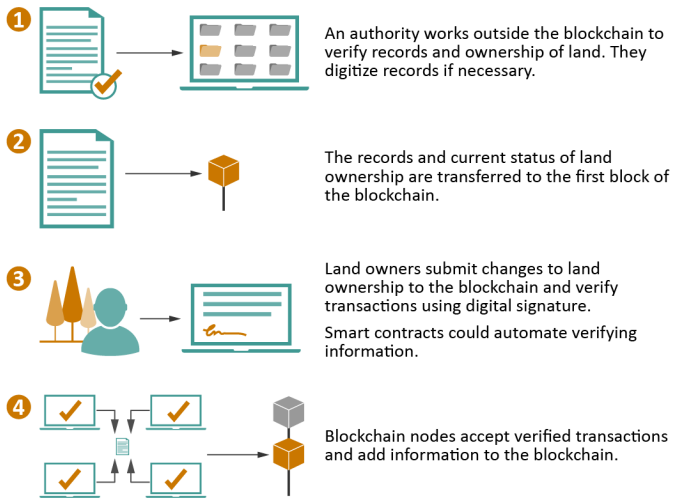
Globally, land is a critical source of wealth. Having legal title to land allows individuals to protect their ownership claims and use land as a financial asset. However, the titling process can be complicated, expensive, and time consuming. Furthermore, fraud, document tampering, complex land histories, and high costs can complicate title registry.

Why blockchain?

Blockchain has multiple qualities that make it suitable for storing a title registry system. A blockchain might both increase the speed of a title registry system and lower the cost of title insurance by making title registration simpler and more trustworthy. It may also simplify access to the myriad of documents and information needed to register title and transfer ownership. Using a blockchain to ensure all documents are accurate and complete may eliminate the need for some intermediaries, such as notaries and registrars.

At least four countries—Georgia, Ghana, Honduras, and Sweden—have piloted a blockchain title registry system, with varying degrees of success. One has attempted to use blockchain for title registry multiple times since 2014, but has faced challenges in its pilot programs. Another ended its pilot due to cost and lack of local expertise.

Simplified Example of Blockchain for Title Registry System



Source: GAO analysis of literature. | GAO-22-104625

Potential challenges and limitations of a blockchain-based system

- **Uncertain benefits.** If a government already operates a title registry system with trust and minimal fraud, then a blockchain may not produce sufficient benefits to justify its use.
- **Data reliability.** If fraudulent documents are added to a blockchain, it will perpetuate the incorrect information. Therefore, the title registry system needs to be trusted prior to transitioning to a blockchain; the blockchain solution cannot replace an untrustworthy registry.
- **Legal compliance.** Blockchain-based title registries may not be compatible with existing legal systems. In addition, these blockchain systems will need to adapt to future changes in laws and regulations. Furthermore, laws may need to be updated to recognize blockchain-based title registry systems.

Examples of possible title registry system challenges

Possible title registry system challenge	Fraud	Document tampering	Time	Cost
Does blockchain help address challenge?	✗ No	✓ Likely	? Unclear	? Unclear

Source: GAO analysis of state government document and literature. | GAO-22-104625

Vignette

Federal Government Operations

The federal government is one of the world's largest and most complex entities. The federal government spent about $6.6 trillion in fiscal year 2020 to fund a broad array of programs and operations. GAO routinely identifies government operations that face management challenges or are vulnerable to fraud, waste, and abuse. Several federal agencies have undertaken efforts to explore the potential of blockchain technologies to improve their operations—we highlight four examples below.

Why blockchain?

Federal agencies, including the Department of Homeland Security (DHS) and the Department of the Treasury (Treasury), have launched proof of concept efforts to investigate whether blockchain technologies could improve efficiency, accountability, and information sharing. Using blockchain can improve efficiency through its ability to remove intermediaries and automate time-consuming processes. A standard-setting group we spoke with stated that the technology may not be more efficient than current technologies in all proposed use cases and stressed that policymakers should focus on specific use cases that would be most likely to benefit from blockchain.

Examples of federal government blockchain proof of concept efforts

U.S. Customs and Border Protection (CBP) within DHS twice evaluated whether employing blockchain would provide compelling operational benefits and cost savings. The goal of the international trade effort was to evaluate blockchain's potential to improve processing of trade-related documents. The objective of the imported products effort was to increase CBP officers', retailers', and end-consumers' ability to quickly and cost effectively determine whether a product was being legally imported into the U.S. CBP identified several advantages of using blockchain in both of these solutions, such as increased the speed of internal processes, improved blockchain interoperability and import traceability, and increased data transparency, security, and immutability.

Additionally, the Bureau of the Fiscal Service (BFS) within Treasury twice examined whether blockchain could improve efficiency of some BFS projects. One of these efforts explored the potential to use blockchain to manage and track government-issued mobile phones. The other sought to improve understanding of whether a blockchain-based system could improve processing and audits of federal grants. Based on this work, BFS reported that there were multiple advantages of blockchain, such as: improving operational efficiency of mobile phone inventories and peer-to-peer transfers by automating certain manual processes, and automating financial controls and execution of grant payment audits.

Potential challenges and limitations of a blockchain-based solution

Based on the results of the four efforts we reviewed, it is unclear whether blockchain could improve efficiency, accountability, and information sharing for those specific use cases. Neither DHS nor Treasury adopted a blockchain-based solution following completion of their efforts. CBP and BFS experienced similar challenges and limitations of using blockchain, including:

- **Workforce development.** The federal government's long-standing workforce management challenges in strategically managing its workforce makes achieving the significantly higher workforce development (e.g. hiring and training) required to use blockchain harder to achieve.
- **Data security compliance.** If federal entities select public blockchains, those platforms may not align with current data security standards as well as laws, regulations, and agency policies that were designed in a pre-blockchain era. One expert emphasized that federal government blockchain efforts often ignore this concern and are consequently never able to find a path to operational deployment.
- **Legal authorities.** As with other non-blockchain technologies, blockchain applications need to ensure they have the proper legal authority to operate. For example, Treasury noted the uniform guidance for grant payments does not include an authorization to directly pay all grant awardees, such as sub-recipients.
- **Common infrastructure.** There is currently no federal guidance related to an appropriate way of creating and maintaining a blockchain network across the federal government.

2.1 Risks and challenges

We identified a number of challenges that may hinder adoption of blockchain across multiple non-financial applications, including a lack of interoperability across blockchains, uncertainty over legal and regulatory responsibilities, limited business and consumer understanding of how blockchains work, and insufficient information to accurately quantify potential costs.

Lack of interoperability and common standards. Most blockchain networks are not capable of communicating with other blockchain networks, creating the potential for data silos and making it difficult for users to transfer data across blockchains easily. Because of this, organizations that choose one blockchain platform may subsequently become locked into that platform without the ability to interoperate with or switch to others. According to multiple blockchain application developers we interviewed, blockchains were not designed to be interoperable, so users must choose the best one available for their purposes. However, it is unlikely that one available blockchain would meet every requirement, which can make users hesitant to adopt blockchain. Over time, firms may also need to support several different blockchains simultaneously, which may also contribute to some firms' reluctance to adopt the technology for business purposes.[12]

Some efforts are underway to help address interoperability challenges, including the development of common blockchain standards, but they are fragmented. Multiple experts said that standards are important to ensuring global interoperability and choice in the marketplace.[13] For example, standards could help users move data from one blockchain to another more easily. Additionally, while at least 30 organizations, such as the Institute of Electrical and Electronics Engineers (IEEE) and GS1, are developing or have developed standards, they remain fragmented, according to multiple organizations. With this fragmentation, developers may use different sets of standards or no standards when developing their blockchain applications, which may perpetuate the problem.[14]

Legal and regulatory uncertainty. The uncertain legal and regulatory environment in the U.S. may be hindering adoption of blockchain for non-financial applications. For example, in the case of supply chain management, one article we reviewed stated that, given the newness of the technology, unclear or nonexistent regulations may be hampering blockchain adoption.[15] Similarly, regulatory uncertainty could affect blockchain's adoption in real estate. According to a real estate firm, regulatory uncertainty surrounding

[12]T. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," *IEEE Access,* vol. 7, (2019): 45201-45218.

[13]We refer to experts specifically as those people who attended our expert meeting, and refer to anyone else we interviewed as either a stakeholder or by their entity affiliation throughout this summary and the remainder of the report.

[14]Global Blockchain Business Council, *Global Standard Mapping Initiative (GSMI) 2020,* (2020); and World Economic Forum, *Global Standards Mapping Initiative: An overview of blockchain technical standards,* (2020).

[15]M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," *International Journal of Production Economics,* vol. 231: 1-21.

blockchain makes investing in a real estate company that uses blockchain technology speculative or risky.

Legal uncertainty resulting from pending and potential future litigation may also affect blockchain adoption.[16] For example, the extent to which U.S. jurisdictions recognize smart contracts varies and can contribute to challenges.[17] When smart contracts are not legally recognized as binding contracts, there may be lengthy disputes and costly processes for all parties involved when a problem or legal issue arises, according to one literature source.[18] Furthermore, because blockchains often aim to remove intermediaries, there may be legal uncertainty around who is responsible if there is a mistake on the blockchain. Using property title transfer as an example, in a non-blockchain based system, a notary or title company may be held responsible if there is a defect in a deed or title of the property. If a blockchain removes those intermediaries, it is unclear who would be held responsible for a mistake on a deed or title.

Limited understanding. Due in part to the relative newness of blockchain technology, businesses, consumers, and the government may not understand how the technology works and lack the technical talent to better understand it, which could limit adoption. Five organizations we interviewed said it was challenging to find talent able to successfully develop, implement, and deploy blockchain technology within their organizations.[19] Multiple experts and studies described how businesses lack information about the technology, its benefits, and how to implement it.[20] For example, users cited as concerns a lack of understanding about how permissioned blockchain systems work and how data on the blockchain are shared among users. We previously reported that federal government agencies have faced challenges in hiring, managing, and retaining staff with digital skills because of a limited pipeline of candidates.[21]

[16]D. Bonyuet, "Overview and Impact of Blockchain on Auditing," *International Journal of Digital Accounting Research*, vol. 20 (2020): 31-43.

[17]For example, in June 2016, Vermont became the first state to enact a law to consider blockchain-based records, such as smart contracts, as a business record pursuant to the Vermont Rules of Evidence. More recently, in 2020, Illinois enacted the Blockchain Technology Act, which in part makes smart contracts and blockchain records admissible as evidence in legal proceedings. Arizona and Tennessee, among other states, have passed similar legislation addressing smart contracts. Other states have formed working groups to explore a variety of topics related to smart contracts and other applications of blockchain technology.

[18]J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," *IEEE Access,* vol. 7 (2019): 36500-36515.

[19]In addition, one cryptocurrency platform representative we interviewed and one expert stated that the U.S. government lacks a strategy to attract and develop experts knowledgeable about blockchain technology.

[20]Kouhizadeh, Saberi, and Sarkis*,* "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," *International Journal of Production Economics* vol. 231: 1-21; A. J. Collart and E. Canales, "How might broad adoption of blockchain-based traceability impact the U.S. fresh produce supply chain?" *Applied Economic Perspectives and Policy,* (2021): 1-18.

[21]GAO, *Digital Services: Considerations For a Federal Academy to Develop a Pipeline of Digital Staff*, GAO-22-105388 (Washington, D.C.: Nov. 19, 2021).

Undefined benefits and costs. Organizations can also face difficulties quantifying the anticipated benefits and costs of switching to blockchain technology. For example, as we described earlier in this chapter, one potential benefit of adopting a blockchain solution may include increased transparency into product provenance, but this benefit may be difficult to quantify. Meanwhile, costs can include not only the initial cost of deploying a blockchain, but the time required for individuals to understand the underlying business processes, which may also be difficult to quantify.[22] One pharmaceutical distributor we interviewed stated that acquiring new technology requires them to justify their needs and expected benefits up front, but they found this difficult to do with blockchain because it is an immature technology with poorly defined costs. As a result, they may choose other technologies.

[22]Alba J. Collart and Elizabeth Canales, "How might broad adoption of blockchain-based traceability impact the U.S. fresh produce supply chain?" *Applied Economic Perspectives and Policy,* (2021).

3 Financial Blockchain Technologies Are in Use and Offer Several Benefits

The most well-known applications of blockchain are in the financial sector, particularly due to the rise in the use of cryptocurrencies such as Bitcoin. Other financial applications have also been deployed, including lending and borrowing through decentralized finance (DeFi). Decentralization of financial systems through blockchain may lead to cost savings, expanded access to financial products, and other transformational changes. However, several risks and challenges may prevent these benefits from being realized, or may even lead to negative consequences for users and the financial system.

3.1 Cryptocurrencies

Cryptocurrencies are generally a digital representation of value protected through cryptographic mechanisms instead of a central repository or authority. They are usually not government-issued legal tender (i.e., fiat currency). They can act as investments or money on blockchain ledgers by allowing users to transfer them to other users without the need for a centralized third party or payment system. Investors can also invest in companies or funds that either hold cryptocurrencies or engage in cryptocurrency activities. Because cryptocurrencies are digitally based and generally do not depend on intermediaries—who charge fees to recoup costs and make a profit—they have the potential to reduce user costs. In addition, users can conduct transactions under pseudonyms, which may appeal to people who seek greater privacy for their financial activities.

Exchanging cryptocurrency

Users may want to exchange one cryptocurrency for another, or for fiat currency (government-issued legal tender such as the U.S. dollar). Companies that perform such services are often referred to as "exchanges." Options include decentralized exchanges—software programs that do not have an identifiable administrator and operate on a peer-to-peer network running a blockchain platform—and cryptocurrency kiosks—similar to ATMs. Kiosks can also sometimes exchange fiat cash for cryptocurrency, which, as we have previously reported, have been increasingly used to enable human and drug trafficking.

Source: GAO, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, GAO-22-105462 (Washington, D.C.: Dec. 8, 2021).

Cryptocurrencies are also growing as a means of payment by individuals, businesses, and governments around the world, for both online and off-line transactions. For example, one of the largest online payment systems in the world recently announced it would allow customers in the U.S. to pay for purchases across millions of online businesses using cryptocurrency. Additionally, several major companies in sectors such as automotive, technology, and retail have begun to accept cryptocurrencies as payment.

Another type of payment involves cross-border capital flows, such as remittances.[23]

[23]Definitions of remittances vary based on the transfer method, purpose, and provider—that is, the entity transferring the funds for the sender. For purposes of this report, we define remittances as transfers of funds from one person or business in one country to another person or business in another country.

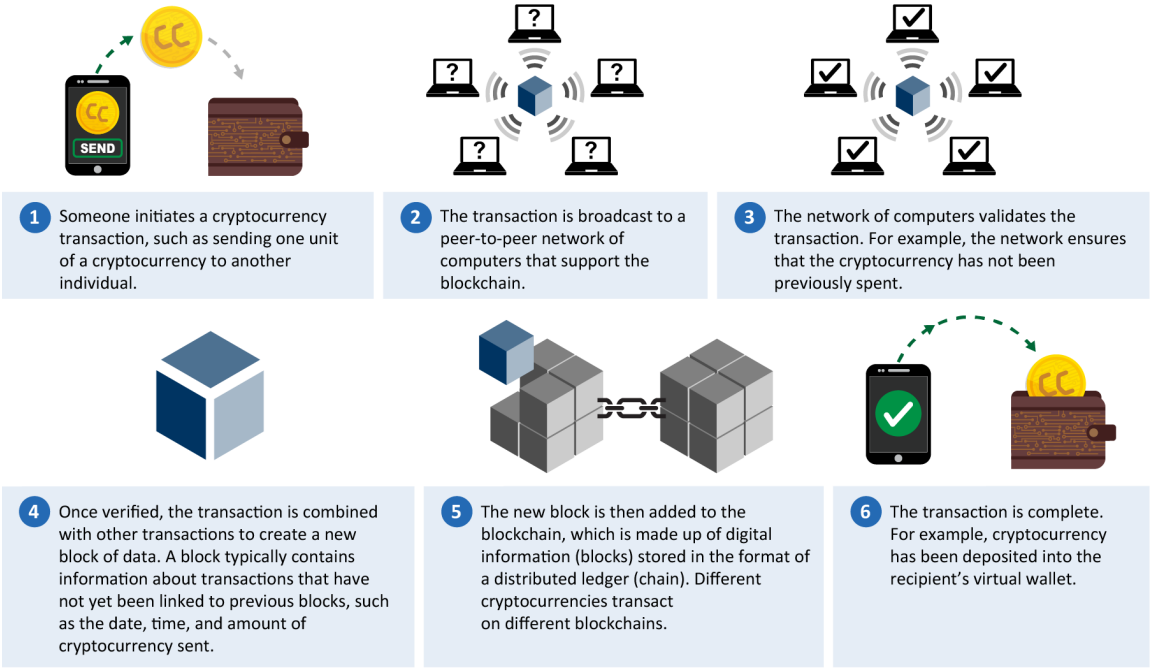
One recent National Bureau of Economic Research working paper estimated that at least 1.4 percent, or 630,000, of the 45 million Bitcoin transactions it reviewed from March 2017 to July 2021 were used for remittance or remittance-like purposes.[24] Cryptocurrencies may offer especially pronounced savings when compared to international monetary transfers and payments, which involve more intermediaries than domestic transfers. According to the World Bank, global personal remittances received were estimated to total $6.9 trillion dollars in 2020 and, as of March 2021, the global average remittance fee for traditional currency remittances was 6.38 percent per transaction, far higher than the fee for a cryptocurrency-based remittance. As an example, sending $500 from the U.S. to South Africa would cost between $8 and $56, according to one large global remittance provider, and around 13 cents on the Bitcoin network, according to one Bitcoin fee estimator.

In order to send cryptocurrency, a user must have a private key—a secret set of letters and numbers that is computationally generated. The computation is infeasible to replicate, and therefore losing a private key means the user will likely lose access to that cryptocurrency. One workaround for this risk is a cryptocurrency wallet, a software program that allows users to trade cryptocurrency by storing these keys along with associated addresses.[25] See figure 6 for an example of a cryptocurrency transaction.

[24]Von Luckner, C.G., Reinhart, C. M., and K.S. Rogoff. "Decrypting new age capital flows," *National Bureau of Economic Research* (Cambridge, MA: Oct. 2021).

[25]Wallets are software programs that allow people to "store" their cryptocurrency. However, these wallets do not store cryptocurrencies the way that traditional wallets store cash. Instead, they store various components of cryptocurrency transactions, such as private keys, public keys, and addresses that allow the user to gain access to the currency. These wallets come in many forms, including web-based, desktop, mobile, paper, and hardware.

Figure 6: Example of how a company might send cryptocurrency to another company using blockchain technology



Source: GAO. | GAO-22-104625

The cryptocurrency market has rapidly expanded over the past several years, at times showing large increases in valuations and users. The total size of the cryptocurrency market is unknown, but some data are available that provide context.[26] According to one index, the total market capitalization of cryptocurrencies it tracked was about $1.75 trillion as of March 2022, compared to about $250 billion in September 2019.[27] The total market capitalization of Bitcoin, one of the most prominent cryptocurrencies, is estimated to be over $740 billion as of January 2022.[28] According to a cryptocurrency asset management company, as of September 1, 2021, 10 major cryptocurrency exchanges had collectively handled an average daily trading volume in Bitcoin of more than $4 billion. As of September 2021, one large U.S.-based cryptocurrency exchange reported having more than 68 million accounts.

However, along with this growth has come price volatility. For example, the fair market value of Bitcoin has changed dramatically over time. The value of one Bitcoin increased from about $960 in January 2017 to over $63,500 by April 2021; as of March 8, 2022, it

[26]We provide some figures to provide context for the possible size of the cryptocurrency market. However, we did not assess the reliability of the data.

[27]Total market capitalization is the sum of individual cryptocurrencies' market capitalizations, which CoinMarketCap determines by calculating the average price of a cryptocurrency multiplied by the circulating supply of that virtual currency. https://www.coinmarketcap.com, accessed March 8, 2022.

[28]https://www.coinmarketcap.com, accessed March 8, 2022.

had declined to just over $38,986.[29] Although the price growth has been beneficial for some investors, it also comes with greater risks than some investments. The Financial Stability Board reported that cryptocurrency prices have been highly volatile, with cryptocurrencies that are not backed by any contractual claim especially subject to price fluctuations.[30] Another study found that the volatility of prices for Bitcoin was almost 10 times higher than the volatility of major exchange rates, such as the U.S. dollar against the euro and the yen.[31]

3.2 Stablecoins

Stablecoins, an even more recent entrant to the global financial system, are a form of cryptocurrency designed to hold a stable value over time (in contrast with traditional cryptocurrencies such as Bitcoin). One of the first major stablecoins was founded in 2014 and has a market capitalization of over $78 billion as of January 2022. The combined stablecoin supply grew from $21.5 billion in October 2020 to $127.9 billion in October 2021, a nearly 500 percent increase.[32]

Stablecoins use one or more of the following methods to maintain a stable value, although there is debate about which approaches may most effectively promote stability:

- **Real-world asset-backed**. This type of stablecoin is generally redeemable on a one-to-one basis with actual fiat currency or other assets held in a trust company or a bank.
- **Virtual asset-backed**. Instead of being backed by real-world assets, these stablecoins are backed by virtual assets, such as a portfolio of cryptocurrencies.
- **Algorithmic**. These stablecoins use algorithms to artificially control the cryptocurrency supply or the supply of the pools of cryptocurrency collateral to maintain a stable value, similar to how central banks function.

According to the Financial Action Task Force, this stabilization function can be either decentralized—distributed among a range of entities or managed by software—or operated by a single central entity.[33] Likewise, the transfers and the user interface may be distributed among many cryptocurrency exchanges or wallet providers, or centralized.

Stablecoins are generally created in exchange for fiat currency that an issuer receives from a user or third party; this user or third party can then use the stablecoins they receive to facilitate trading, lending, and borrowing of other digital assets. These capabilities reduce the need for fiat currencies and traditional

[29]The open value is the starting value of one Bitcoin recorded each day, https://coinmarketcap.com/currencies/bitcoin/historical-data/, accessed December 3, 2021 and March 8, 2022.

[30]The Financial Stability Board is an international body that monitors and makes recommendations about the global financial system. Financial Stability Board, "Crypto-asset markets: Potential channels for future financial stability implications," (October 10, 2018).

[31]Dirk G. Baur and Thomas Dimpfl, "The volatility of Bitcoin and its role as a medium of exchange and a store of value," *Empirical Economics* (January 5, 2021).

[32]President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, "Report on Stablecoins" (Washington, D.C.: November 2021).

[33]Even if operated by a central entity, the nodes of the blockchain maintain some decentralization. The Financial Action Task Force is an international standard-setting organization focused on money laundering and terrorist financing. Its members include the U.S., China, the Russian Federation, and the European Commission. Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins* (Paris, France: June 2020).

financial institutions. According to the International Monetary Fund, stablecoin trading volume outpaces all other digital assets, primarily because they are used to settle certain types of financial transactions.[34]

Stablecoins, similar to other cryptocurrencies, can also be used as a means of payment to settle contracts and other transactional needs and have multiple potential benefits. For example, individuals who live in countries with unstable currencies might consider cryptocurrencies, particularly stablecoins, to be a more stable store of value than their fiat currency. In a country with a more stable currency, stablecoins tied to that currency may offer benefits over other cryptocurrencies if they are more interchangeable with the fiat currency. This, along with other more general benefits of cryptocurrencies such as their borderless nature and potentially lower transaction costs, might enable stablecoins to substitute for payment methods such as credit cards.[35] Stablecoins also play a central role in facilitating trading, lending, and borrowing activity in DeFi by creating the stable prices that participants require (see below). Further, according to the Financial Action Task Force, use of stablecoins with centralized management could help regulators mitigate money laundering or transnational financial crime because centralized entities can be regulated more easily.[36]

Potential Future Stablecoin Scenarios

An International Monetary Fund policy paper described four scenarios of how stablecoins might be used internationally as a method of payment:

- **Niche uses for cross-border payments**. A stablecoin could be used as a preferred vehicle for small-value transactions, such as remittances across borders, due to the lowered cost and increased efficiency of stablecoin-based cross-border payments.
- **Greater currency substitution in some countries**. A stablecoin could induce greater use of a more stable foreign currency in a country with high inflation and unstable exchange rates.
- **Global adoption**. A single stablecoin could be adopted across multiple countries and replace the local currency as a store of value, means of payment, and unit of account, and also become widely used for international transactions. Eventually the stablecoin may not need to be pegged to another currency and could become a fiat currency.
- **Global adoption with multipolarity**. This scenario could arise if multiple stablecoins compete with one another. For example, there may be "digital currency areas," where the use of a stablecoin is not determined by geographic barriers but instead by the boundaries of the e-commerce or social media platforms that use it.

Source: International Monetary Fund, *Digital Money Across Borders: Macro-Financial Implications* (Washington, D.C.: Sept. 22, 2020).

Stablecoins also have some potential drawbacks. For example, according to the literature we reviewed and one stablecoin developer we interviewed, consumers may not understand what the value of their stablecoin is pegged to or in what assets their stablecoin may be investing its reserves. The value of stablecoins might also fluctuate more than consumers anticipate. In addition, certain factors may make it more difficult for consumers and the broader financial system to access capital. For example, other creditors could have a claim on the reserve assets that

[34]International Monetary Fund, Global Financial Stability Report: Covid-19, Crypto and Climate: Navigating Challenging Transitions, (Washington, D.C.: Oct. 2021).

[35]Credit card transaction costs are deducted from payments to the merchants. Merchants do not receive the full purchase amount because a certain portion of the sale is deducted to compensate the merchant's bank, the bank that issued the card, and the card network that processes the transaction.

[36]Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins* (Paris, France: June 2020).

competes with stablecoin holders' claim on those same assets.[37]

3.3 Lending and borrowing through decentralized finance

Intermediaries play a central role in traditional financial markets, serving as agents and brokers of trust, liquidity, settlement, and security. The range and importance of intermediaries have grown over time to meet the needs of an increasingly complex financial system. However, one report issued by The Wharton School and the World Economic Forum raised concerns about the inefficiencies, structural inequalities, and hidden risks of the intermediated financial system.[38]

Decentralized finance (DeFi)—a broad term for financial services built using the decentralized foundations of blockchain technology—attempts to address those risks, among others. It encompasses a variety of technologies, business models, and organizational structures, but in general, it uses software instead of financial institutions to implement financial services and combine those services in flexible ways. The total value locked in DeFi contracts grew from about $100 million in 2018 to over $80 billion as of May 2021, according to the Federal Reserve and others.[39] One expert we spoke with expected to see DeFi continue to grow, likening it to a reimagined Wall Street.

One example of a DeFi service is blockchain-based lending, which allows users from around the world to borrow and loan digital assets. Lending and borrowing are central to finance because they facilitate risk-taking and expand the supply of capital. DeFi-based lending platforms are unique in that they allow both borrowers and lenders to remain anonymous. DeFi-based loans therefore do not rely on trust between the parties. A DeFi-based, fully secured, collateralized loan locks collateral into a smart contract and only releases it once the debt is repaid (see fig. 7). A DeFi loan may be used to get a loan in a type of digital asset, such as a cryptocurrency, that is different from the asset used as collateral. For example, borrowers might want to use a DeFi loan if they want to borrow a digital asset that is more price stable than the collateral.[40] In another example, they may need liquidity but want to avoid being taxed when selling the collateralized asset.

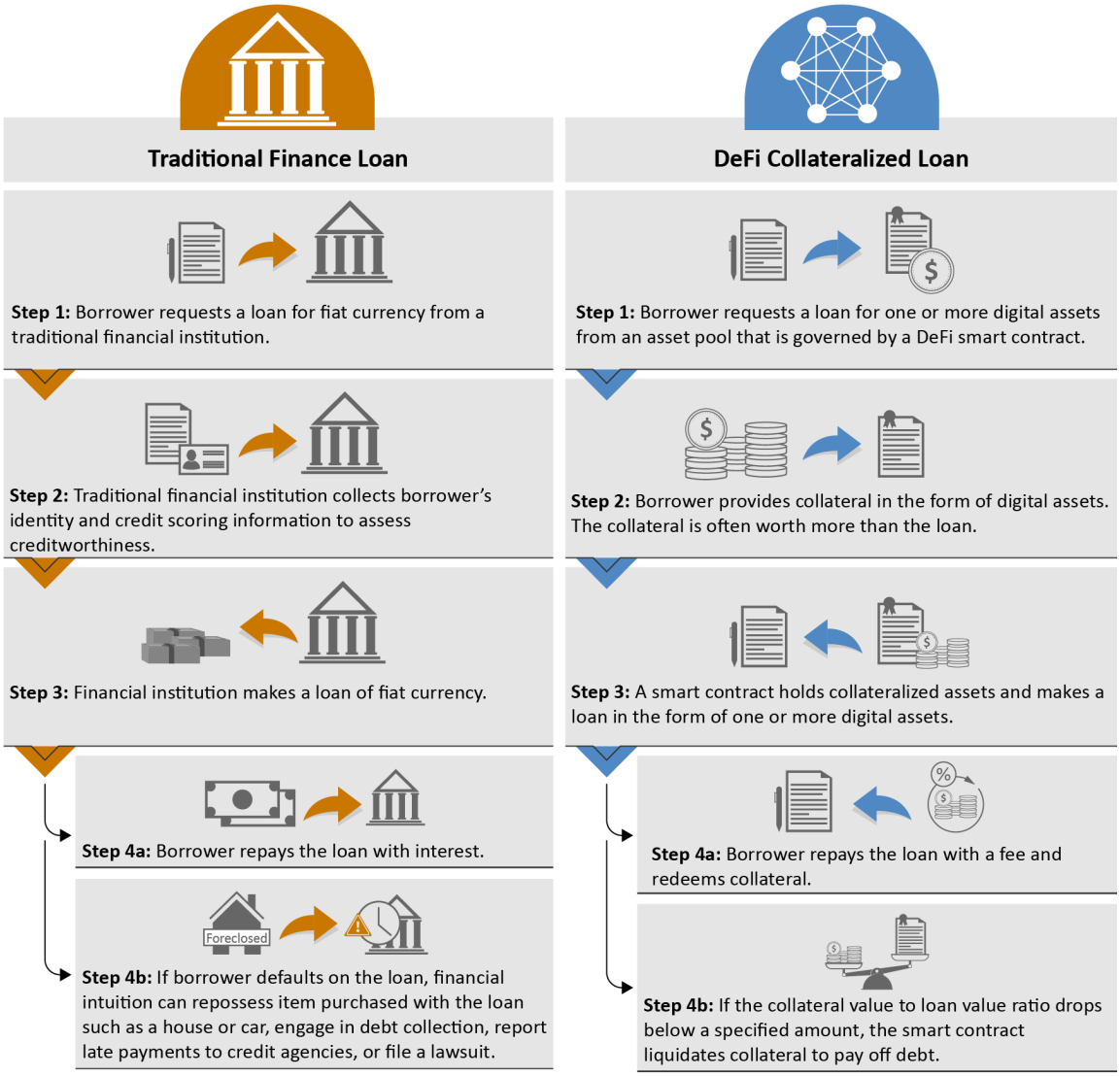
[37]For a discussion of the latter issue, see President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins*, (Washington, D.C.: November 2021).

[38]Wharton Blockchain and Digital Asset Project in Collaboration with the World Economic Forum, *DeFi Beyond the Hype: The Emerging World of Decentralized Finance*, (Philadelphia: PA, May 2021).

[39]Total value locked is a measure of DeFi market size that refers to the value of digital assets committed for transactions in DeFi systems. Federal Reserve Bank of St. Louis, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,* (St. Louis, MO: Feb. 5, 2021) and Wharton Initiative on Financial Policy and Regulation and the World Economic Forum, *DeFi Beyond the Hype: The Emerging World of Decentralized Finance* (Philadelphia, PA: May 2021).

[40]As discussed above, certain cryptocurrencies are prone to price volatility.

Figure 7: Comparison of traditional finance loan and decentralized finance (DeFi) collateralized loan



Source: GAO analysis of federal government publications and other literature. | GAO-22-104625

In addition, new innovations are occurring in the DeFi-lending space, some of which resemble more traditional financial products but without a centralized issuer. For example, fixed-rate loans offer a stable interest rate despite fluctuations in the value of the underlying assets. Another innovation is credit delegation, which allows users to deposit assets into a DeFi lending service and then authorizes trusted users to draw against the collateral. This allows a depositor who is not using their full line of credit to delegate part of it to someone else whom they trust, and charge that person interest. Borrowers can also refinance loans at more favorable terms. Another example is a set of corporate credit services that allow institutions to borrow from liquidity pools managed by experienced investors.

DeFi-based loans may offer a number of benefits:

- Some aspects of DeFi may be more inclusive than traditional financial products. According to the Bank for International Settlements, like cryptocurrencies, DeFi may reduce user costs because it is decentralized rather than relying on intermediaries to make transactions, reducing one potential barrier to entry.[41] Further, DeFi may offer greater access to financial services for the 1.7 billion adults, globally, who do not have access to a bank account. One Federal Reserve report discussed how anyone can use DeFi protocols, which might lead to a more accessible financial system with less discrimination.[42] However, DeFi loans may require collateral, something that might be a barrier to those who have been left out of the traditional financial system.
- DeFi-based loans are transparent, with all transactions publicly observable. This transparency could assist regulators in monitoring financial markets for illicit activity or systemic risk.[43] It could also help regulators and others understand loan marketplaces in real time and help to prevent and manage crises.[44] For example, in the case of a crisis, the availability of current and historical data for DeFi loans is much greater than that of traditional financial loans, where information can be scattered across a large number of proprietary databases or even completely unavailable.

DeFi-based lending also presents some potential drawbacks. For example, the Securities and Exchange Commission (SEC) noted that many DeFi promoters do not provide investors with the detail needed to assess risk likelihood and severity.[45] Further, a World Economic Forum report explained that, if DeFi continues to grow and attract less-sophisticated market participants, these investor protection concerns may increase.[46] Some types of DeFi loans have been used to

[41]G7 Working Group on Stablecoins*, Investigating the Impact of Global Stablecoins,* (Basel, Switzerland: Oct. 2019).

[42]F. Schar, "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets," *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2 (2021): 153-174.

[43]While there is no agreed-upon definition of systemic risk, the term generally refers to the risk that an event could broadly affect the financial system rather than just one or a few institutions.

[44]F. Schar, "Decentralized Finance," 153-174.

[45]Securities and Exchange Commission, *Statement on DeFi Risks, Regulations, and Opportunities*, (Washington, D.C.: Nov. 9, 2021).

[46]World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, (June 2021).

steal millions of dollars through network attacks by temporarily manipulating prices to force artificial liquidation of smart contracts.

3.4 All blockchain-based financial products face challenges

In addition to the previously described individual challenges that cryptocurrencies and DeFi face, the entire category of blockchain-based financial products faces a set of common challenges. These include risks for users and to the broader financial system due to a current lack of consumer protections, and the ability to use the technology to facilitate illegal activity.

- **Fewer consumer protections.** Consumers and investors may face increased risks. For example, federal deposit insurance may not cover losses to cryptocurrency balances, and consumers may not be aware of associated risks if cryptocurrency exchanges go out of business.[47] If tokens do not meet the definition of a security, protections under the Securities Act of 1933 and the Securities Exchange Act of 1934 may also not apply. In addition, funds can be stolen through fraudulent token sales, using fake business plans, which criminals have used to defraud consumers of billions of dollars in cryptocurrency. The SEC has reported that an investor's ability to recover funds may be limited if key parties to token sales are located overseas or operating unlawfully.[48]
- **Risks to the financial system.** Multiple organizations have recognized the potential future risks cryptocurrencies pose to financial stability and the formal financial system. For example, a Financial Stability Board report stated that large operational disruptions in stablecoins that are relied upon for regular payments (such as remittances) could significantly affect economic activity and financial systems.[49] Additionally, the International Organization of Securities Commissions identified potential market integrity risks of cryptoasset trading platforms as one of its top priorities. This includes situations where trading platforms give preferential treatment to a subset of their users or offer advice to customers related to an asset in which the trading platform may have an interest. Officials from multiple organizations told us that while some risks are not currently significant given the limited size of cryptoasset markets relative to other financial markets, cryptocurrencies could pose a danger to the stability of and undermine confidence in existing monetary and financial systems if they become a more significant part of financial markets.[50] For example, one interagency report described how insured

[47]GAO, *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges,* GAO-14-496 (Washington, D.C.: May 2014).

[48]Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207* (July 25, 2017).

[49]Financial Stability Board, *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations*, (Basel, Switzerland: Oct. 13, 2020).

[50]Global Blockchain Business Council, *Global Standard Mapping Initiative (GSMI) 2020,* (Washington D.C.: 2020); World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, June 2021; and Financial Stability Board, *Crypto-asset markets: Potential channels for future financial stability implications*, (Oct. 10, 2018).

depository institutions could lose retail deposits to stablecoins whose reserve assets do not support credit creation, which might then lead to increased borrowing costs and impair credit availability in the real economy.[51] Further, the report explained that the prospect of a stablecoin not performing as expected could result in a "run" on that stablecoin, which it called a self-reinforcing cycle of redemptions and fire sales of reserve assets.[52] These concerns may also be relevant for non-stablecoin cryptocurrencies that have comparable international reach, scale, and use.

Blockchain-based financial products can also pose challenges to law enforcement, regulators, and others. These challenges include:

- **Illicit activities.** Officials at the Drug Enforcement Administration told us that drug traffickers have increased the use of cryptocurrency for illicit activities, because it is widely adopted and easy to use and transfer.[53] In addition, law enforcement officials previously told us that the perception of anonymity makes cryptocurrency a preferred tool for certain types of trafficking activities. Money-laundering organizations also use cryptocurrency to transfer proceeds from illegal activities across borders on behalf of transnational criminal organizations. For example, according to the Drug Enforcement Administration, money-laundering organizations in Asia have been working with drug trafficking organizations in Central America with increased frequency, and cryptocurrencies are one of their methods for facilitating drug money movement. Terrorists are also using cryptocurrency platforms, and we previously reported that cryptocurrencies pose an emerging terrorist finance vulnerability because they are accessible from anywhere and difficult to trace.[54] However, we found that it is easier to track cryptocurrency activities than cash-based transactions, which leave no digital trail. For example, public blockchains allow investigators to trace transactions and participants.
- **Regulatory oversight.** Unclear and complex regulation could cause some blockchain-based businesses to alter development of their blockchain product, fail to launch their product, or move their product to areas with greater regulatory clarity, according to multiple experts we interviewed. One industry association report stated that the regulatory complexity in the U.S. has driven many new blockchain ventures overseas and caused many existing companies to stop providing service to the U.S. market.[55] For

[51]President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins*, (Washington, D.C.: Nov. 2021).

[52]Fire sales occur when an institution is forced to sell an asset at a price below its fundamental value.

[53]GAO, *Trafficking and Money Laundering: Strategies Used by Criminal Groups and Terrorists and Federal Efforts to Combat Them,* GAO-22-104807 (Washington, D.C.: Dec. 23, 2021).

[54]GAO, "*Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight*," GAO-18-254 (Washington, D.C., Mar. 22, 2018).

[55]Global Blockchain Business Council, *Build Back Better: Digital Updates for Today's Challenges Annual Report*. (Geneva/London/Washington, D.C./New York, NY, 2021). While regulatory uncertainty was identified as a challenge hindering blockchain adoption, a report from the UCLA Law Review states that as more regulators around the world announce new

example, staff from one U.S. firm that developed a blockchain-based payments technology previously told us that they and their peers only work with foreign customers due to the fragmented U.S. regulatory structure and differing agency positions on blockchain related topics.[56] Experts and officials from one financial regulatory agency also discussed how efforts to coordinate regulatory efforts across the federal government are ongoing and incomplete.

Regulations are complex for some blockchain applications, according to multiple studies and experts.[57] For example, the Department of the Treasury Financial Crimes Enforcement Network (FinCEN) determined that certain businesses engaging in cryptocurrency transactions would be subject to regulation as money services businesses. The Internal Revenue Service treats Bitcoin as property for federal tax purposes.[58] Further, SEC has stated that certain types of initial coin offerings (ICOs) may be securities offerings and fall under the SEC's jurisdiction of enforcing federal securities laws. Issusers of ICOs need to consider whether the digital asset has the characteristics of any product that meets the definition of a "security" under federal security laws. In addition, as we note in chapter 2, it is unclear the extent to which various U.S. jurisdictions recognize smart contracts as legally binding contracts and who would be responsible should disputes arise. Further, an interagency report described how stablecoin arrangements are not subject to a set of consistent prudential regulatory standards.[59] We have previously reported that the U.S. financial regulatory structure is itself fragmented, with overlapping responsibilities shared between and among state and federal financial regulators for different types of financial institutions (see fig. 8).[60]

---

regulations on cryptocurrency activity, there is growing concern additional regulation could stifle innovation. For example, the New York State Department of Financial Services (NYDFS) issued regulations requiring all businesses handling cryptocurrency to apply for a "Bitlicense," a business license of cryptocurrency activities. According to this report, the announcement led to a "Bitcoin exodus" in which at least 10 cryptocurrency businesses decided to shut down after calculating the costs of acquiring a permit; Nareg Essaghoolian, "Initial Coin Offerings: Emerging Technology's Fundraising Innovation," *UCLA Law Review,* vol. 66 (2019): 294.

[56]GAO, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight,* GAO-18-254 (Washington, D.C.: Mar. 22, 2018).

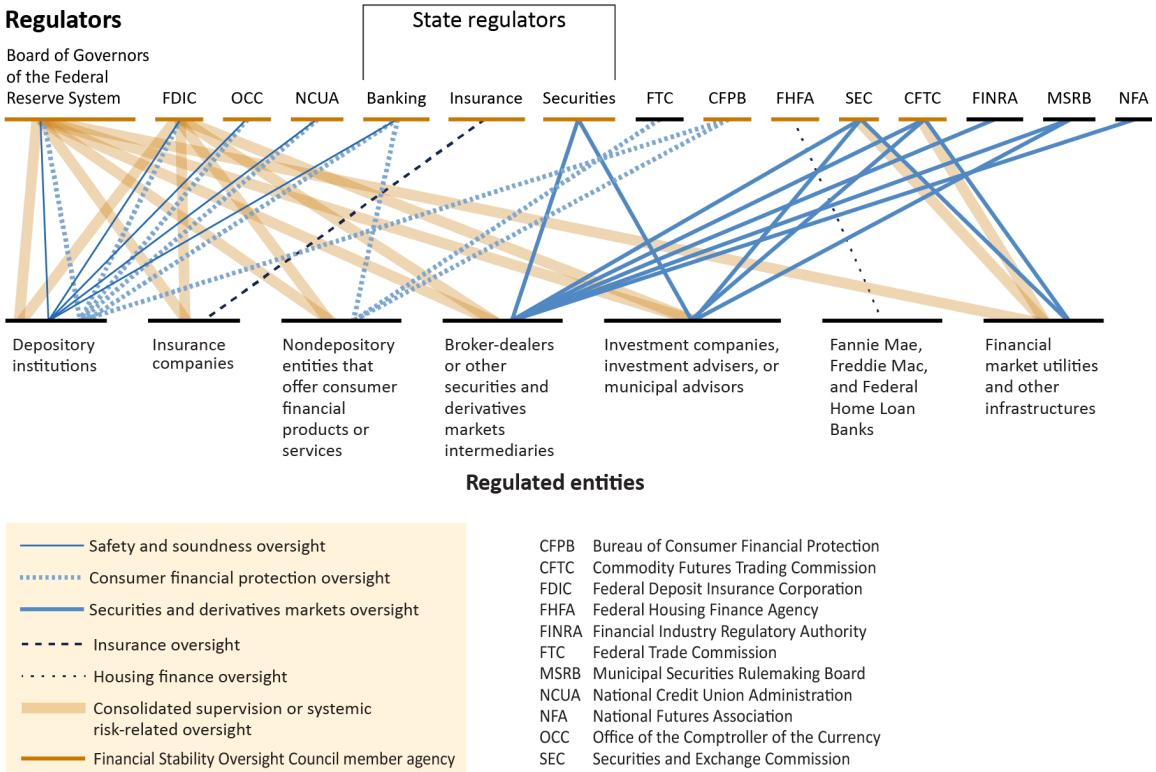
[57]Huanhuan Feng, Xiang Wang, Yanqing Duan, Jian Zhang, and Xiaoshuan Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," *Journal of Cleaner Production,* vol. 260 no. 121031 (2020) and Ali Omar, Jaradat Ashraf, Kulakli Atik, and Abuhalimeh Ahmed, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities," *IEEE Access*, vol. 9 (2021); Marco Maffei, Raffaela Casciello and Fiorenza Meucci, "Blockchain technology: uninvestigated issues emerging from an integrated view within accounting and auditing practices," *Journal of Organizational Change Management,* vol. 34, no. 2 (2020); Apolline Blandin, Gina Pieters, Yue Wu, Thomas Eisermann, Anton Dek, Sean Taylor, and Damaris Njoki, "Third Global Cryptoasset Benchmarking Study," *Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School* (2020) and Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev, "Blockchain beyond the hype: What is the strategic business value?" *McKinsey & Company* (2018).

[58]GAO, *Financial Technology: Information on Subsectors and Regulatory Oversight,* GAO-17-361, (Washington, D.C.: Apr. 19, 2017).

[59]President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins*, (Washington, D.C.: Nov. 2021).

[60]GAO, *Financial Regulation: Complex and Fragmented Regulatory Structure Could be Streamlined to Improve Effectiveness*, GAO-16-175, (Washington, D.C.: Feb. 25 2016).

Figure 8: U.S. Financial Regulatory Structure



Source: GAO. | GAO-22-104625

Note: This figure depicts the primary regulators in the U.S. financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets, including Department of the Treasury Financial Crimes Enforcement Network, and there may be other possible regulatory connections than those depicted in this figure.

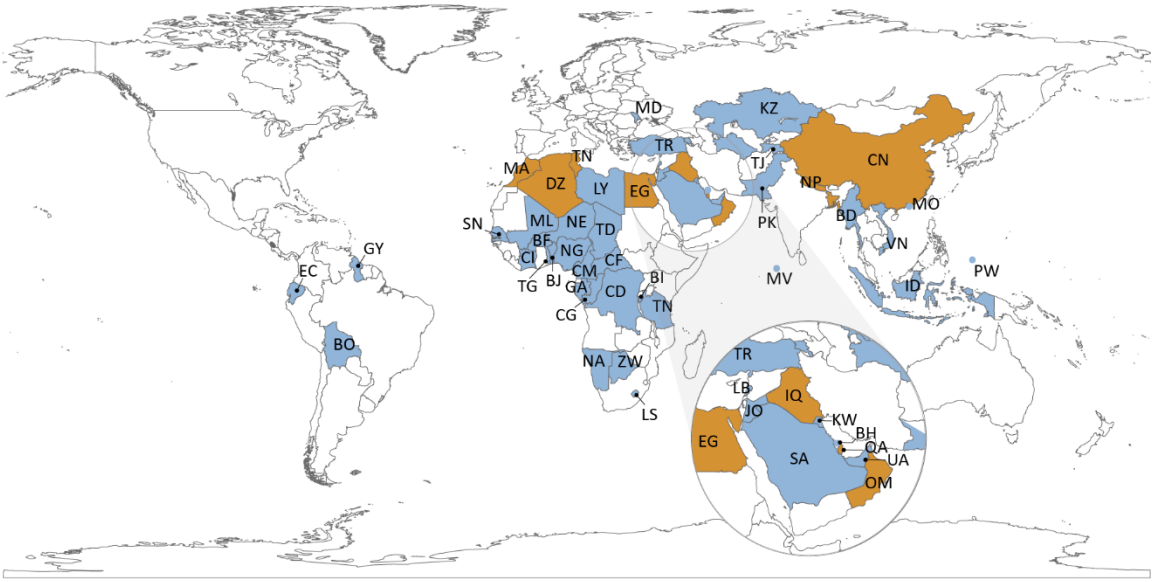
Regulating blockchain-based financial applications can be challenging. We found that one reason is that it is difficult for regulators to determine how to regulate applications that use decentralized protocols. For example, the decentralized and anonymous nature of DeFi services may make it difficult to identify a responsible party if these services are used to facilitate illicit activities. In addition, the operational complexity of a stablecoin arrangement and number of different key parties that may be involved pose challenges for supervisory oversight.[61] Further, stablecoins themselves may be securities, commodities, or derivatives, and thus fall under the jurisdiction of either the Securities and Exchange Commission or the Commodity Futures Trading Commission.

- **Regulatory Arbitrage.** Similarly, the legal and regulatory status of cryptocurrencies varies greatly within and among countries, creating the potential for arbitrage opportunities (i.e., exploiting variations in how agencies implement regulatory responsibilities to minimize regulatory scrutiny). We previously reported that firms exploited differences in financial regulations to avoid more rigorous oversight regimes.[62] For example, some countries allow individuals to use cryptocurrencies while others have enacted absolute or implicit bans on cryptocurrencies. The Law Library of Congress reported that, as of November 2021, nine countries had an absolute ban on cryptocurrencies and 42 had an implicit ban (see fig. 9). Also, tax laws vary by country, as do anti-money laundering and anti-terrorism financing laws (see fig. 10). The same Law Library of Congress report described how 103 countries applied at least one of these laws, with the majority of countries reviewed applying both. However, a 2018 report described how just 33 countries were found to regulate cryptocurrencies in these areas, with only five applying both tax laws and laws concerning anti-money laundering and anti-terrorism financing.

[61]President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins* (Washington, D.C.: November 2021).

[62]GAO, *Financial Regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness*, GAO-16-175 (Washington, D.C.: Feb. 25, 2016).

Figure 9: Legal Status of Cryptocurrencies Worldwide

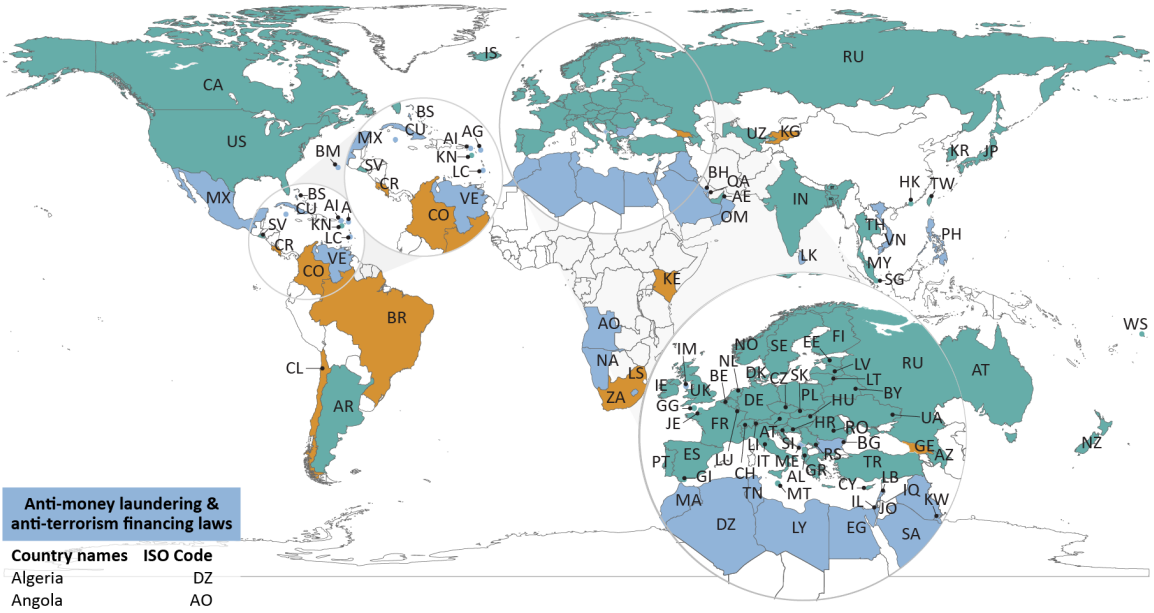


Implicit ban			
Country names	**ISO Code**	**Country names**	**ISO Code**
Bolivia	BO	Libya	LY
Bahrain	BH	Macao	MO
Benin	BJ	Maldives	MV
Burkina Faso	BF	Mali	ML
Burundi	BI	Moldova	MD
Cameroon	CM	Namibia	NA
Central African Republic	CF	Niger	NE
Chad	TD	Nigeria	NG
Congo	CG	Pakistan	PK
Côte D'Ivoire	CI	Palau	PW
Democratic Republic of Congo	CD	Saudi Arabia	SA
Ecuador	EC	Senegal	SN
Gabon	GA	Tajikistan	TJ
Georgia	GE	Tanzania	TZ
Guyana	GY	Togo	TG
Indonesia	ID	Turkey	TR
Jordan	JO	Turkmenistan	TM
Kazakhstan	KZ	United Arab Emirates	AE
Kuwait	KW	Vietnam	VN
Lebanon	LB	Zimbabwe	ZW
Lesotho	LS		

Absolute ban	
Country names	**ISO Code**
Algeria	DZ
China	CN
Egypt	EG
Iraq	IQ
Morocco	MA
Nepal	NP
Oman	OM
Tunisia	TN
Qatar	QT

Source: Law Library of Congress. | GAO-22-104625

Figure 10: Global Regulatory Framework for Cryptocurrencies



Anti-money laundering & anti-terrorism financing laws

Country names	ISO Code
Algeria	DZ
Angola	AO
Anguilla	AI
Antigua and Barbuda	AG
Bahamas	BS
Bahrain	BH
Bermuda	BM
Bulgaria	BG
Cuba	CU
Egypt	EG
Isle of Man	IM
Israel	IL
Iraq	IQ
Jordan	JO
Kuwait	KW
Lebanon	LB
Libya	LY
Mexico	MX
Montenegro	ME
Morocco	MA
Namibia	NA
Oman	OM
Philippines	PH
Qatar	QA
Saint Lucia	LC
Saudi Arabia	SA
Sri Lanka	LK
Tunisia	TN
United Arab Emirates	AE
Venezuela	VE
Vietnam	VN

Application of tax laws

Country names	ISO Code
Brazil	BR
Chile	CL
Colombia	CO
Costa Rica	CR
Georgia	GE
Kenya	KE
Kyrgyzstan	KG
Lesotho	LS
South Africa	ZA

Both

Country names	ISO Code
Albania	AL
Argentina	AR
Australia	AU
Austria	AT
Azerbaijan	AZ
Bangladesh	BD
Belarus	BY
Belgium	BE
Bhutan	BT
Canada	CA
Cayman Islands	KY
Cote D'Ivoire	CI
Croatia	HR
Cyprus	CY
Czech Republic	CZ
Denmark	DK
El Salvador	SV
Estonia	EE
Finland	FI
France	FR
Germany	DE
Gibraltar	GI
Greece	GR
Guernsey	GG
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Ireland	IE
Italy	IT
Japan	JP
Jersey	JE
Korea, Republic of	KR
Latvia	LV
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Malta	MT
Mauritius	MU
Montserrat	MS
Netherlands	NL
New Zealand	NZ
Norway	NO
Poland	PL
Portugal	PT
Romania	RO
Russian Federation	RU
Saint Kitts and Nevis	KN
Samoa	WS
Serbia	RS
Singapore	SG
Slovakia	SK
Slovenia	SI
Spain	ES
Sweden	SE
Switzerland	CH
Taiwan	TW
Thailand	TH
Turkey	TR
Ukraine	UA
United Kingdom	UK
United States	US
Uzbekistan	UZ

Source: Law Library of Congress. | GAO-22-104625

4 Policy Options

GAO developed four policy options that could help enhance benefits or mitigate challenges of blockchain technologies. The policy options identify possible actions by policymakers, which may include Congress, federal agencies, state and local governments, academic and research institutions, and industry. In addition, policymakers could choose to maintain the status quo, whereby they would not take additional action beyond any current efforts. See below for details of the policy options and relevant opportunities and considerations.

Policy Option

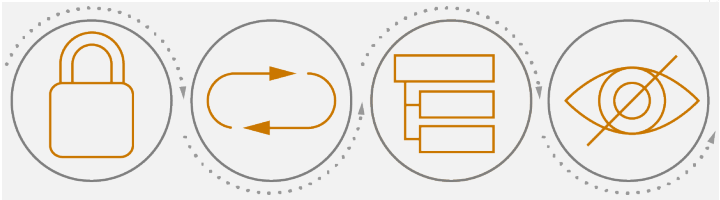
Standards

Policymakers could collaborate to unify standards that focus on the development, implementation, and use of blockchain technologies.

This policy option could help address challenges around interoperability and data security.

Source (illustration): anttoniart/stock.adobe.com.

Opportunities



- This option could simplify the wide variety of standards that at least 30 standard-setting entities are developing in the U.S. and abroad.[63] It could also help identify gaps and reduce overlap in standard-setting efforts. Policymakers could collaborate to establish clear, concise, and shared definitions for blockchain-related terms that can be used to create and update standards.
- To operationalize this option, policymakers could identify the areas in which standards would be most beneficial across different sectors of the economy or applications of blockchain. Then policymakers could develop and periodically update those standards to help ensure that they remain current and relevant.
- One expert told us that the focus of standard-setting organizations should be on increasing interoperability between existing systems and blockchain systems, as well as within the blockchain ecosystem. For example, the World Economic Forum published a framework in 2020 designed to achieve blockchain interoperability and highlighted ongoing efforts by standard-setting organizations.[64] Interoperability advancements could, in turn, enable developers to focus on strengthening a smaller number of security and privacy standards that would apply across many blockchains.

Considerations

- Could require consensus from many public- and private-sector stakeholders, which can be time- and resource-intensive. In addition, one expert stated that standards should be developed not only at the technology level but also at the application level. We previously reported that development of standards requires multiple iterations that can take anywhere from 18 months to a decade to complete.[65]
- It may not be clear which entities should take the lead in establishing internationally recognized standards for different technologies and application areas. For example, GS1, a nonprofit that creates and maintains global standards for business communication, created the Global Trade Item Number to provide firms managing global supply chains with a way to identify any item that is traded. New standards may need to come from an authoritative organization within each industry affected by blockchain.
- May require new funding or reallocation of existing resources to support new efforts.

Source: GAO (icons). | GAO-22-104625

[63]We use the term standard to refer to a document, established by consensus and approved by a recognized body, which provides—for common and repeated use—rules, guidelines, or characteristics for activities or their results aimed at optimizing order.

[64]World Economic Forum, *Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability* (Cologny, Switzerland: Apr. 9, 2020).

[65]GAO, *Health Information Technology: Approaches and Challenges to Electronically Matching Patients' Records across Providers*, GAO-19-197 (Washington, D.C.: Jan. 15, 2019).

Policy Option

Oversight

Policymakers could clarify existing oversight mechanisms, including regulations, or create new mechanisms to ensure appropriate oversight of blockchain applications.

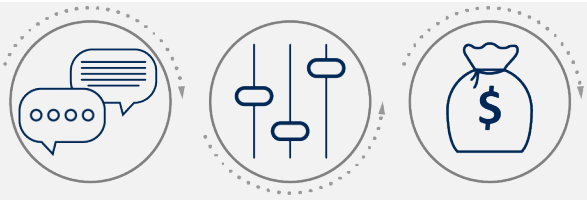
This policy option could help address challenges with legal and regulatory uncertainty and regulatory arbitrage.

Source (illustration): Vdant85/stock.adobe.com.

Opportunities

- U.S. oversight clarity could help keep U.S.-based blockchain firms from moving to other countries. Clear, industry-specific oversight frameworks could allow individuals and firms to more successfully engage in blockchain-related commerce in the U.S.
- Policymakers, including regulatory entities and developers, could use tools such as regulatory sandboxes to improve blockchain oversight.[66] For example, 11 companies participated in the state of Arizona's financial technology sandbox from October 2018 to April 2021. At the federal level, the Consumer Financial Protection Bureau has created a Compliance Assistance Sandbox for companies to obtain safe harbor for testing innovative products and services for a limited time while sharing data with the Bureau. Efforts like this could provide mechanisms for policymakers to more effectively carry out their statutory obligations by better enabling compliance in the face of regulatory uncertainty.
- Policymakers could provide coordinated and timely clarity to promote safety and soundness, consumer protection, and compliance with applicable laws and regulations to combat illicit activity in blockchain-related commerce. For example, the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) recently proposed a rule requiring banks to submit reports, keep records, and verify the identity of customers in certain cryptocurrency transactions to ensure the cryptocurrency industry appropriately addresses challenges around anti-money laundering and national security risks.[67]

Considerations



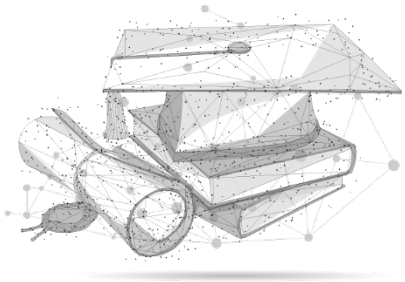
- Policymakers will need to determine the appropriate level of oversight. Aggressive oversight could hamper innovation and competition as the technology matures, whereas too little oversight could leave consumers and businesses unprotected. An expert and two interviewees told us that policymakers should focus on identifying and regulating illicit activities instead of regulating the technology.
- Soliciting input across a range of stakeholders in various sectors may be time consuming and challenging. For example, federal agencies' rulemaking processes may include lengthy internal and interagency deliberation and reviews, as well as opportunities for public comment.[68]
- May require new funding or reallocation of existing resources. One possible source, advocated by an interviewee, would be industry-specific consortia, which could fund and collaborate on developing emerging technologies, including blockchain.

Source: GAO (icons). | GAO-22-104625

[66]Regulatory sandboxes are a novel concept and vary by jurisdiction. While there is no generally accepted definition, sandbox programs define rules and requirements for eligibility and testing and may provide special authorizations, exemptions, or other relief to eligible businesses for a limited period. Office of the Comptroller of the Currency, *OCC Innovation Pilot Program* (Washington, D.C.: April 30, 2019).

[67]85 Fed. Reg. 83840 (Dec. 23, 2020) (proposed rule); 86 Fed. Reg. 3897 (Jan. 15, 2021) (extension of comment period).

[68]GAO, *Federal Rulemaking: Improvements Needed to Monitoring and Evaluation of Rules Development as Well as to the Transparency of OMB Regulatory Reviews*, GAO-09-205 (Washington, D.C.: Apr. 20, 2009).



Policy Option

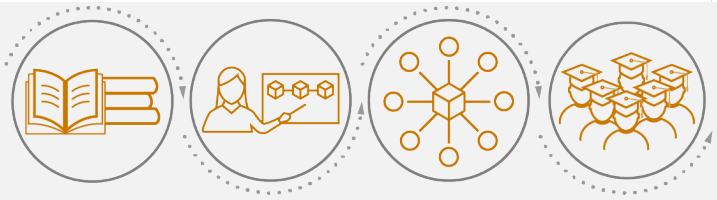
Educational materials

Policymakers could support the development of educational materials to help users and regulators better understand blockchain technologies beyond existing financial applications.

This policy option could help address challenges around limited understanding and undefined benefits and costs.

Source (illustration): Brazhyk/stock.adobe.com.

Opportunities

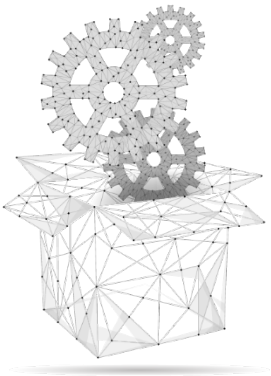


- This option could enable instructors to train a workforce to be more skilled in developing, implementing, and using blockchain-based products. Instructors could use the educational materials to develop vocational training that may help establish professional development courses and certifications in sectors affected by blockchain. It could also increase consumer literacy and help reduce negative public perceptions of blockchain.
- Could stimulate critical thinking and innovation. For example, additional education could prompt innovative research and development on blockchain applications that track and trace prescription medicines in pharmaceutical supply chains.
- Could expand beyond currently available education and training, which generally focuses on beginner-level knowledge and financial applications, according to an expert.
- Could help prepare policymakers to better use and regulate the latest technologies. For example, following the 2021 Colonial Pipeline ransomware attack, the Department of Justice brought together a group of skilled investigators, trained law enforcement and prosecutors to successfully review the cryptocurrency ledger, track multiple transfers, and seize a portion of the cryptocurrency paid to the bad actors.

Considerations

- Educational materials will likely need to be tailored to meet a wide variety of learning needs across multiple target audiences. Different groups of educators may need to coordinate with one another to ensure similar messaging across target audiences. As blockchain technology evolves, policymakers could reevaluate whether educational materials meet the learning needs of these target audiences.
- It may be difficult to identify who could most effectively create educational material for any particular target audience. One expert told us that the current education space is too focused on introductory-level concepts and needs more focus on advanced learning. As advanced educational materials are developed, policymakers could consider adopting a standardized training approach to ensure a focus on the same key skills and competencies.
- May require new funding or reallocation of existing resources to support new efforts. Two experts told us this could be especially critical for education in innovative uses of blockchain beyond existing financial applications.

Source: GAO (icons). | GAO-22-104625



Policy Option

Appropriate uses

Policymakers could support activities designed to determine whether blockchain is appropriate for achieving specific missions and goals or to mitigate specific challenges.

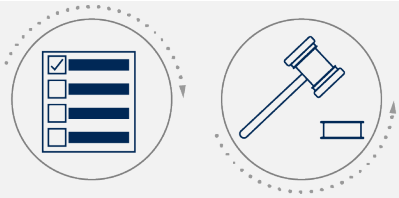
This policy option could help address challenges around risks to the financial systems and undefined benefits and costs.

Source (illustration): Елена Бутусова/Elena Butusova/stock.adobe.com.

Opportunities

- Actively investigating where and when blockchain would be the most useful could allow entities to capture the full benefits the technology might offer.
- Blockchain technologies could help modernize some existing systems and processes. We previously reported that U.S. federal agencies have struggled with appropriately planning and budgeting for modernizing legacy systems; upgrading underlying infrastructure; and investing in high-quality, low-cost service delivery technology.[69] Blockchain could be one means of improving or replacing existing systems for greater efficiency and effectiveness. Additionally, it could be part of larger data management efforts by policymakers.
- Supporting blockchain use, where appropriate, such as by conducting new pilots, identifying lessons from existing pilots, or transitioning some efforts beyond the pilot stage could enhance transparency and accountability of existing systems and services. According to one think tank report, some companies have started experimenting with blockchain-based systems to add transparency, trust, and traceability to their operations.[70] For example, as we discussed earlier in this report, blockchain has been piloted for use in coffee supply chains. Further, we also described how the federal government has piloted using blockchain across several different proof of concept efforts. These efforts were designed to evaluate the potential for blockchain to offer operational benefits and cost savings.

Considerations



- Legal or regulatory uncertainty may hinder some potential users from benefitting from blockchain. For example, currently the Commodity Futures Trading Commission (CFTC) lacks the legal authority to partner and collaborate with outside entities engaging directly with financial technology and innovation within a research and testing environment, according to the former CFTC Chairman.[71]
- It could be difficult to revert to a non-blockchain technology once an entity has invested a significant amount of time and resources.
- May require new funding or reallocation of existing resources. For example, one interviewee told us it generally was not possible to download blockchain software and begin using it immediately; rather, they found it was necessary to invest in a team of engineers to integrate it into existing systems.

Source: GAO (icons). | GAO-22-104625

[69]GAO, *Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, D.C.: Jun. 11, 2019).

[70]Information Technology and Innovation Foundation, *A Policymaker's Guide to Blockchain* (Washington, D.C.: Apr. 30, 2019).

[71]*Examining the Upcoming Agenda for the CFTC, Before the H. Comm. On Agriculture*, 115th Cong. 30-31 (Jul. 25, 2018) (statement of CFTC Chairman J. Christopher Giancarlo).

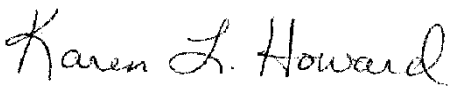
5 Agency and Expert Comments

We provided a draft of this report to the Department of Homeland Security, the Department of Justice, the Department of the Treasury's Office of Domestic Finance, the National Institute of Standards and Technology, and the Office of the Comptroller of the Currency with a request for technical comments. We incorporated agency comments into this report as appropriate.

We also provided a draft of this report to 15 participants from our expert meeting and incorporated comments as appropriate.

This report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact Karen L. Howard at (202) 512-6888 or howardk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



Karen L. Howard, PhD
Director
Science, Technology Assessment, and Analytics

Appendix I: Objectives, Scope, and Methodology

We examined (1) non-financial applications of blockchain, including potential benefits and challenges, (2) financial applications of blockchain, including potential benefits and challenges, and (3) policy options that could help enhance benefits or mitigate challenges of blockchain technologies.

To address all three research objectives, we assessed available, developing, and proposed blockchain applications as well as their benefits, drawbacks, and challenges surrounding their development and use. To do so, we reviewed key reports, peer-reviewed articles, and whitepapers describing blockchain applications; conducted an expert meeting in conjunction with the National Academies of Sciences, Engineering, and Medicine (NASEM); and interviewed a variety of stakeholders, including agency officials, industry organizations, and researchers at academic institutions.

Scope

We focused our research to include financial applications, shared data services, and smart contracts. Financial applications includes cryptocurrencies and decentralized finance (DeFi). Shared data services includes applications in supply chain management, public records, voting, and real estate. We did not assess all possible applications of blockchain technologies. For example, we excluded decentralized marketplaces. We selected eight stand-alone use cases for the vignettes to expand on the complexities of applying blockchain in specific areas. The use cases were the pharmaceutical supply chain, the coffee bean supply chain, decentralized autonomous organizations, digital ID, voting, carbon credits, real estate, and federal government use. We selected vignette topics to address requester needs or highlight applications for blockchains not presented in the main report.

Literature search

For all the objectives, using a snowball technique, we reviewed relevant literature identified by agencies, experts, stakeholders, and our literature search.[72] To gain insight into blockchain technologies' maturity, applications, potential benefits, challenges, and drawbacks, we reviewed agency documents, peer-reviewed literature, white papers, conference papers, industry articles, and other publications. We used keywords to search databases such as Institute of Electrical and Electronics Engineers (IEEE) Xplore, and Google Scholar. Additionally, a GAO research librarian conducted two literature searches to find articles regarding blockchain technology applications, challenges, and policy options. The librarian conducted searches in various databases, including Scopus, MEDLINE, Abstracts in New Technology & Engineering, and Inspec. We used search terms such as "Blockchain," "decentralized finance," "Stablecoins," "hybrid smart contracts," and "Decentralized autonomous organizations" and narrowed our search to articles published within the last 5 years. For these searches, results could originate from scholarly or peer reviewed material, government reports, conference papers, trade or industry papers,

[72]The snowball technique involves identifying new articles or reports in those a researcher has already found on the topic.

working papers, and association, nonprofit and think tank publications but not from general news. We selected the most relevant articles for further review based on our objectives and reviewed the abstracts for additional search terms to refine the results.

Expert meeting

We convened a GAO expert meeting with the assistance of NASEM to provide expert insights on using blockchain technology for financial applications, shared data services, and decentralized autonomous organizations; challenges surrounding development and adoption; and potential policy options. The meeting was held over 2 days with 15 experts. (See app. II for a list of these experts and their affiliations.) We worked with NASEM staff to identify experts from a range of stakeholder groups, including federal agencies, academia, industry, and legal scholars with expertise covering significant areas of our review. We evaluated the experts for potential conflicts of interest, which were considered to be any current financial or other interest that might conflict with the service of an individual because it could (1) impair objectivity or (2) create an unfair competitive advantage for any person or organization. The 15 experts were determined to be free of reported conflicts of interest, except those that were outside the scope of the forum or where the overall design of our meeting and methodology was sufficient to address them, and the group as a whole was determined to not have any inappropriate biases. The comments of these experts generally represented the views of the experts themselves and not the agencies, universities, or companies with which they were affiliated, and are not generalizable to the views of others in the field.

We divided the 2-day meeting into five moderated discussion sessions: (1) financial applications, (2) shared data services applications, (3) smart contracts and decentralized autonomous organizations (DAOs), (4) challenges surrounding development and adoption, and (5) policy ideas to enhance benefits or mitigate challenges. Each session featured an open discussion among all meeting participants based on key questions we provided. The meeting was transcribed to ensure that we accurately captured the experts' statements. After the meeting, we reviewed the transcripts to characterize their responses and to inform our understanding of all three researchable objectives. Consistent with our quality assurance framework, we provided the 15 experts with a draft of our report and solicited their feedback, which we incorporated as appropriate.

Interviews

We interviewed key stakeholders in the field of blockchain technologies, including:

- Nine relevant federal agencies: the Congressional Research Service; the Department of Homeland Security; the National Institute of Standards and Technology; the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives Criminal Division, Drug Enforcement Administration, and Federal Bureau of Investigation; the Department of the Treasury's Office of Domestic Finance and Office of the Comptroller of the Currency
- Two state agencies
- Four academic researchers or institutions

- Two standards-setting groups
- Four industry organizations
- Three blockchain investment firms
- One blockchain venture capital firm
- Eight blockchain application developers
- Three consumer goods corporations
- One consulting firm

Because this is a small and non-generalizable sample of the stakeholders involved in researching and using blockchain technologies, the results of our interviews are illustrative and represent important perspectives, but are not generalizable.

Policy options

We intend policy options to provide policymakers with a broader base of information for decision-making.[73] The options are neither recommendations to federal agencies nor matters for congressional consideration. They are also not listed in any specific rank or order. We are not suggesting that they be done individually or combined in any particular fashion. Additionally, we did not conduct work to assess how effective the options may be, and express no view regarding the extent to which legal changes would be needed to implement them.

We developed four policy options to enhance the benefits or mitigate the challenges of blockchain technologies. To develop the policy options, we identified 132 policy ideas based on our literature review, expert meeting, and interviews with federal agencies, selected state agencies, academic researchers, blockchain organizations, industry groups, and other stakeholders. We generated policy options by grouping policy ideas by themes that addressed the objective and fit the scope of our work.

We conducted our work from November 2020 to March 2022 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

[73]Policymakers is a broad term including, for example, Congress, federal agencies, state and local governments, academic and research institutions, and industry.

Appendix II: Expert Participation

We collaborated with the National Academies of Sciences, Engineering, and Medicine to convene a two-day meeting of experts to inform our work on blockchain technology; the meeting was held virtually on July 14–15, 2021. The experts who participated in this meeting are listed below. Many of these experts gave us additional assistance throughout our work, including 5 who reviewed our draft report for accuracy and provided technical comment.

Kyle Burgess

Specialist Leader

Deloitte

Quinn DuPont

Founder and CEO

Alumni Labs

Tonya Evans

Professor

Penn State Dickinson Law

Penn State Institute for Computational and Data Sciences Co-Hire

Mark D. Fisk

IBM Consulting – Federal

Partner - Data and Technology Transformation Services

Stefan Gstettner

Partner and Director

Boston Consulting Group

Emin Gun Sirer

Associate Professor and Co-Director, Initiative for Cryptocurrencies and Smart Contracts

Cornell University

Stuart Levi

Partner, Blockchains and Digital Assets; Intellectual Property and Technology; Outsourcing; Cybersecurity and Privacy

Skadden

Anil John

Technical Director, Silicon Valley Innovation Program

Department of Homeland Security

Caroline Malcolm

Head, Global Blockchain Policy Centre

Organisation for Economic Co-operation and Development

Pramita Mitra

Research Supervisor, IoT and Blockchain Applications

Ford Motor Company

Dawn Song

Professor, Computer Science

University of California, Berkeley

Mark Treshock

Global Blockchain Solutions Leader, Healthcare and Life Sciences

IBM

Sheila Warren

Chief Executive Officer

Crypto Council for Innovation

Aaron Wright

Associate Clinical Professor of Law

Benjamin N. Cardozo School of Law, Yeshiva University

Frank Yiannas

Deputy Commissioner for Food Policy and Response

Food and Drug Administration

Appendix III: Selected Definitions

- **Best practices**. Processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas.
- **Consensus protocol**. The steps a blockchain takes to ensure verified blocks are added to the blockchain and unverified blocks are ignored. It is the way in which at least a majority of blockchain network members agree on the information of a proposed transaction, which is then updated to the ledger.
- **Cryptocurrencies**. Digital assets, credits, or units that are built on technologies like blockchain. Users can secure and authenticate cryptocurrency transactions using cryptographic techniques on the blockchain. Blockchain protocols can generate cryptocurrencies.
- **Immutable**. Immutable is the property of not being subject to change. In the context of data, it refers to data that can only be written, not modified or deleted.
- **Node**. Blockchain nodes consist of individuals systems—computers or servers—in the peer-to-peer blockchain network that are operated by a single person, group, business, or organization.
- **Oracles.** Oracles are external sources including people, devices, or software that add information to a blockchain, such as freight shippers in a product supply chain. Decentralized protocols may rely on oracles to access off-chain information, such as crypto-asset exchange rates, in order to process transactions on the blockchain.
- **Regulatory sandbox.** Regulatory sandboxes are a safe space for novel products or services and define rules and requirements for eligibility and testing and may provide special authorizations, exemptions, or other relief to eligible businesses for a limited period.
- **Smart contracts**. Software code stored on a blockchain that contains a set of conditions, so that transactions automatically trigger when the conditions are met.
- **Stablecoins**. Cryptocurrencies designed to maintain a stable value compared to other types of cryptocurrency by maintaining reserve assets that could include fiat currencies, corporate and municipal bonds, cryptocurrencies, or other digital assets.
- **Standards**. A document, established by consensus and approved by a recognized body, which provides—for common and repeated use—rules, guidelines, or characteristics for activities or their results aimed at optimizing order.
- **Tokens**. Tokens are digital assets on the blockchain. The process of adding new digital assets to a blockchain is called tokenization.
- **Virtual currencies**. Digital representations of value, usually other than a government-issued legal tender (e.g., U.S. dollars), that function as a unit of account, a store of value, or a medium of exchange. Cryptocurrencies are a type of digital currency.

Appendix IV: Consensus Protocols

Consensus protocols are the steps a blockchain takes to ensure verified blocks are added to the blockchain and unverified blocks are ignored. Table 1 shows a selection of consensus protocols, how they operate, and considerations for each consensus protocol. The choice of protocol depends on whether it is for a permissionless or permissioned blockchain and the level of trust between participants.

Table 1: Examples of consensus protocols for blockchains and corresponding considerations

Protocol	Operation	Considerations
Proof of work	The nodes that want to publish a block attempt to solve a puzzle that requires computational resources. The puzzle is difficult to solve, but the solution is easy for any node to verify.	This consensus protocol is energy intensive. If only a few users control most of the computational resources, then the security of the blockchain is threatened. The transaction speed is slow because participants have to wait for a node to solve the puzzle. Some public blockchains and cryptocurrencies use this protocol.
Proof of stake	Nodes publish in proportion to how much cryptocurrency or tokens they have invested or staked in the blockchain. Staked cryptocurrency and tokens are invested in the blockchain and cannot be spent.	The proof-of-stake protocol is more energy efficient than proof of work and designed for public blockchains. Users who possess a lot of tokens or cryptocurrency are able to more easily stake assets and publish blocks. Some public blockchains and cryptocurrencies use this protocol.
Proof of authority/proof of identity	The publishing node provides information about the user's identity, which is proven and verified by the blockchain. The chance of being selected by users to publish a block depends on the reputation of the publishing node.	The proof of authority protocol works with permissioned blockchains with high levels of trust. Use cases where the identity of all nodes are known such as private consortiums could consider this protocol.
Proof of elapsed time (PoET)	To select publishing nodes at random all publishing nodes are given a random wait time from a secure hardware time source within their computer system. After waiting, a node can publish a block and the process starts over.	The PoET protocol requires a random wait time and a way to verify that the full wait time elapsed before a new block is published to the blockchain. This protocol works best with permissioned networks. Use cases where there is a high level of trust between the nodes could consider this protocol.

Source: GAO analysis of NIST publications and other publications. | GAO-22-104625

Appendix V: GAO Contacts and Staff Acknowledgments

GAO contacts

Karen L. Howard, (202) 512-6888 or howardk@gao.gov

Staff acknowledgments

In addition to the contact named above, Laura Holliday (Assistant Director), Jon D. Menaster (Analyst-in-Charge), Angelica Aboulhosn, Nora Adkins, Jacob Beier, Christina Bixby, Brian Bothwell, Claire McLellan, Anika McMillon, Matthew Metz, Ben Shouse, Courtney Thacker, and Wesley Wilhelm made key contributions to this report.

(104625)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact: Website: https://www.gao.gov/fraudnet/fraudnet.htm
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, YoungC1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

Stephen Sanford, Managing Director, spel@gao.gov, (202) 512-9715
U.S. Government Accountability Office, 441 G Street NW, Room 7B37N, Washington, DC 20548