Congressional Research Service
Informing the legislative debate since 1914

Blockchain: Background and Policy Issues

Chris Jaikaran
Analyst in Cybersecurity Policy

February 28, 2018

Congressional Research Service
7-5700
www.crs.gov
R45116

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The rise of cryptocurrencies like Bitcoin and the use of Initial Coin Offerings to raise capital has drawn increased attention from both the public and private sector concerning the use of digital ledgers to conduct business (called blockchain technology) and its potential. Yet many remain unclear on what the technology actually is, what it does, and the tradeoffs for its use.

A blockchain is a digital ledger that allows parties to transact without the use of a central authority as a trusted intermediary. In this ledger, transactions are grouped together in blocks, which are cryptographically chained together in a way that is tamper-proof and creates a mathematically indisputable history.

Blockchain is not a new technology; rather it is an innovative way of using existing technologies. The technologies underpinning blockchain are asymmetric key encryption, hash values, Merkle trees, and peer-to-peer networks. Blockchain allows parties who may not trust each other to agree on the current distribution of assets and who has those assets, so that they may conduct new business. But, while there has been a great deal of hype concerning blockchain's benefits, it also has certain pitfalls that may inhibit its utility.

With blockchain, as transactions are added, the identities of the parties conducting those transactions are verified, and the transactions themselves are verifiable by other users. The strong relationship between identities, transactions, and the ledger enables parties that may not trust each other or an individual computing platform to agree on the state of resources as logged in the ledger. With that agreement, they may conduct a new transaction with a common understanding of who has which resource and their ability to trade that resource.

Blockchain is not a panacea technology. A blockchain records events as transactions when they happen, in the order they happen, and in an add-on only manner. Previous data on the blockchain cannot be altered, and users of the blockchain have access to the data on the blockchain in order to validate the distribution of resources. Though there are benefits to blockchain, there are also pitfalls and unsolved conditions which may inhibit blockchain use. Some of those concerns are data portability, ill-defined requirements, key security, user collusion, and user safety. As with adopting any technology, users must examine the business, legal, and technical aspects of that technology.

Blockchain is currently being tested by industry, but at this time does not appear to be a complete replacement for existing systems. Although the adoption of blockchain is in its early stages, Congress may have a role to play in several areas, including the oversight of federal agencies seeking to use blockchain for government business, and exploration of whether regulations are necessary to govern blockchain's use in the private sector.

Some federal agencies are seeking to better manage identities, assets, data, and contracts through the adoption of blockchain technology. In addition, some federal agencies are issuing guidance on industry use of blockchain, and whether or not the current legal framework governs blockchain use.

Contents

Contacts

Introduction

Blockchain has garnered attention as a novel technology with potential to improve how we conduct business. Initially popularized by Bitcoin and other cryptocurrency uses, companies are seeking novel ways of applying the technology. But despite public intrigue and excitement around the technology, questions still surround what it is, what it does, how it can be used, and its tradeoffs.

This report explains the technologies which underpin blockchain, how blockchain works, potential applications for blockchain, concerns with it, and potential considerations for Congress.

Blockchain is not a new technology; rather it is an innovative way of using existing technologies. It enables parties who may not have reason to trust each other to agree on the current distribution of assets and who has those assets, so that they may conduct new business. But, despite the hype surrounding the technology, it has certain pitfalls which can inhibit its utility.

A blockchain is a digital ledger that allows parties to transact without the use of a central authority to validate those transactions. These transactions are not limited to financial ones, but may include item tracking, identity logging, verifying the completion of an action, or others. The use of a central, validating authority (i.e., a third party) can be avoided because in a blockchain, as transactions are added, the identities of the parties conducting those transactions are verified, and the transactions are verified as they are added to the ledger as a block of transactions. The ledger is auditable because each block of transactions is dependent upon the previous block in such a way that any change would alert other users of a change to the history of transactions. The strong relationships between identities, transactions, and the ledger enable parties to verify with a high degree of confidence the state of resources as logged in the ledger. With an agreement on that history, parties may then conduct a new transaction with a shared understanding of who has which resource and of their ability to trade that resource.

Underlying Technology

Blockchain is not a new, stand-alone technology; rather it is an innovative use of existing technologies. Four particular technologies are used to enable blockchain: asymmetric key encryption; hashes; Merkle trees; and peer-to-peer networks.

Asymmetric Key Encryption

Asymmetric key encryption, also known as a public-private key cryptosystem, serves to create identities on a blockchain. A user creates two elements, a public key which helps identify their transactions on the blockchain, and a private key which is necessary to conduct a transaction with the public key. Asymmetric encryption allows for the authentication of users because only those with the private key can decrypt data encrypted with the public key or encrypt the data for public key decryption, thereby creating a signature.[1]

The public key may be broadcast on the blockchain itself, or may be tied to an address which is broadcast instead. In some blockchain systems, the real-world identity of each address or public key is logged so that individual users may be tracked. In others, a user may be able to generate

[1] For more information on encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran.

public and private keys independently and broadcast the public key or address without identifying themselves, creating a pseudonymous identity on the blockchain.

In a blockchain, the public key is used to identify a user on the blockchain and verify the resources (e.g., assets or records) tied to that user's public key or address. The resource could not be used unless the holder of the public key to which the resource is tied unlocks (or decrypts) the resource with their private key, allowing it to be transferred to another identity on the blockchain (a public key or address) and locked with that second user's private key. This transaction would be logged on the blockchain, so that other users could verify the resource has changed possession.

An example of how asymmetric key encryption is used daily is when a user connects to a website via Hypertext Transfer Protocol-Secure (HTTPS). To enable the secure connection to the website, a user starts the process by sending a request to the site. The site then sends its public key to the user, and the user's computer then generates a new, secure key (to be used in the HTTPS connection), encrypts it with the website's public key, and sends that back. The user knows that only the website that has the private key can decrypt the information the user just sent. With the new, user-generated key, the website creates the secure connection with the user, indicated to the user by the HTTPS icon (frequently a lock symbol) in the browser window.

Hash Values

A hash uses similar mathematical functions as an encryption method to produce a string of characters as an output given some data as input. This is a one-way function, meaning a hash value may be created from an input, but the input cannot be recreated from the hash. In blockchains, a number of transactions are tranched together to make a single block, which is then hashed.

Hash values are used to validate the block's integrity. Any alterations to the transactions that make up a block will change the hash value of the block as a whole. If a block's hash value stays the same over time, users can have a high degree of confidence that the transactions in that block have not been tampered with. This allows users on the blockchain to determine whether or not they can trust the history of transactions on the blockchain.

Merkle Trees

Databases and ledgers are large and are constantly being edited as new entries are added and data is modified or deleted. If one wanted to have a hash value for the database, one would have to constantly hash it, and maintain a way of ensuring they have the right hash value to align with the current state of the system in order to judge its integrity. Additionally, the larger the database becomes, the more computationally intensive hashing it becomes. A Merkle tree is a cryptographic concept introduced by Ralph Merkle in 1980 as a way around this problem.[2]

In a Merkle tree, data is segmented apart from a single whole data file. There is a root block of data with a hash value, then subsequent blocks of data (sometimes referred to as child, branch, or leaf blocks) that have their own hash value. Each subsequent block of data takes the hash value of their previous block (sometimes referred to as a parent block) as an input in the creation of the hash value of the new block. This creates a chain or tree of hash values, cryptographically tying new blocks of data to previous ones in a way that prohibits altering previous data. If data in a

[2] Ralph C. Merkle, "Protocols for Public Key Cryptosystems," conference paper, Oakland, CA, April 1980, at http://www.merkle.com/papers/Protocols.pdf.

previous block were to be added, modified, or deleted, the hash value of the subsequent blocks of data would not compute to what they would need to be, alerting users that a change was made. This also allows hash values to be created for smaller, more discrete blocks of data. Hashing these smaller blocks is computationally less resource intensive than rehashing an entire set of data each time an edit is made.

Blockchains borrow the concept of Merkle trees to make hash chains. In a blockchain, a first block is created and a hash value is computed for it. This is the root block. Subsequent blocks then use the hash value of the previous block in the chain as one of the inputs to create that next block. This chaining of hash values creates a strong relationship between blocks on the chain, and an auditable and immutable record of the transactions on the blockchain.

Peer-to-Peer Networks

A peer-to-peer (P2P) network allows a disparate system of computers to connect directly with each other without the reference, instruction, or routing of a central authority. P2P networks allow for the sharing of files, computational resources, and network bandwidth among those in the network.

In a blockchain, a P2P network allows the users of the blockchain to broadcast directly to and among each other the current state of the blockchain (so that users may agree on the history of transactions), and when a new block is added. This also allows for redundancy of the data in the blockchain, as any user may download a complete copy of the current ledger of transactions and add a new block, so that there will not be a single point of failure for the blockchain if a node on the network goes down.

In some blockchain implementations, users do not host copies of the ledger among themselves. Instead, users use a cloud service provider (CSP) to maintain active and back-up copies of the blockchain, and compute the transactions and blocks as they happen. In these cases, peer-to-peer networking is necessary to run the blockchain. While the CSP is not a central validating authority in this example, it does become a third party to the transaction.

Blockchain in Use

Blockchain uses asymmetric encryption, hash values, Merkle trees, and P2P networks to build a ledger. The transactions captured in that ledger are not limited to financial ones (e.g., trading currency for goods and services). Those participating on a blockchain have a common understanding of how transactions are added and build upon one another, who can participate on the network, and how conflicts are resolved.

Transactions in a Blockchain

Blockchains consist of a series of blocks of transactions. A transaction is an event in which a resource or asset changes possession from one party to another. These individual transactions are signed by the users engaging in those transactions through the use of public-private key encryption. Because the private key is necessary to release and accept a resource in a transaction on the blockchain, the users transacting on the blockchain are, in effect, signing the transaction to ensure its security. Transactions are grouped together and made into a block. In some blockchain implementations, these are validated upon its creation through the act of *mining* for the creation of blocks (mining is further explained below). The integrity of the entire ledger is ensured by

each block having a hash value which is dependent on the previous block's own hash value. Each of these three steps relies on strong cryptography which ensures the ledger's validity.

Transactions may not post immediately to a blockchain. If a lot of transactions are occurring in a short amount of time, the blockchain platform may create a pool of pending transactions which are processed in accordance with rules of that blockchain—which may allow for fees, user priority, or some other method to post certain transactions into a block before others.

Blockchain Governance

A blockchain can be public or private. In a *public* blockchain, anyone can create a public-private key pair and download a copy of the blockchain. This is usually accomplished through a software package which governs transactions on the blockchain. In a *private* blockchain, the membership of users on the blockchain is controlled. In private blockchains, the users authorized to participate may be bound by contractual relationships with each other, their blockchain addresses may be closely tied to their real-world identities, or participation on that blockchain may be agreed upon by other members in the blockchain. In any case, members of a private blockchain may be more trusting of each other than in a public blockchain.

A blockchain can be permissioned or permissionless, which is independent of whether the blockchain is public or private. A *permissioned* blockchain is one in which the permission of a user is assigned to them. Some users may only be able to view a whole or portion of the blockchain; others may be able to add new blocks. In this system, the administrator(s) do not serve as a central authority, since they do not govern the creation of blocks on the blockchain, just the rights of users on the blockchain. In a *permissionless* blockchain, all users have equal rights, with any one able to download the full blockchain and have an opportunity to potentially add additional blocks.

Discussing a blockchain as public or private refers to the level of freedom users have to create identities on that blockchain. Discussing a blockchain as permissioned or permissionless refers to the level of access the user would have on that blockchain. Users on the blockchain must reach *consensus* on the rules for creating and publishing new blocks and resolving disagreements.

Blockchains have users and nodes on the blockchain platform. The *users* on a blockchain could be the individuals, businesses, or other identities which have a public-private key pair and conduct transactions. A *node* is a computing system on that blockchain. A user may have a node (e.g., an individual's computer or a business's computing network), or a group of users could pool resources to create a single node (e.g., users who share their computing power to mine for new blocks on the blockchain). In a blockchain platform that uses a CSP, the CSP is a node on the blockchain, but may also be a user.

The creation and publication of a new block in the blockchain is called *mining*. In mining blocks, users seek to add the next block to the chain. Mining is incentivized by improving the user's standing in that blockchain, through either a monetary, reputational, or stake award for adding new blocks. New blocks may be added to a blockchain through a variety of methods. Three such methods are proof of work, proof of stake, and round robin.

In a *proof of work* scheme, those seeking to add a block to the blockchain are presented a difficult computational problem. By solving the problem, they win the opportunity to post the next block and possibly a reward for doing so. Their solution is broadcast to others users who can validate it immediately without going through the same resource intensive computation required to solve the problem. In this scheme, the problem is frequently a direction that the hash value contains certain elements (e.g., the value begins with four zeros). In order to produce a hash value with those

elements, additional information is added as an input (along with the previous block's hash value, the transactions in the block, data and time information, etc.). This additional information is called a nonce, and could be as simple as a number which would alter the hash value. Finding the nonce value that solves the problem wins for that miner the right to publish the next block.

In a *proof of stake* scheme, the next block may be awarded to the user who has an appropriate stake in that block. This may be because the block contains transactions regarding that user. Or, the user has an X percentage of stake in that blockchain, so they are awarded the right to publish X percent of blocks to that blockchain. Proof of stake schemes are computationally less resource intensive than proof of work. In the *round robin* scheme, users on the network take turns adding new blocks. Because some level of trust is necessary for round robin schemes to work, they are used in permissioned blockchains.

If there is a disagreement in the blockchain, most users on the node will consider the longest chain on the block to be the valid ledger and use that one as the basis for future transactions. In the event that two different miners publish blocks at the same time, and those blocks contain different information, blockchains may allow both blocks to be published for that round, then allow the system to resolve itself upon the publication of the next block, which would then create the largest chain of transactions, and therefore, the most trusted ledger. Another way of resolving disagreements is through using byzantine fault tolerance, whereby users on the blockchain platform will vote on which block they choose to accept and the plurality of votes determines the next block to be published.[3]

Applications

Blockchain is not a panacea technology. A blockchain records events as transactions when they happen, in the order they happen, in an add-on only manner. Previous data on the blockchain cannot be altered, and users of the blockchain have access to the data on the blockchain in order to validate the distribution of resources. However, if an entity has critical data that it wants to share (e,g,, sensitive corporate information from one facility to another), then a combination of current database, cloud, and identity management technologies will likely be adequate for its needs. But if the entity seeks to have its data be immutable and auditable, then a blockchain may be appropriate. While an entity may find immutable and auditable transactions enticing, the inability to edit those transactions (even in cases of error, when an additional invalidating transaction will be necessary) may make blockchain a suboptimal record keeping technology. Examples of blockchain uses that are in use, are being piloted, or have been discussed are listed below, in alphabetical order.

Cryptocurrencies

Bitcoin is the most popular cryptocurrency, garnering the largest market share, and arguably initiated the interest in blockchain technology. Cryptocurrencies, like Bitcoin, are built to allow the exchange of some digital asset of value (the cryptocurrency) for a good or service.[4] They are frequently permissionless and use a proof of work model to add blocks. In these systems, anyone can create a *wallet* which includes their private key, their public key, and an address which is

[3] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3 (July 1982).

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," paper, October 2008, at https://bitcoin.org/bitcoin.pdf.

derived from their public key. They then acquire (through mining, or purchase) the cryptocurrency, and add that as a transaction to the blockchain, so that their address is linked to their value. If they purchase something, they will then unlock the cryptocurrency with their private key, transfer it to the seller who then locks it with their private key. This transaction is published to the blockchain so all users are able to validate that the buying user has that much less of the cryptocurrency and the selling user has that much more of it. Bitcoin and other cryptocurrencies each have their own blockchain.

Cybersecurity

Because of its popularity and the digital nature of blockchain, it has been suggested as a solution to cybersecurity challenges. However, proposed uses of blockchain to solve cybersecurity challenges have relied less on the combination of blockchain's underlying technologies. Rather, specific technologies that enable blockchain can be applied today to solve cybersecurity challenges. Asymmetric encryption can be used to enable identities, whether for users or devices, to increase confidence in trusted communications. Hash values can be used to improve confidence in the integrity of data. Indeed, Merkle trees were first proposed as a data integrity check for large data sets. Another area where blockchain has been proposed is for cyber supply chain risk management—the use of blockchain to ensure the integrity of hardware and software as it moves from development to end-user. This application is an example of blockchain's applicability for provenance and supply-chain management, both described further below.

Healthcare

There have been a variety of proposals for using blockchain in the healthcare sector, many of which involve the management of patient information maintained in electronic health records (EHRs). One such proposal is to authenticate patients and health providers on a blockchain in order to enable the sharing of electronic health information.[5] In this proposal, the EHR is held on a system hosted by the provider, but the record's existence is published to the blockchain and the patient may use the blockchain to authorize access to that record. However, applications of blockchain for healthcare implicate both federal laws (i.e., the Health Insurance Portability and Accountability Act of 1996, HIPAA, P.L. 104-191, and the Health Information Technology for Economic and Clinical Health Act, HITECH, Title XIII of Division A of P.L. 111-5) and state health record privacy laws, which may inhibit its use.

Identity Management

Some have argued that blockchain technology could be used in identity management because its use of asymmetric encryption and immutable transactions provides for a secure computing environment for the authentication of identities. In this use, a user has a private key to validate transactions made with their public key, which are then published (or data about the transaction are published) to the blockchain. This is designed to ensure that only the user with the private key is able to conduct transactions and to resolve the double-spend problem because the transaction is published so other users can validate the distribution of resources to that public key or address.[6]

[5] Ariel Ekblaw, Asaph Azaria, John Halamka, and Andrew Lippman, "A Case Study for Blockchain in Healthcare: 'MedRec' Prototype for Electronic Health Records and Medical Research Data," paper, August 2016, at https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf.

[6] The double spend problem refers to transactions which may not immediately post, allowing a party to spend that resource many times before it is reflected in ledgers. For more information see David Mills et al., "Distributed Ledger (continued...)

However, this form of identity management requires both a computing device and an Internet connection to work. Private entities may be able to require users to maintain a compatible device for their blockchains and the Internet connection required to execute a transaction on the blockchain, but other entities (like the public sector) may face difficulty in moving to a blockchain-only identity management model because some of their customers may lack the computing elements necessary to conduct the transaction—creating a cost-sharing problem.

Provenance

Because asymmetric encryption allows for the authentication of users, blockchain has been suggested as a solution to the provenance of items. Provenance refers to the ability to know the history of an item; so that users can be assured that they may be legitimate consumers of the item. By using blockchain, proponents seek to enable the transfer of property, rights, or goods without the clearance of a third-party intermediary, thereby reducing costs. In this model, a user would publish to the blockchain that they have the right to an asset—the user's claim to that right would still need to be verified, which may be governed by the rules of the blockchain—and others may purchase or license that asset, which would then be published to the blockchain for other users to verify.

There are examples of using blockchain for both physical and digital item provenance. Cook County, IL, has investigated using blockchain to track the transfer of land.[7] In its pilot, it sought to track the conveyance of real property on a blockchain. This could have the potential to affect the titling industry as anyone could verify that a seller is legally in possession of the property they seek to sell and are in a position to conduct a valid sale. For digital items, Kodak has announced that it will endorse blockchain technology to track the rights of digital images and provide a way for content users to pay for the license to use an image. However, implementation concerns have generated significant criticism of Kodak's plans among industry analysts.[8]

Smart Contracts

Blockchain's digital nature has led to it being associated with smart contracts. A contract in the physical world is an agreement among parties that, upon execution of certain conditions, a transfer of assets will occur. A smart contact codifies these attributes in code, so that machines can validate that conditions are met, and initiate the transfer of assets. In addition to the parties engaging in the transaction, other users of the blockchain platform may provide computational resources necessary to process or validate the contractual transaction, thereby gaining a stake in the transaction or contributing to the verification of the transaction on the ledger.

For example, Ethereum (an open-source, public, blockchain-enabled computing platform) allows users to build smart contracts. In Ethereum, users build their smart contract and pay fees so that other users contribute computational resources to enable the smart contracts and validate the transactions.

(...continued)

Technology in Payments, Clearing, and Settlement," *The Federal Reserve Board*, 2016, at https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

[7] John Mirkovic, "Blockchain Pilot Program Final Report," report, May 30, 2017, at http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf.

[8] Kevin Roose, "Kodak's Dubious Cryptocurrency Gamble," *New York Times*, January 30, 2018, at https://www.nytimes.com/2018/01/30/technology/kodak-blockchain-bitcoin.html.

Supply Chain Management

Supply chain management of physical and digital goods on blockchain is similar to the smart contract application. In this application, goods are tagged with a digital value (e.g., a scannable code for physical goods, or a tracker for digital goods) and as it passes from one entity to the next, that entity accepts it and then transfers it to another using its public-private key. These transactions are added to the blockchain to enable participants to track the disposition of the good from creation through distribution, to retail, and potentially to the end user.[9] However, this system only indicates which party had control of the real-world item at which point. As the item itself does not contain traceable code, it must be affixed with a tracker, such as a scannable code or a sensor which enables its tracking. Someone in this chain may still manipulate the item, alter trackers, or otherwise adulterate items in the supply chain which may not be logged on the blockchain.

An example of supply chain management on a blockchain platform is tracking of minerals from the Democratic Republic of the Congo that will be used to build batteries.[10] As in this example, blockchain can only provide assurance of a product's purported disposition in the supply chain (such as acceptance by a ship's captain of the good on their vessel). The blockchain does not address other supply chain issues, such as the security and stability of the operation, or nefarious actors who may tamper with the trackers or goods themselves.

Concerns

Blockchain's cryptographic attributes may present a compelling reason for its use over other technologies. But there are pitfalls and unsolved challenges which may inhibit its wide use. Some of these concerns are discussed below.

Data Portability

As with other record keeping systems, once data is logged in one system, transferring that data to a new system may be problematic. This issue impacts many blockchain applications. Once a user chooses to use one blockchain, they are unable to remove their previous records of transactions and transfer them to a new system as those transactions are part of the blockchain and any alteration to the chain would result in users being unable to generate legitimate hash values for new blocks. The existence of that data is permanent on the blockchain. Additionally, if a user seeks to copy their data from one blockchain to another, there are no standards for data construction from one blockchain to the next, so all the elements of data from one blockchain may not be imbedded in another, nor will how they process public-private keys or hash values. The lack of standards in blockchain technologies extends beyond how data is stored to how public-private keys are generated, how hash values are generated, and how data is broadcast across peers. The lack of standards effectively means that once a user chooses one blockchain for their use, they may be unable to transfer to another blockchain. While they may be able to recreate their current allotment of resources on a new chain and conduct transactions from that point, their history will be encapsulated on the previous chain.

[9] For more information in supply chain issues and blockchain, see CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

[10] Barbara Lewis, "Blockchain to Track Congo's Cobalt from Mine to Mobile," *Reuters*, February 2, 2018, at https://www.reuters.com/article/us-mining-blockchain-cobalt/blockchain-to-track-congos-cobalt-from-mine-to-mobile-idUSKBN1FM0Y2.

Ill-Defined Requirements

As with adopting any technology, adopters must examine the business, legal, and technical aspects of adopting blockchain.[11] Because blockchain is in the early stages of its development and adoption, users are likely to face a set of questions that do not have clear answers. What is the *business* case for the technology? Do customers demand attributes that the new technology provides? Will employees benefit from the use of the technology? What are the *legal* implications for using the new technology? Will adhering to compliance regimes be easier or more difficult? Will data held in the new technology be accessible to auditors for review? Will it inhibit regulated transparency? Finally, what particular *technology* will be adopted? What are the attributes to that technology (e.g., using one hashing algorithm instead of another)? How will it affect current business or management practices, and how might it adapt over time?

Key Security

As with other forms of encryption, the creation, storage, and loss of control of the private key creates problems. If a user were to have the device that stores their private key compromised, an attacker would have access to their private key and be able to transfer resources from their public key to another public key or address controlled by the attacker. If the user's hard drive fails, or they forget or otherwise lose their private key, they effectively lock the resource tied to their public key forever, inhibiting any other transaction with that asset.

User Collusion and Control

Groups of users on the blockchain may combine computing resources and collude to mine blocks. In some blockchain implementations this is allowed and encouraged. However, it does present a situation where groups of users may wield unintended influence over which transactions make it into a block, and the blocks that are posted. Additionally, a user, or group of users (the attacker) with sufficient computational power may be able to recreate the blockchain, thereby altering previous transactions and broadcasting to blockchain users that the attacker's chain is valid. As it would be the longest chain, other users may automatically accept it, even though it was illegitimate. This is called the 51% attack. While it is computationally difficult to carry out against established blockchains, it may allow an opportunity for nefarious users to corrupt a new blockchain platform, which has a shorter ledger, thereby ensconcing the attackers as controllers of block creation.

User Savviness and Safety

Another issue that affects other technologies, and one that applies to blockchain, is the level of comfort and knowledge a user must have with the technology in order to properly and safely use it. For instance, many drivers do not know how a car works but can still safely drive a car. Or, many users do not know how computers and networking work, but can still type out and send an email. Safe and efficient lay-user participation is possible because certain design and implementation decisions were made by government (e.g., seatbelt requirements and the need for a driver's license) and engineers (e.g., simple user interfaces) that enable users to use those technologies. As blockchain technology is developed, adopted, and used, similar design

[11] Manu Sporny, "DHS Blockchain/Distributed Ledger Conference," October 10, 2017.

requirements or standards may be necessary to ensure proper use and safe adoption of the technology.

As with any new technology, users may also need to be aware of its pitfalls and tradeoffs before adopting it. For instance, stories have circulated that users who own Bitcoin have lost access to their private keys, thereby prohibiting the use of that asset in the future—they effectively lost the asset and, without a central authority, have no recourse to restore that asset.

Potential Considerations for Congress

Although blockchain is already being used to execute financial transactions, it is relatively nascent in other sectors of the economy. Because of its novelty, blockchain is being piloted by industry, but at this time does not appear to be a replacement for existing systems. Given these conditions, the technology does not contain the same level of adoption that previous technology had when facing potential legislative action. However, in addition to examining legislative options concerning the technology's use, Congress may, if it chooses to do so, provide oversight of federal agencies seeking to (1) use it for government business, and/or (2) regulate its use in the private sector.

For example, the General Services Administration and the Department of Homeland Security are examining blockchain as a way to achieve efficiencies in the current business of government.[12] They are seeking ways to better manage identities, assets, data, and contracts.

Additionally, federal agencies are creating test beds for blockchain technology. The National Institute of Standards and Technology (NIST) has established a "workbench" to test blockchain.[13] The workbench is a virtual environment within NIST that is being used as a platform for research and testing. Test beds like this one can serve as a model or shared service for other federal agencies to examine blockchain applications and uses, providing those agencies first-hand experience with the technology as well as information concerning its limitations. This experience can better inform program managers so that they can determine if they seek to use the technology and it can also help them in their interactions with the private sector concerning the technology.

Agencies such as the Securities and Exchange Commission and the Commodities Futures Trading Commission are issuing advisories to industry concerning blockchain technology. In some cases, these actions are to positively declare that the current legal framework governing other transactions also apply to transactions on a blockchain.[14]

In these areas, Congress may evaluate whether agencies are achieving Congress's policy goals. These goals may be technology agnostic and thus already established, or Congress may develop new policy goals for the adoption of emerging technology across a variety of sectors.

Another potential issue of congressional interest is where the concentration of federal authority over blockchain expertise, research, and authority should reside. Issues such as this typically arise

[12] For examples, see https://emerging.digital.gov/blockchain-forum/, https://emerging.digital.gov/blockchain-programs/, and https://www.dhs.gov/science-and-technology/news/2017/09/25/news-release-dhs-st-awards-750k-virginia-tech-company.

[13] Charles Romaine, NIST, testifying before the U.S. Congress, House Committee on Science, Space, and Technology, Subcommittee on Oversight, *Beyond Bitcoin: Emerging Applications for Blockchain Technology*, 115th Cong., 2nd sess., February 14, 2018.

[14] U.S. Securities and Exchange Commission, "Investor Bulletin: Initial Coin Offerings," alert and bulletin, July 25, 2017, at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

at the onset of a new technology. One option is to place authority for a technology within a single agency (e.g., nuclear energy in the Department of Energy). Historically, this option has been used when a technology is advanced and in relatively wide use, or is targeted at a specific industry or has a very specific application. When a technology has a broad application (e.g., information communication technologies) Congress has historically opted to have several federal agencies oversee the technology, charging different agencies with overseeing the different applications of that technology (e.g., DHS for federal agency security of information communication technology and the Department of Commerce for the development of guidelines for its use).

Conclusion

Interest in blockchain technology continues to grow in both the public and private sectors. However, it is helpful to remember it is not a single technology, but a novel way of using existing technologies already to enable transactions. Those transactions can also occur through using a combination of commercial off-the-shelf technologies without using blockchain. But, because of the cryptography involved in blockchain implementations, those transactions can occur among parties that might not otherwise have an established means to carry out a trusted transaction or do not mutually trust each other. As the public and private sectors consider blockchain use, awareness of both its advantages and limitations will better inform decisions concerning its adoption or avoidance.

Congress is aware of the growing interest in blockchain technology and has held several hearings on the technology and its potential implications for the economy and government use. Congressional interest in blockchain technology is likely to continue to grow as the technology becomes more established and especially if its application becomes more widespread.

Author Contact Information

Chris Jaikaran
Analyst in Cybersecurity Policy
cjaikaran@crs.loc.gov, 7-0750