

Harnessing the Blockchain Revolution:

CompTIA's Practical Guide for the Public Sector



Executive Summary

Blockchain technology is perhaps the most talked about and yet the most misunderstood emerging technology in the world today.

Since its inception, the secure, distributed ledger technology has widely been viewed through the lens of virtual currencies, particularly the hype surrounding the buying and trading of Bitcoin and other digital coin offerings. Indeed, surveys have shown that consumers are largely aware of what Bitcoin is, but do not know or understand about the blockchain technology that powers it.

Indeed, the increased popularity of the original Bitcoin application as well as intensified regulatory scrutiny of new “initial coin offerings” has dominated news coverage of blockchain-related technology. But those news stories have obscured the quiet blockchain revolution that has been taking hold at major corporations, among forward-thinking policymakers, and with startup technologists, who have been exploring how blockchain technology could make a wide variety of corporate and government operations more efficient and secure. A [May 2018 Deloitte survey](#) of corporate executives around the world found that 74 percent see a “compelling business case” for the use of blockchain, and 34 percent reported that their company has already begun work on blockchain systems; and another 41 percent said they expect to deploy a blockchain application within the next year.

Indeed, the public and private sector use cases for blockchain touch almost every sector — from health care and real estate to cybersecurity and education. As a somewhat early adopter, the federal government has begun blockchain projects at the Department of Defense, the Department of Homeland Security, the Food and Drug Administration, and the General Services Administration, among others. State and local governments also have

begun to employ blockchain, for example, in land title and health provider registries. In the private sector, meanwhile, companies have announced major investments in blockchain, such as Walmart and IBM partnering on a pilot project to secure the food supply chain.

These early adopters are not using blockchain just because it’s the hot new topic in tech circles. Inherent in the technology’s value are a number of benefits, such as:

- Security and audit trails that are built into the way it creates immutable records of new data and transactions;
- The ease at which it can facilitate, record and share data and transactions in a relatively frictionless fashion with little need for human interaction;
- The ability to consolidate data across various systems; and
- Its capacity to provide end-to-end visibility and transparency into an entire network.

In fact, [Gartner](#) recently pegged the business value of blockchain to grow to \$176 billion by 2025 and more than \$3 trillion by 2030 through increased business efficiency.

Those predictions suggest that the related trade in cryptocurrencies will become less volatile and that regulators will continue to target scam artists to protect investors.

As public sector institutions experiment with blockchain solutions, each organization should thoughtfully evaluate where they want to be on the continuum of blockchain adoption — from taking a risk-averse wait-and-see approach to becoming a potential pioneer for new use cases and implementation. Those positions will likely be impacted by an organization’s ability to find the right partners with which to build a consortium. As more organizations adopt and experiment with blockchain, it is critical to foster a community of shared learning to accelerate public sector competency.

As more and more businesses, governments, and other institutions begin to look seriously at blockchain’s benefits, so too might they begin considering how to incentivize the continued development of blockchain innovations that can be used to make government operations more secure, transparent, and efficient.

To do that, CompTIA suggests policymakers consider developing policies for blockchain environments that encourage developers and market participants to continue innovating and providing solutions that will aid the public sector in achieving its mission and goals.

But policymakers first should understand the promise, the uses and the questions that blockchain currently presents. We hope this guide will provide a framework for that analysis.

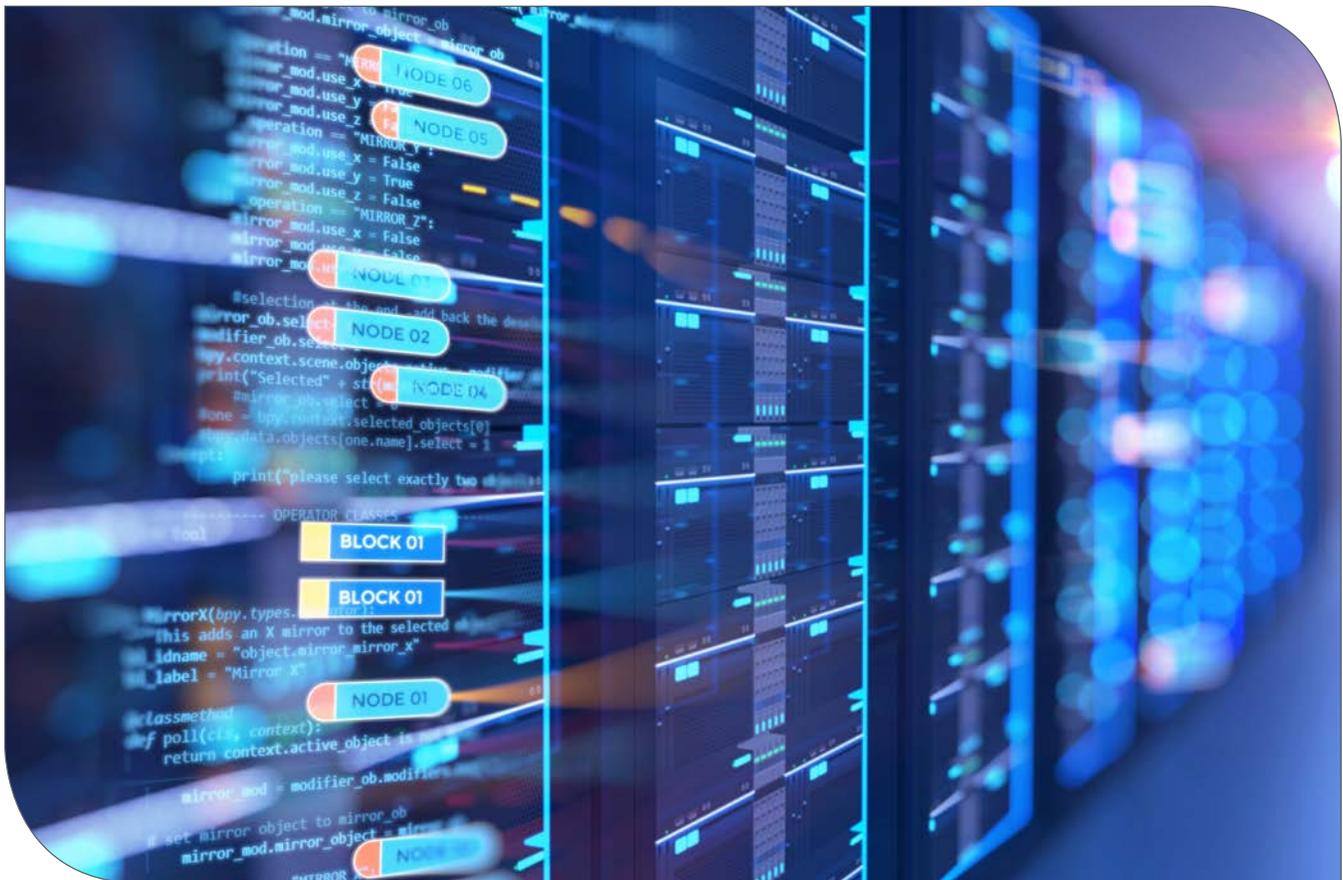


Table of Contents

- I.** What is Blockchain Technology? [4](#)
- II.** A Look at Blockchain Technology (Graphic) [6](#)
- III.** The Benefits of Blockchain Technology [7](#)
- IV.** The Blockchain Universe (Graphic) [9](#)
- V.** Blockchain Applications by Use Case and Sector [10](#)
 - a. Finance and Payment Systems [10](#)
 - b. Supply Chain Management and Logistics [12](#)
 - c. Autonomous Vehicles [14](#)
 - d. Blockchain for Records Management [14](#)
- VI.** Federal Government Blockchain Programs [18](#)
- VII.** State and Local Blockchain Programs [20](#)
- VIII.** Public Sector Blockchain Adoption Considerations [22](#)
- IX.** Policy Recommendations [24](#)
- X.** Pilot Toolkit [26](#)
- Appendix A** Frequently Asked Questions [28](#)
- Appendix B** Relevant Blockchain Research from U.S. Institutions [29](#)
- Appendix B** Blockchain References [30](#)
- Appendix D** Glossary of Terms [31](#)
- Acknowledgements [32](#)

What is blockchain technology?

Though the concept of a blockchain has been around since 1991, the first real blockchain technology first emerged about a decade ago with the release of Bitcoin, which was billed as a “peer-to-peer electronic cash system.” Bitcoin has been shrouded in mystery given its creator, who billed him or herself as Satoshi Nakamoto, has never been conclusively identified. As enthusiasm for Bitcoin grew over the years, a blockchain industry slowly evolved.



The introduction in 2014 of Ethereum, a decentralized blockchain applications platform, popularized the concept of smart, self-executing contracts using the blockchain. Importantly, Ethereum’s developers created a platform that has allowed other blockchain projects to use their underlying code to create unique applications, products, services and virtual currencies, [which has helped fuel both the cryptocurrency boom and innovation for other blockchain use cases.](#)

Whether through Bitcoin, Ethereum or another application, blockchain is a method for recording transactional information by storing, securing, and sharing data between separate parties. But rather than keeping a record of all transactions in a central location or database, blockchain utilizes a distributed transparent ledger.

IBM’s “**Blockchain Basics**” guide explains it this way:



Distributed to all member nodes in the network, the ledger permanently records, in a sequential chain of cryptographic hash-linked blocks, the history of asset exchanges that take place between the peers in the network.

All the confirmed and validated transaction blocks are linked and chained from the beginning of the chain to the most current block, hence the name blockchain. The blockchain thus acts as a single source of truth, and members in a blockchain network can view only those transactions that are relevant to them.

In this way, blockchain enables free exchange of data, or value, between entities that may or may not know each other. This data or value can be in the form of information, currency, or anything else that may represent or provide value to others on the blockchain. The blockchain method provides many benefits over centralized forms of recordkeeping, including transparency of data and no single point of failure.

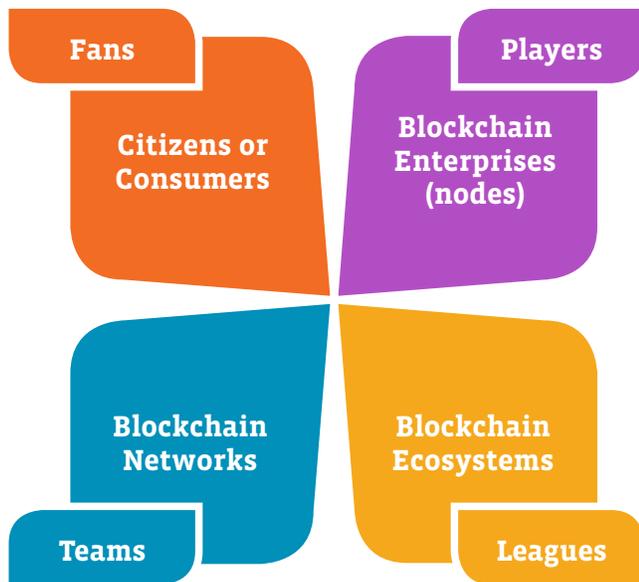
And the transactions, once executed, are tamper-evident because of the transparent nature of the ledger.

It's often said that blockchain is a team sport. It's a team sport because its success – its existence even – relies on a consortium of collaborators to work together in establishing technical protocols and governance models. By definition, as a distributed ledger technology, blockchain requires more than one player. Taking that analogy a bit further, a team of blockchain players will also be enhanced when there are other teams in the league and each league is more transformative when it interacts with other leagues.

As evidenced by the emerging blockchain use cases, the real value is found in the largely frictionless transactions throughout the networks, ecosystems, and, ultimately, interoperationally among those ecosystems. For example, a blockchain food traceability implementation by a global retailer by itself would not have achieved its transformative potential without expansion beyond that retailer's supply chain. Expanding all the way back to the farmer and including all the parties in and interacting with that supply chain is what makes it so powerful. The highest value will be realized when those supply chain ecosystems are then also interoperating with other retail and food supply ecosystems, payment and fintech ecosystems, legal, insurance and risk management ecosystems, global transportation and customs regulatory ecosystems, health and wellness ecosystems, and more.

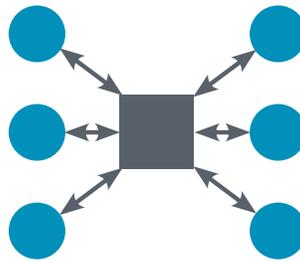
As sports professionals know, to achieve peak performance players and teams must be properly equipped. Similarly, to realize the \$3 trillion in business value identified by Gartner, enterprises (the public and private sectors alike) must also be properly equipped. An enterprise-grade blockchain effort requires that it be:

- Built on open standards
- Scalable and enterprise secure
- Developed with industry expertise by convening new ecosystems

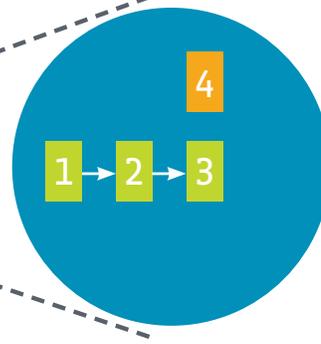
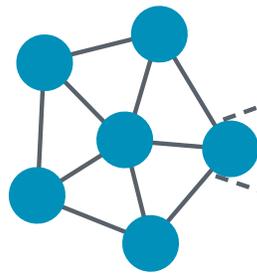


A Look at Blockchain Technology

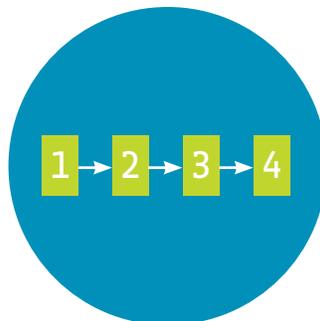
Most transactions today pass through a centralized third party that maintains a master ledger of all transactions. This ensures integrity but also creates overhead.



In systems that utilize distributed ledger technology such as blockchain, every node on a participating network keeps a copy of the full ledger of transactions. The cryptography built into the ledger maintains integrity while reducing overhead.



When a new transaction is introduced, each node begins validating the transaction using an algorithm defined by the blockchain network.



Once the transaction is validated, the new block is added to the chain. Each node on the network updates its copy of the ledger, and the node that successfully validated the block receives some sort of reward.

What are the benefits of using blockchain technology?

Immutable Transaction Ledger and Audit Trails

Blockchain data is tamper-resistant, meaning that one can't simply modify the ledger without anyone else knowing. Blockchain data is cryptographically linked and secured so that making changes to the ledger is both difficult and easily detectable.

Indeed, participants must use digital signatures with private keys that track the transactions from specific participants. While most blockchain transactions today are pseudo-anonymous, some private blockchain entities require ID verification and two-factor authentication before allowing users to access their services. This further reduces the dangers of malicious actors participating freely.

Consolidating Databases Securely and Sharing Data

Another emerging benefit of blockchain is the potential to consolidate transaction data from many disparate database systems without creating the security risks of a centralized authority or owner. That consolidated data can then be shared easily among the participants in the blockchain.

Traditional databases are typically owned and operated by a single person or organization. This brings about a number of security risks and process inefficiencies, depending on the particular use case at hand. For instance, the ease with which a single person could access and tamper with a database without other members knowing can be alarming. In fact, an unauthorized or unethical user could tamper with traditional databases in just a few command line entries, effecting the

status or ownership of data that represents real value. Additionally, enterprise resource planning and supply chain management systems often are set up separately to store information related to the ordering, processing, and fulfillment of a final product. However, if a problem occurs or if there's something of interest within the supply chain that needs to be investigated or addressed, there are often many layers of information systems that have to be used to reach a final answer or discovery. This is inherently inefficient and can directly result in consequences for all members of the supply chain.

Blockchain has the ability to consolidate, store, and share data from all of these disparate systems while maintaining a decentralized system of ownership. Each member of the supply chain would have access to their own blockchain node meaning they are all equal-owners and have copies of the blockchain ledger. The result of this is that each member has access to more information than they currently have access to in their own systems, but they don't have to relinquish control of their data to other participants.

While blockchain currently can be used to consolidate transaction data, it should be noted that the existing technology still has some scalability limits that could make integrating large databases unwieldy. However, as

of the writing of this guide, [new applications to enhance blockchain's scalability](#) are emerging. More information on blockchain scalability can be found in [Chapter VIII](#).

Customizable Smart Contracts Increase Transparency

Blockchain provides the ability to experience end-to-end visibility and transparency into a network that would otherwise be divided by the various information systems being used. Participants can ensure that their business partners or employees are transacting ethically, within rules that are agreed to through a blockchain enabled feature called smart contracts.

Smart contracts are customizable pieces of code that serve the purpose of enforcing business rules and other agreements on all transactions that occur on the blockchain. This feature gives a blockchain application the flexibility and customization required to be effective for many business or public sector uses.

Security and Data Protection

In today's digital and interconnected world, data security and data protection are top of mind for both public and private sectors, which is why many technologists have been looking to blockchain to add an additional layer of security and resiliency.

Blockchain secures its records via a highly-encrypted, 256-bit string called a hash that is updated for every transaction and is recorded across all nodes in the blockchain system. Even if cyber criminals were able to copy or steal blockchain records, it is highly unlikely that they could break through

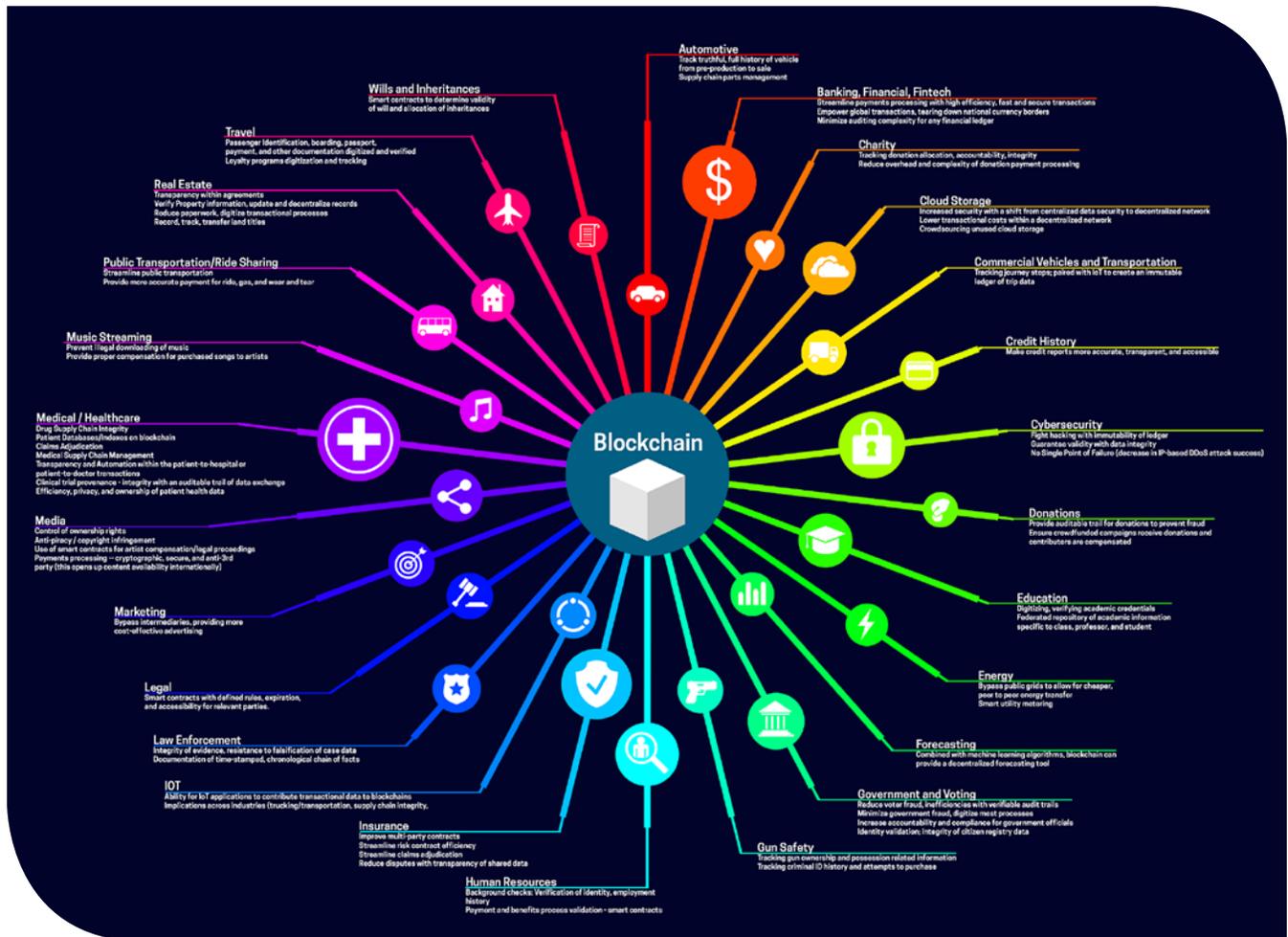
the sophisticated encryption associated with a blockchain record. Likewise, records in one blockchain system node that might be accidentally or purposefully lost or destroyed could be reconstituted from the other copies that are kept in the multitude of other nodes that record each and every transaction.



In that way, blockchain is considered one of the most secure technologies emerging today, because of its inherent security features, including:

- **Immutable data** records
- **Audit trails** can verify the authenticity of data.
- **Confidential or private information** can be secured through additional encryption.
- **Data protection** is built into blockchain because the decentralized nature of the records means that copies can be accessed via the multi-node aspect of the technology.
- **Privacy applications** could allow large groups of data to be anonymized to gain insight from that information while hiding or eliminating the personally identifiable information, or PII, within.
- **System Verification and Access IDs** ensure that systems talking to each other are verified and authorized to access/exchange data, while access IDs combine two or more factor authentication to ensure secure and authorized access.
- **Public / Private / Court Keys** could allow access to data or other records, such as communication records or bank transactions, for law enforcement investigations. (**Note: This could be controversial from a privacy standpoint. It would have to be built into the technology, and would need to be accessible to law enforcement only with proper legal process.**)

The Blockchain Universe



Courtesy Fluree DB

Blockchain Applications by Use Case and Sector

The potential industry and government sector opportunities for blockchain are seemingly endless, and according to market intelligence firm IDC, the 2018 [worldwide spend on blockchain](#) will be \$2.1 billion dollars. While many public and private sector entities are exploring blockchain technology, the growth sectors currently are in financial services and supply chain management.

The IDC infographic below depicts the top growth industries for blockchain.

Financial, manufacturing, and distribution sectors are rife with potential use cases, with many companies looking to transition from a proof of concept (POC) environment to full blockchain deployments in the near future. Professional services, discrete manufacturing and resource industries are the most aggressive investors in blockchain.



Source: IDC

A Finance and Payment Systems

Given Bitcoin was developed as an alternative payment system or currency, the implications of blockchain for finance and payments has been the most obvious use case for the technology.

In the U.S., many companies, such as Goldman Sachs, CME Group, and others, have begun to dip their toe into blockchain-powered cryptocurrency markets by opening or planning to open Bitcoin futures operations. Other

investment banks and hedge funds are looking at whether to offer cryptocurrency trading. However, broader adoption of cryptocurrency trading by legacy Wall Street firms will largely depend on how the Securities and Exchange Commission and the Commodity Futures Trading Commission decide to regulate such products.

Some countries, such as the United Kingdom and Canada, are attempting to stimulate innovation in the finance and payment systems space by creating regulatory sandboxes. In [announcing their sandbox in 2017](#), for example, the Canadian

Securities Administrators solicited bids for blockchain applications including:

- Online platforms, including crowdfunding portals, online lenders, angel investor networks or other technological innovations for securities trading and advising;
- Business models using artificial intelligence for trades or recommendations;
- Cryptocurrency or distributed ledger technology-based ventures; and
- Technology service providers to the securities industry, such as non-client facing risk; and
- Compliance support services (also known as regulatory technology or regtech).

These regulatory sandboxes highlight that finance and payment applications of blockchain extend beyond stock market-like trading of virtual assets. The potential benefits of using blockchain in finance and payments include streamlining payment systems; securing financial data; eliminating middlemen, such as banks, for conducting trustworthy transactions between entities or individuals; and guarding against waste, fraud and abuse, to name a few.

The International Monetary Fund has recognized the potential for blockchain to transform banking and finance worldwide and has cautioned regulators to take a light touch on regulation given the potential benefits of blockchain for central banks and other financial institutions.



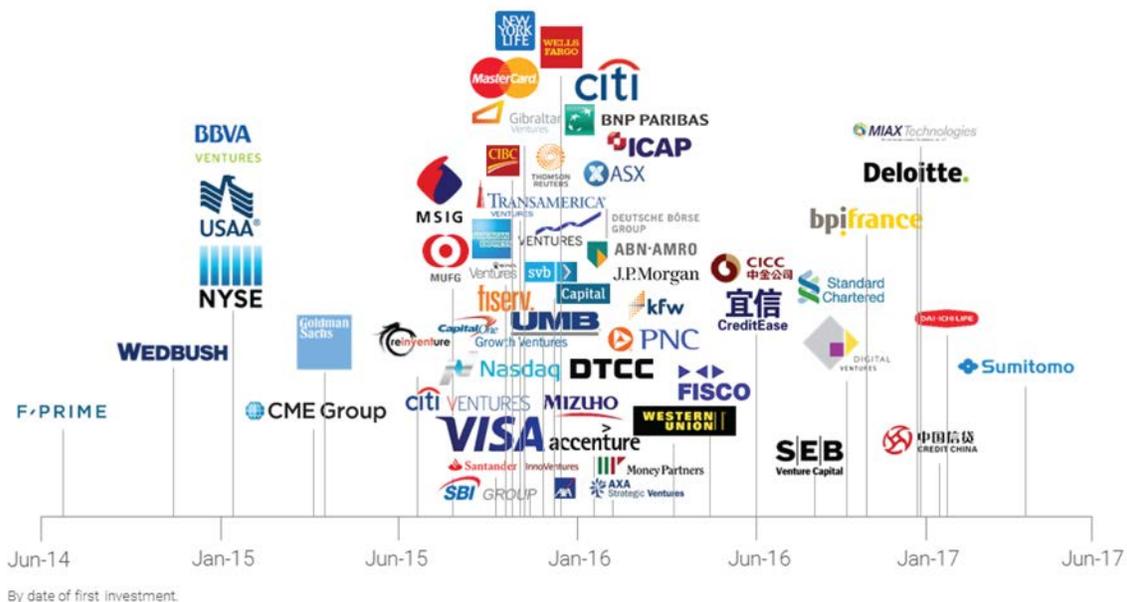
In its April 2018 [Global Financial Stability Report](#), the IMF stated:

Crypto assets have the potential to combine the benefits of traditional currencies and commodities. Like fiat money, they can potentially be exchanged for other currencies, be used for payments, and store value. As investment products, they may offer portfolio diversification, although their ability to do so is still limited by their short track record, regulatory uncertainty, and primitive market infrastructure.

The technology underlying crypto assets—distributed ledger technology (DLT)—could also lead to more efficient market infrastructure (IMF 2016a and CPMI 2017). This technology differs from traditional payment systems, which require a clearing entity, such as a central bank, that settles transactions and distributes funds between participants. DLT, in contrast, uses multiple copies of the central ledger, which are kept by individual entities.

Indeed, blockchain is being looked at by entities of all sizes as a solution for ordinary retail payments; B2B payments; stock market trades and transactions; cross-border payments that short-circuit exchange rate fees; and even to augment governments' central currencies.

Financial services firms invest early in blockchain



Source: CBI Insights

The U.S. Federal Reserve has [pointed out](#) the potential benefits of blockchain as well, but cautioned that the immutable nature of blockchain transactions and other issues does create some legal concerns that will need to be worked out before blockchain begins to be used more widely by central banks.

Taxes

From the federal to the local level, blockchain could be used in the collection and recording of business, property, personal income, excise, and other taxes. In addition to creating an immutable record and an audit trail, a blockchain could also allow for taxes to be instantaneously collected and recorded at the moment of services or compensation. This could significantly reduce the friction and time in processing taxes both for the entity collecting the tax as well as for those paying the tax.

Benefits Distribution

The verification process for benefits distribution has historically been time-consuming and fraught with errors, both honest clerical mistakes and occasionally intended misrepresentation. Blockchain-based authentication could be utilized to determine eligibility and access to social safety net services, such as Social Security and Medicare, in a way that could greatly reduce fraud, waste and abuse through the use of smart contracts and automation. This also could ease the administrative burden and arguably free more dollars for the original intent of the program.

Grant Making

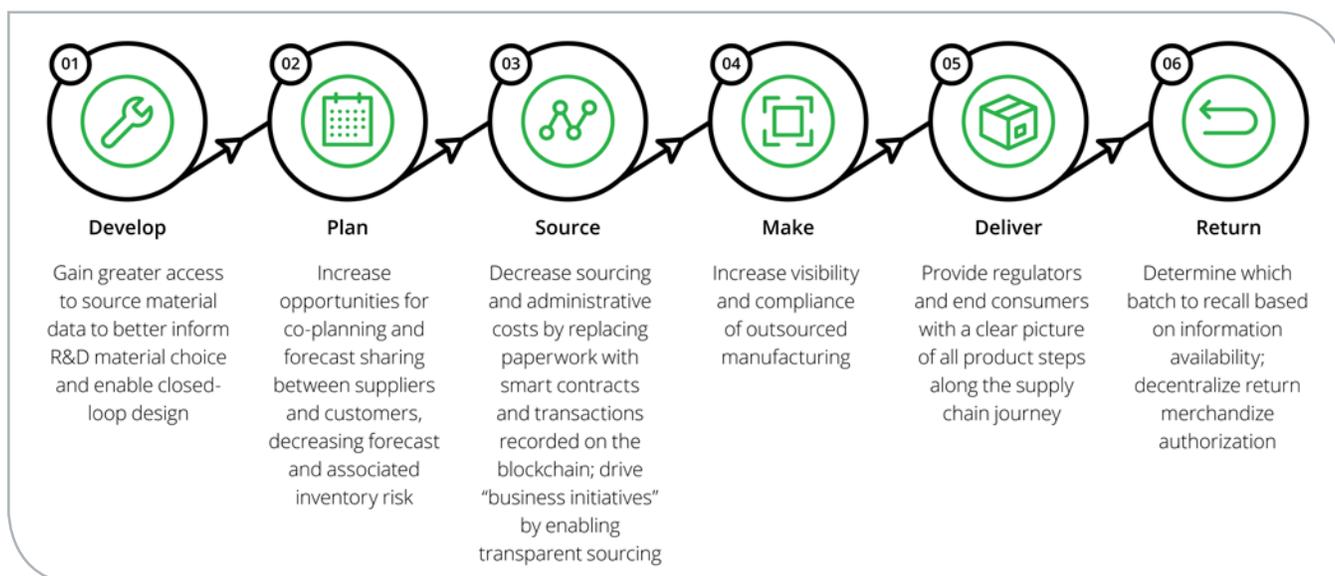
Similar to benefits distribution, grant making could be simplified and made more efficient through blockchain verification processes and distribution.

B Supply Chain Management and Logistics

The use case for blockchain that is most mentioned outside of finance and payment systems is supply chain management. For both the public and private sectors, the ability to track with certainty the origins and destinations of products and services would substantially simplify what is now an incredibly complex global system.

Deloitte has [described](#) the benefits thusly:

The availability of this information within blockchain can increase traceability of material supply chain, lower losses from counterfeit and gray market, improve visibility and compliance over outsourced contract manufacturing, and potentially enhance an organization's position as a leader in responsible manufacturing.



Source: Deloitte

Private sector companies seeking to employ blockchain for supply chain management include pharmaceutical distributors; agriculture/food distribution; retailers; digital media; cargo shipping; airlines; and delivery carriers, to name a few.

Food Safety

Food safety is essentially a supply chain management issue, and the unique benefits of using blockchain to secure the food supply chain from farm to table brings substantial public health benefits. Blockchain could allow public health agencies and food sellers to quickly and easily trace the source of a food-borne illness, which would speed recalls and prevent more people from being sickened.

In 2017, Walmart and IBM [announced](#) a partnership with Unilever, Tyson, Dole and Nestle to pilot a blockchain project designed to track the food supply chain from food suppliers to store shelves.

Transportation and Customs

Blockchain technology for supply chain management can be used in a variety of transportation, customs, and import/export related systems for supply chain management and other functions.

At ports, airports, and rail stations as well as in the trucking and commercial delivery sectors, blockchain could be used by both the public and private sectors as a way to establish end-to-end tracking of imports, exports, shipping containers, products, packages, and services. For vehicles on the move, technology such as license plate readers, radio frequency technology, or toll readers, could be used in conjunction with blockchain to ensure transactions and information can be authenticated, billed and reconciled in real time.

Maersk, the Danish container shipping giant, has been [testing a blockchain solution](#) from the University of Copenhagen to digitize the ships' cargo inventories in a partnership with IBM.



Source: Walmart

C Autonomous Vehicles

As driverless cars and trucks become more and more of a reality, the types of blockchain applications for autonomous vehicles, or AVs, may include a blend of payment systems, supply chain management, and information sharing.

Automakers, such as BMW, Ford, Renault, and General Motors, have [begun exploring blockchain solutions](#) that range from managing driving data to ride-share transactions and vehicle identity and usage information. The automakers' consortium, known as Mobility Open Blockchain Initiative (MOBI), aims to explore how blockchain can be used to create an ecosystem for AVs by creating common standards so that cars and trucks can communicate with each other and make payments as needed.

Chris Ballinger, the chairman and CEO of MOBI, [has said](#) that he believes the decentralized nature of blockchain not only will ensure that AV data is not owned by any one entity, but also might be able to improve road safety and reduce traffic congestion.

D Blockchain for Records Management

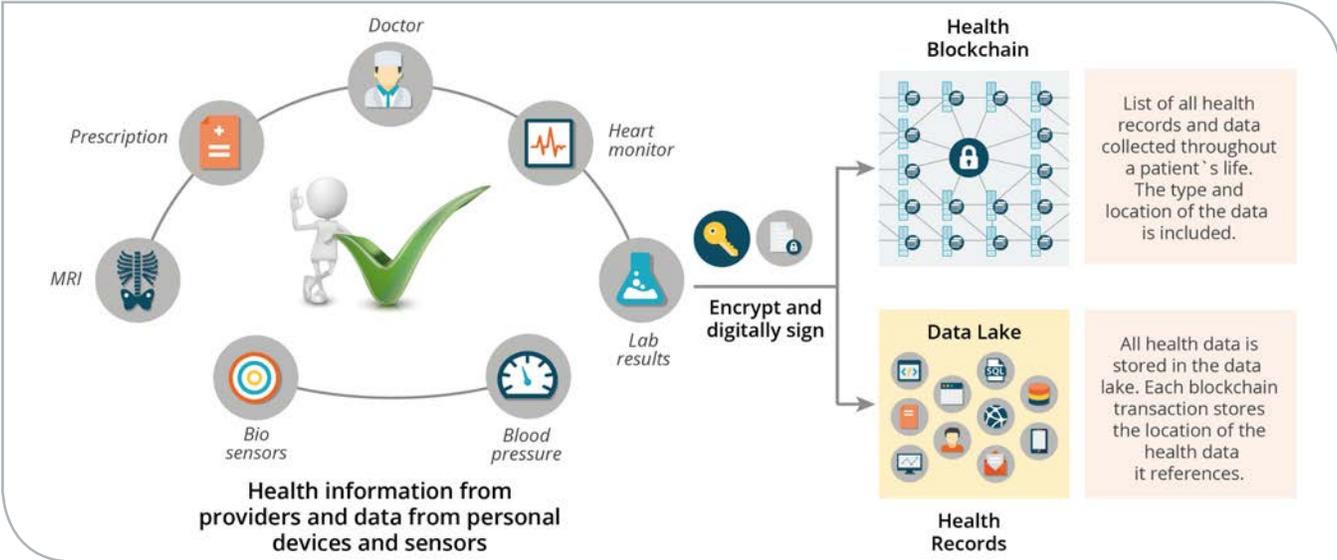
Healthcare

Both public and private sector health care systems are looking into the uses of blockchain technology as a more secure way to share and store health records, conduct billing, and liaise with insurance carriers.

Public health officials, in particular, see blockchain as a way to share medical records securely, which will aid doctors to better understand a patient's history, give patients more control over their information, and protect such information from malicious actors, according to a September 2017 report in [MIT Technology Review](#).

The technology also has shown promise in helping to verify doctor credentials. One Tennessee company is developing blockchain technology to “provide the market with a solution to address the effort, cost, redundancy, and complexity of obtaining and verifying practitioner identity and credentialing information,” according to its [press release](#). Of course, blockchain applications do not just apply to private sector doctors and hospitals, the ability to store and share medical records on the blockchain offers promise for government health care programs and entitlements, as well.

Health information technology solution provider Cerner has also placed an emphasis on blockchain. The company is creating a demonstrable prototype leveraging blockchain to provide security and auditability for a payer chart review process. A description of Cerner's prototype can be found [Here](#).



Source: HealthIT.gov

Education

The applications of blockchain in education range from verifying teaching credentials and sharing student transcripts to transferring credits between institutions and issuing continuing education certifications. Using the decentralized nature of blockchain could give students and educators more control over their own information without having to contact the institutions issuing the degrees or certifications.

In 2017, Sony [announced](#) it had developed blockchain technology for K-12 that “centralizes the management of data from multiple educational institutions and makes it possible to record and reference educational data and digital transcripts.” Putting such information on the blockchain makes it more difficult to alter or fabricate, and in announcing the initiative, Sony asserted that it will allow schools to “safely integrate and connect previously gathered data as is from ‘Student information systems’ and ‘learning systems,’ even if that data came from different providers.”

Additionally, Central New Mexico Community College became one of the first institutions of higher learning to use the blockchain to issue digital diplomas on the blockchain, allowing graduates to “independently manage their own, hard-earned education records and securely share them with employers or other schools for the rest of their lives,” according to the [press release](#).

Additionally, educational institutions could use blockchain or cryptocurrencies to ease payment for services.

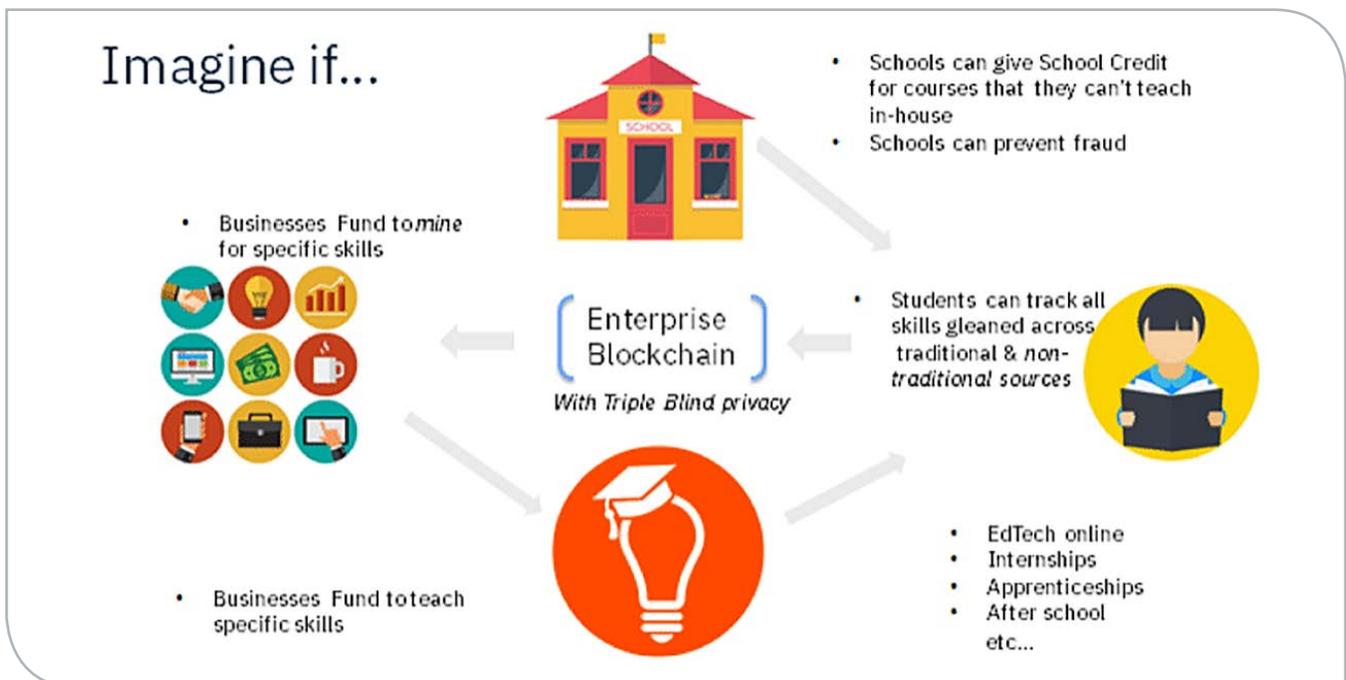
Election Management and Voting

The security inherent in blockchain has made it a potentially attractive solution for local election managers, because the technology could help minimize any potential voting fraud and also allow for a standardized ID of sorts beyond drivers licenses to validate voter eligibility.

However, the scale and scope of integrating blockchain into our voting systems, especially in high-population and high-turnout areas, still face challenges. This is because the longer and bigger blockchains become, the more unwieldy they are. Additionally, the amount of computing power needed to process such a large volume of records could prove a challenge.

So, any blockchain-based voting application would have to be implemented on a tiered basis to be effective and secure. One tier of blockchain based voting would be local in nature but would tabulate and summarize the state and federal level totals and pass just those summary transactions up to the state level. Likewise, tier 2 at the state level would record all of the state and federal level votes, tabulate and summarize those values and pass just the federal level (such as presidential or congressional votes) up to a third tier national level blockchain for further tabulation and results.

While using blockchain for elections presents some scalability challenges, some states are already testing it. In March 2018, West Virginia [announced](#) a blockchain-powered pilot program for overseas military voters but limited it to those who claim residency in two counties.



Source: Hyperledger

Intellectual Property

Patents, trademarks and copyrights are some of the most important business records that companies rely on the government to safeguard and authenticate. Using blockchain, those records could be easier to process and simpler to validate, and the technology could help streamline the approval process for new patents while keeping intellectual property encrypted for protection.

Personal Identification

With scourges like identity theft making personal information a commodity, some private and public sector institutions are looking at blockchain as a solution for people to control their personal information and for entities to more easily validate it. Possibilities include using blockchain for digital, multi-factor authentication and representation for things like Social Security cards, drivers' licenses, and non-driver ID cards.

As [some have pointed out](#), such systems will likely need to be generated by government entities and that blockchain may be just one part of a larger identity management system.

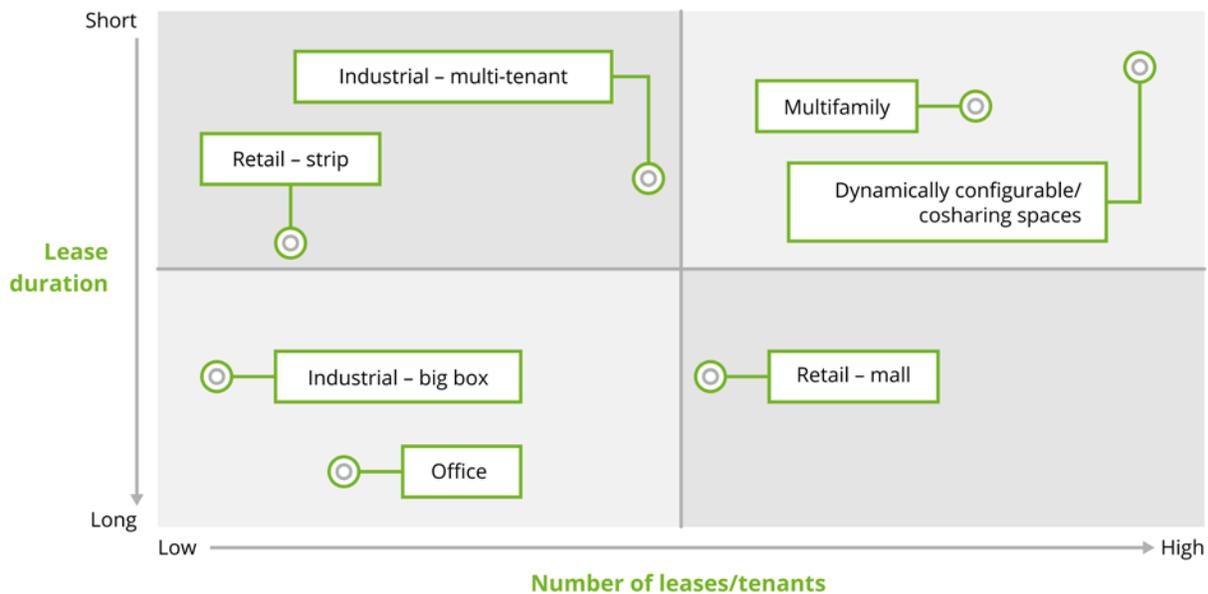
Property Ownership

A variety of property related transactions could be recorded and managed on the blockchain, including transactions involving leasing, purchasing and sales.

A Deloitte report posited that blockchain technology could help consumers by reducing costs associated with title management; improving the property search process for would-be buyers; expediting pre-transaction activities such as underwriting, financial evaluation and obtaining a mortgage commitment; managing ongoing lease agreements; and enabling more efficient financing and payments.

In the public sector, some localities are already experimenting with using blockchain technology and smart contracts to create secure records of deeds and other real property.

Illustrative framework to assess applicability of blockchain



Source: Deloitte Center for Financial Services analysis

Business Incorporations

Similar to property ownership and transaction records, blockchain could be used to securely record company registrations and provide consumers with a way to validate its legitimacy. This is especially important today given digital scams and imposters targeting legitimate enterprises.

In 2017, [Delaware](#) became the first state to facilitate the ability of corporations to record issuances, transfers and ownership of stock using blockchain technology.

Licensures

All kinds of licensures from simple drivers' licenses to service and professional licenses could be addressed via a blockchain-based system.

Besides building more efficient and frictionless systems, it would also be much easier for a consumer of services provided by licensed individuals or business to validate that license on the spot via smart phone or web app with no need for human verification. This would greatly improve the government's ability to ensure that goods and services are only being delivered by those who are licensed to do so.

Courts and the Legal System

Tracking of court proceedings and cases processed is another system that could benefit by the use of blockchain to record all proceedings in business, civil and criminal courts.



Federal Government Blockchain Initiatives

Many federal agencies and departments are exploring the uses of blockchain technology for various purposes. While the below is not an exhaustive list, it's clear the federal government is looking deeply at whether blockchain solutions are appropriate for everything from health records and cybersecurity to database management and other general efficiencies.



Some federal agencies and departments have already begun to explore blockchain including:

- Department of Defense
- Department of Homeland Security
- Food and Drug Administration
- General Services Administration
- Department of State
- National Institute of Standards and Technology
- Department of the Treasury

Department of Defense



In the most recent [military spending bill](#) signed by President Trump, the Department of Defense was authorized to investigate the “potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies.” It has also been reported that the Department of Defense [has been studying](#) blockchain for the purposes of delivering secure messaging and protection of the digital 3D printing supply chain.

Department of Homeland Security



As discussed previously, blockchain shows tremendous promise for cybersecurity. So, it's no surprise that in 2016 the Department of Homeland Security's Science and Technology Directorate awarded a \$199K contract for "[Blockchain Software to Prove Integrity of Captured Data from Border Devices](#)" to Factom. The purpose of the contract is to authenticate "Internet of Things" (IoT) devices to prevent spoofing and ensure data integrity by making use of blockchain technology. This contract was awarded through the Science and Technology Silicon Valley Innovation Program.

That same year, the department [awarded grants](#) to four companies to develop solutions under the rubric of "[Applicability of Blockchain Technology to Identity Management and Privacy Protection](#)."

Food and Drug Administration



The Food and Drug Administration has [initiated a study](#) to determine how data from electronic medical records, clinical trials, and health data from wearable devices could be best utilized with blockchain technology for the purposes of sharing and auditing the data. The initial phase will focus on clinical trials and data from oncologists.

General Services Administration



The [General Services Administration](#) has built its own federal procurement blockchain proof of concept. This exercise was meant to demonstrate how blockchain could improve the federal procurement process. The proof of concept showed [results](#) that allowed the awarding of contracts to be [reduced by ten times](#). This was accomplished by automating processes like financial review and making use of smart contracts to calculate certain factors. Use of this automation and smart contracts also reduced the occurrence of clerical errors, fraud, or personal bias in the awarding of contracts.

As one General Services Administration official [said](#) in November 2017, "Rather than take a number of days to do financial analysis and a number of days to develop a negotiation position, rather than have to log into a bunch of different systems to find that information and organize it, we are able to do that now in one second. And that lessens the burden on the industry partner, and it allows the contracting

professional to focus more on critical thinking tasks rather than the process tasks associated with interacting with multiple systems."

In addition, the General Services Administration has created a blockchain community with blog posts and other forms of communication to foster the education and inclusion of blockchain technology as they approach agency issues.

Department of State



The Department of State has formed a working group to determine how blockchain can best be utilized to assist State with their responsibilities. While still in the exploratory stage, the Blockchain@State group is looking to blockchain as a way for "increasing transparency, maximizing the impact and accountability of foreign assistance, and improving IT platforms," [according to the department](#).

National Institute of Standards and Technology



The National Institute of Standards and Technology (NIST) most recently issued the "[Draft NIST Interagency Report \(NISTIR\) 8202: Blockchain Technology Overview](#)." The purpose of the overview was to introduce blockchain to the uninitiated, discuss the use of blockchain as it relates to cryptocurrency, and explore some of its broader applications.

Department of Treasury

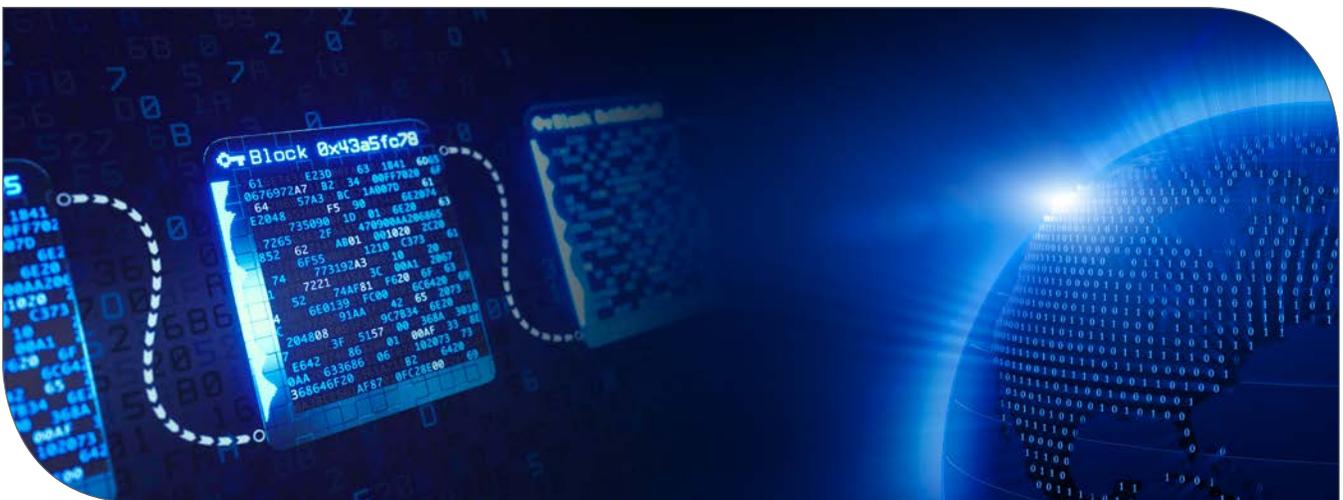


The Bureau of the Fiscal Service's Office of Financial Innovation and Transformation (FIT) is exploring how to use blockchain to keep track of and manage physical assets, such as computers, cell phones and other equipment.

As FIT's [press release](#) noted, "Distributed ledger technology has shown great potential for streamlining burdensome reconciliation operations that are involved in many financial processes. The pilot project will test whether the inventory of an agency's physical assets can be continuously monitored and reconciled in real time as the physical assets are transferred from person to person throughout the pilot."

State and Local Blockchain Initiatives

Many states are moving forward on blockchain initiatives in various ways. Some, such as Illinois, have taken the lead in adoption of the technology to identify more efficient and cost effective ways to provide services to their residents.



Some states are working on pilot programs for the securing of data and the continuous tracking of assets, including marijuana. Cities are also working on pilot programs. [Austin, Texas](#) and [South Burlington, Vermont](#) are piloting separate programs that, respectively, would assist in the distribution of services to the homeless as well as the registration of local land and property ownership.

Others have, or are in the process of, enacting legislation to assist blockchain industry growth. However, to date,

no state has taken any pilot program to full adoption. This highlights that the technology is still in its infancy and experimentation is more common than use in a large-scale manner. However, the increasing number of states becoming active in the sector does speak to the growing popularity of blockchain technology.

Illinois

Illinois is considered a national leader in its attempts to adopt blockchain technology, including exploring

blockchain for use in the following government programs or functions:

- SNAP/TNF (food stamps)
- Medicaid/Medicare
- Unemployment Insurance
- Workers' Compensation
- Student Loans
- Tax Collection

The state has detailed its efforts in the "[Illinois Blockchain and Distributed Ledger Task Force Final Report to the General Assembly](#)" dated January 31, 2018. This report details both the possibilities and the hurdles that Illinois could face from wider adoption of blockchain solutions.

Delaware

Delaware [has instituted a pilot program](#) whereby the application of blockchain technology to its public archives will allow the storage, distribution, encryption and sunseting of documents. Eventually, [the pilot program will be expanded](#) to allow the government to take additional actions with the documents inclusive of the issuance of the notice-of-lien and other official actions.

State Legislation Passed

At least 10 states — Arizona, Colorado, Delaware, Illinois, Nevada, New Hampshire, Tennessee, Vermont, Washington, and Wyoming — have all passed blockchain related legislation.

Arizona [passed legislation](#) stating signatures in electronic form cannot be denied legal effect. It also defines smart contracts and blockchain technology.

Colorado [passed](#) legislation directing the state Office of Information Technology to explore blockchain for a variety of state data initiatives, including business licensing, cybersecurity, and sharing data.

Delaware enacted [legislation](#) allowing corporations to use blockchain to maintain corporate records, including stock transaction records.

Illinois [passed legislation](#) creating the Blockchain and Distributed Ledger Task Force, which has recently released their first report.

Nevada has [passed legislation](#) banning local governments from taxing blockchain use. Additionally, the law specifically provides that blockchain should be afforded legal recognition to electronic records.

New Hampshire [passed legislation](#) that exempts digital currency from the state's money transmission regulation.

Tennessee [enacted](#) legislation to recognize the legal authority to use distributed ledger technology and smart contracts in conducting electronic transactions.

Vermont [enacted legislation](#) that would allow for broader business and legal application of blockchain technology.

Washington [passed legislation](#) requiring virtual currency to be subject to the money transmitter laws.

Wyoming adopted [several pieces](#) of legislation related to cryptocurrencies that lawmakers said were aimed at making the state "a blockchain-friendly environment for businesses." The measures exempted the buying, selling, issuing and transfer of cryptocurrency from licensure requirements; exempted some cryptocurrency developers from state securities and money transmissions laws; exempted cryptocurrency from state taxation; and authorized corporations to use a blockchain to create, record and store corporate records.

Legislation Under Consideration: A Sampling

New York is exploring [various bills](#) including the creation of a task forces to study the potential impacts of blockchain; the creation of a state-issued cryptocurrency; the legalization of electronic signatures secured through blockchain; and directing the state Board of Elections to examine the use of blockchain in elections.

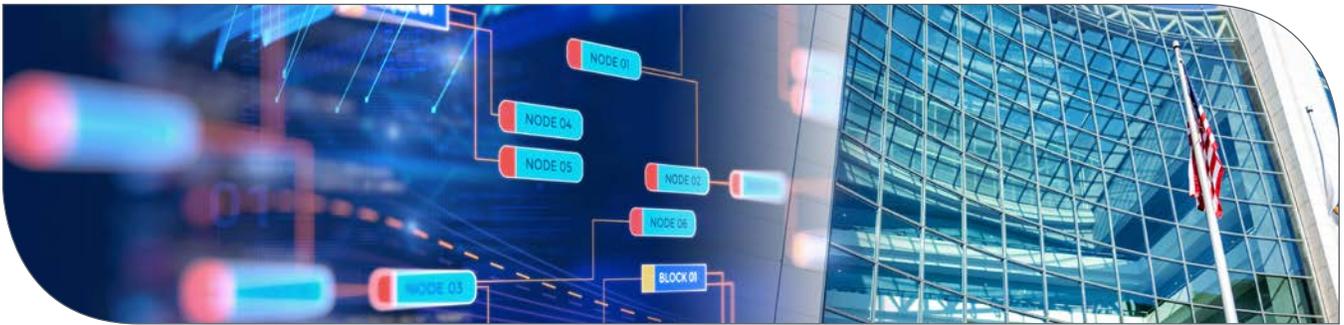
Vermont is considering [a bill implementing](#) rules for blockchain-based limited liability companies organized for the purpose of using blockchain for a material portion of their business activities.

Virginia is evaluating [legislation to assess](#) the impact of cryptocurrencies on the taxpayers.

Other states with blockchain-related legislation under consideration include [Hawaii](#), [Florida](#), [Nebraska](#), [New Jersey](#), [Washington](#), and [West Virginia](#).

PUBLIC SECTOR BLOCKCHAIN ADOPTION

Blockchain technology is evolving at a rapid pace, and there is a general agreement that blockchain can be used to improve the way the government currently does business. But as more public sector leaders begin experimenting with and investing in blockchain technology, there are several business, organizational, technological, and human capital considerations that should be addressed before adopting blockchain.



Adopting the Right Procedures

When a public sector organization seeks to experiment with blockchain, their first step is typically to identify a business problem that will demonstrate the power of blockchain over traditional databases or transaction systems. This can be challenging for two reasons:

1. In order to design an appropriate blockchain solution, there must be a significant level of understanding of blockchain platforms that are suitable for the problem at hand, and there should also be a significant level of understanding of the current process itself. Finding the right technical and functional talent to manage and execute a government blockchain project is a major challenge government leaders are facing today and will likely depend on public-private partnerships or a project solicitation.

This balance of functional, technical, and business talent is

critical to ensuring the business problem is well scoped and viable as a potential blockchain solution.

2. Once a clear business problem is defined, the next step is to determine which stakeholders are involved in the current process and whether or not a consortium is beneficial or required in order to establish a minimum viable blockchain ecosystem.

Pulling together the right players to build a consortium is no easy task. Public sector leaders need to now come together to strategically design a network not only based on their functional interests, but now also based on the common needs of a partnership. Blockchain is a team sport, and to many in government who are used to the concept of sole ownership and responsibility when it comes to their data and business processes, this new operating model will take some getting used to.

Scalability

Blockchain technology has tremendous promise for a wide variety of public sector uses and has the ability to process a large volume of transactions or data in a relatively short period of time. However, scalability is still an issue when it comes to integrating very large databases or processing extremely high volumes of data at one time. And the larger the blockchain, the more cumbersome it can be to process transactions.

While scalability solutions are forthcoming from a variety of developers, public sector leaders should consider the size of the project when evaluating whether a blockchain solution is the right choice.

Workforce Considerations

Challenges persist whenever an organization shifts to new technological capabilities. For example, the federal government has a mixed record in integrating cloud computing into its systems, despite a February 2011 White House policy to put “**Cloud First.**”

But the program ran into several problems along the way:

- Failure in some instances to assess and articulate the security benefits and risks to specific cloud computing applications;
- Failure to articulate to end user employees the benefits of the technology and the return on investment; and
- Failure to provide adequate skills training on how to use the new technology.

Despite the establishment of the Federal Risk and Authorization Management Program (FedRAMP) as a government-wide program to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, the program was viewed by some vendors and contractors as a barrier to entry to the federal marketplace.

Additionally, a significant component of changing technological applications is in ensuring that the workforce has the proper skills and training to operate and manage the technology. Cloud computing transformations at the federal level ran into significant barriers from workforce challenges.

When deciding to implement blockchain technology into new programs, it will be imperative that organizations do the following:

- Highlight and clearly define for employees the cyber capabilities of blockchain technology;
- Clearly articulate to employees the potential and actual return on investment for investments in emerging technologies, such as blockchain;

- Provide end user employees with adequate training to ensure they can use the technology properly and efficiently.

Regulatory Issues

Government leaders have recognized the importance of balancing regulation with innovation. Given how new the technology is, early restrictions on blockchain innovators could hinder the technology’s greatest potential.

Regulation in the blockchain space is inconsistent or nonexistent, but in the cryptocurrency space, the Securities and Exchange Commission and the Commodities Futures Trading Commission have begun asserting their jurisdiction.

Still, it is not yet clear whether regulation will be driven top down (Federal → State) or bottom up (State → Federal). Part of the challenge comes from the need to anticipate downstream consequences based on where the technology is headed in order to make well-informed decisions. Due to the current volatility and rapid evolution of the underlying technology, it remains difficult to speculate what exactly the government’s role will be, particularly when it comes to blockchain applications that are not tied or are loosely tied to cryptocurrency.

Across all layers of government, leaders are struggling to understand the risks associated with the integration of blockchain and their existing IT systems. The spectrum of privacy and security challenges today are not well-identified and cover areas including access key management, corrupt oracles, and identity verification.

Law Enforcement Considerations

Criminal elements, including terrorist financing, money laundering and tax evasion, remain a troubling aspect of the cryptocurrency space of blockchain technology. The pseudo-anonymous nature of cryptocurrency transactions on the blockchain still allows criminal elements to mask illicit transactions and fund their malicious activities.

While some may debate whether criminal law should be altered to ensure law enforcement access to unfiltered blockchain information, current laws, particularly those related to fraud, are being used by federal officials to go after many bad actors.

The Internal Revenue Service and other law enforcement agencies have made some strides in unmasking illicit activity by serving cryptocurrency exchanges with summonses to reveal their customers and in tracking IP addresses to identify tax scofflaws and other criminal elements. The SEC has similarly taken several enforcement actions against fraudulent cryptocurrency offerings using current laws.

Policy Recommendations

1 Federal Blockchain Stakeholders Advisory Group

To facilitate the maturation of blockchain technology, CompTIA recommends that Congress create a working group of federal stakeholders to provide recommendations to Congress on how to plan and encourage the growth of blockchain technology.

The working group, which would consist of private industry, academia, non-profits, and trade associations, would be responsible for examining the following aspects of the blockchain technology ecosystem:

Current and Future Security Requirements

As the blockchain ecosystem grows, so do threats to the ecosystem. Advances in quantum computing call for a focus on secure quantum computing encryption. NIST recently held a competition for quantum resistance. It will be critical for cyber requirements to be in lockstep with the emergence of the technology.

The Regulatory Environment

As blockchain becomes more prevalent in both the federal and state marketplaces, it will be important to ensure a nurturing environment for this nascent technology. The current regulatory environment should be adjusted to make it more friendly and adaptable for emerging technologies to experiment and innovate.

Standards and Interoperability

In order for blockchain technology to have the potential to grow, the industry should develop standards for blockchain and distributed ledger technology (DLT) terminology as a means to clarify definitions in the sector and set a platform for the development of other related standards. Once terminology surrounding blockchain and DLT has been determined, privacy, security, and identity issues can then be collectively addressed through the development of one or a suite of standards.

Defined Marketplace and Potential for Disruption

In order to assure the continued adoption of blockchain technology, it will be critical for end users to share best practices, case studies, and return-on-investment stories to help the nascent industry grow.

The Current Use of Blockchain Technology by Federal Agencies

Federal agencies already have implemented various blockchain technology projects. To fully benefit from blockchain technology, federal agencies need to consider the following five requirements related to the use of blockchain technology: (1) technological expertise; (2) funding necessary for implementing blockchain technology projects; (3) architectural plans on how to implement blockchain technology projects; (4) red tape/culture; and (5) interoperability, privacy, and security. The working group should discuss these challenges and propose approaches for addressing them.

2 Regulatory Sandboxes

To incentivize more innovation and experimentation in blockchain technology, developers and companies need to be assured that the risk/reward balance is favorable.

To help manage risk, drive economic development and develop a strong regulatory regime, CompTIA recommends that the federal government and state governments consider creating a blockchain and emerging technology “regulatory sandbox.”

This type of sandbox is an environment that should be established by a known regulator. It allows early blockchain adopters and innovators to operate in a controlled, regulated environment without fear of regulatory sanctions. A regulatory sandbox can make it possible to achieve a balance between the fast-paced innovation that typifies blockchain and the need for a risk-free development environment.

These sandboxes provide a set of pre-approved, published rules that allow innovators to test their products and business models. The rules help limit exposure and provide best practices and steps for testing innovative practices.

Sandboxes provide a way for regulators and law enforcement to develop policies that govern blockchain technology as well as police the industry for malicious actors and scam artists.

Many other countries, and some states, have implemented regulatory sandboxes:

- The [U.K. Financial Conduct Authority \(FCA\)](#) established a regulatory sandbox for blockchain and other emerging technologies in 2016. In its 2017 assessment of the program, the FCA stated, “Early indications suggest the sandbox is providing the benefits it set out to achieve with evidence of the sandbox enabling new products to be tested, reducing time and cost of getting innovative ideas to market, improving access to finance for innovators, and ensuring appropriate safeguards are built into new products and services.”
- [The Bank of Thailand](#) also established a regulatory sandbox in 2016 with the goal of encouraging innovation in fintech and providing consumers with better and faster access to financial tools and from more diverse sources. Fourteen Thai banks joined together to take advantage of the sandbox and [launched their blockchain platform](#) for administering letters of guarantee in July 2017.
- [Australian Securities and Investments Commission Sandbox](#), established in 2017, allows “eligible fintech businesses to test certain specified services for up to 12 months without an Australian financial services or credit license.” It provides for “three broad options” for product testing or operating a service without a license, including “relying on existing statutory exemptions or flexibility in the law – such as by acting on behalf of an existing licensee; relying on ASIC’s ‘fintech licensing exemption’ for the testing of certain specified products and services; and for other services, relying on individual relief from ASIC.”
- In the United States, [Arizona has instituted the first state wide regulatory sandbox](#). This particular sandbox, which was established by law in March 2018, is focused on emerging tech and the financial services sector, and it will take effect later this year. Under the program, companies will be able to test their products for up to two years and serve as many as 10,000 customers before needing to apply for formal licensure.
- [The state of Illinois is also considering a regulatory sandbox](#). The Regulatory Sandbox Act (SB3133) is currently making its way through the Illinois legislature.

Pilot toolkit



One of the best ways to get started using blockchain is to work with a consultant or well-educated individuals who understand four elements related to the intended project:

1

The reason why your organization would need blockchain.

2

The workings of the blockchain protocol and technological framework options.

3

Your organization's information technology (IT) environment.

4

How to develop sophisticated applications.

One of the best ways to get started is to create a pilot toolkit. This toolkit would be composed of:

1. A synopsis of the organization's needs.
2. Why blockchain is a viable solution.
3. Whether there are non-blockchain solutions that are available and effective.
4. A recommendation of a particular blockchain framework.
5. A discussion of the need for resources, including:
 - a. Programmers/developers
 - b. IT workers
 - c. Support staff, including legal, leadership, as well as business development

Blockchain Policy Frameworks

One of the more important factors in beginning a pilot blockchain project is choosing the blockchain, or framework, that is right for your organization. From a technological standpoint, it will be important for organizations to look at the pros and cons of various available frameworks.

Frameworks can be “permissioned” or “permissionless.” For the public sector, a permissioned framework is generally recommended, because it allows the creators of a blockchain to determine the entities or individuals who can write to a blockchain, view it, or interact with it in any way. Most frameworks that focus on the finance industry, supply chain management, and other business solutions allow the blockchain creators to set permissions. Bitcoin and many other publicly traded cryptocurrencies are “permissionless.”

Many frameworks already exist, including:

- [Hyperledger Fabric, Indy](#) or [Sawtooth \(www.hyperledger.org\)](#): A series of projects led by the Linux Foundation that provide myriad frameworks for consensus building (Fabric), centralized identity (Indy), and distributed ledgers (Sawtooth). A cross-industry framework. Permissioned.
- [Ethereum \(www.ethereum.org\)](#): A leading platform for building smart contracts, supply chain management, and, of course, the Ether cryptocurrency. A cross-industry framework. Permissionless.
- [J.P. Morgan Quorum \(https://www.jpmorgan.com/global/Quorum\)](https://www.jpmorgan.com/global/Quorum): A financial services framework. Focuses on implementing solutions for high-volume transactions. Permissioned.
- [Multichain \(www.multichain.com\)](#): Ideal for implementing a private blockchain. Cross-industry, but does not support smart contracts. Permissioned.
- [Ripple \(https://ripple.com\)](https://ripple.com): A financial services framework. Ideal for creating global payment systems via blockchain. Permissioned.
- [R3 Corda \(www.r3.com\)](#): Focuses on creating various solutions via blockchain, including cryptocurrency, finance, commerce, smart contracts and supply chain management. Permissioned.

Public blockchains have an entity that governs the creation of the framework. Generally, the creators of the framework govern their own frameworks. Quorum, however, is run by both J.P. Morgan and Ethereum; it was developed to allow Ethereum to provide a permissioned blockchain framework.

The aforementioned frameworks tend to be specific to an industry sector need. For example, organizations interested in supply chain management and smart contracts may want to consider using Ethereum or Hyperledger as their framework of choice. If financial transactions are paramount, then a framework such as R3 Corda or J.P. Morgan Quorum would be preferable. Consult carefully with reputable developers and blockchain consultants.

Regardless of which is used, all blockchain frameworks use a consensus algorithm to prevent the problem of “double spending,” which is a set of coins is spent in more than one transaction, or where two conditions exist that can cause a smart contract to fail. Consensus algorithms include:

- **Proof of work:** Any mining-oriented blockchain, including Bitcoin and Ethereum. The first algorithm used.
- **Byzantine Fault Tolerance:** Uses special entities called “validators” (also called “generals”) to manage the blockchain. Validators exchange messages between each other to ensure consensus.
- **Proof of Stake:** Instead of mining coins, this algorithm focuses on who has obtained a portion of the coins.
- **Decentralized acyclic graph (DAG):** Used to model information to achieve consensus.

When developing your own pilot toolkit, your organization should look to the above considerations. Implementing blockchain will require experts in each area. You may be able to hire these individuals. It is more likely, however, that you will contract with an entity or obtain these services on an as-needed, cloud and as-a-service basis.

Appendix A

Frequently Asked Questions

Why was blockchain first created?

An anonymous person or group that goes by the name of Satoshi Nakamoto proposed the first use of blockchain as we now know it to develop and implement a trust mechanism for the Bitcoin cryptocurrency. Satoshi's white paper is considered an essential first resource when understanding blockchain and the possible services it can provide. You can read Satoshi's white paper [Here](#).

Does the United States Government advocate the use of blockchain?

Several departments are considering the use of blockchain, including: the General Services Administration, the Department of State, the Department of Defense, the Department of Homeland Security, and the Department of Treasury. A bipartisan Blockchain Caucus was created in the U.S. House of Representatives in 2016 as way to promote innovation in the industry and look for blockchain solutions that can be used for federal programs.

Does the use of blockchain allow illegal or unethical activities?

Blockchain technology in and of itself is legal to use in most countries. The primary reason why blockchain would be limited in any country is that it uses an encryption level, or strength, that is not allowed in the country.

As with any technology, blockchain applications may be targeted by malicious actors. Illegal and unethical uses of cryptocurrencies, for example, is an issue regulators, such as the Securities and Exchange Commission and Commodity Futures Trading Commission, have been tackling. But in and of itself, blockchain is considered legal and proper to use in most parts of the world.

Is blockchain the same thing as Bitcoin?

No. Blockchain is an enabling technology that can be used in many different situations. Bitcoin is an example of a cryptocurrency that is powered by blockchain. Blockchain is a distributed, digital ledger that records transactions permanently, chronologically, and usually in a public manner.

What is a “smart contract?”

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts do not need third parties to validate their accuracy or authenticity.

Is there a single blockchain?

No. It is possible for any individual organization or person to create their own blockchain application. Cryptocurrencies such as Bitcoin, Ethereum, and Zcash, for example, have distinct blockchains.

Are there public and private blockchains?

Yes. It is possible to create a public, or permissionless, blockchain, which allows everyone to see and participate in the transactions. Permissionless blockchains are popular among cryptocurrencies. It also is possible to create a private, or permissioned, blockchain, which allows only certain individuals to participate. For more information, consult the following resources:

- [The difference between public and private blockchain \(IBM\)](#)
- [What is the difference between private blockchains and public blockchains like Bitcoin? \(Quora\)](#)

Is blockchain really secure?

There is no such thing as a technology that is completely fool-proof. The hashing algorithms and techniques found in the blockchain protocol are at least as secure as well-regarded encryption technologies, such as Transport Layer Security (TLS), which is used to encrypt transactions when you use your Web browser to make a purchase, or technologies to create the Virtual Private Network (VPN) connections that many use to connect securely to their company resources.

Some consumers of cryptocurrencies have fallen victim to well-publicized security issues involving “wallet software” used to conduct transactions. But these hacks generally involve ancillary elements, and not the blockchain itself. The software used to create specific blockchain interfaces is created by people, and people make mistakes. But bug fixes and workarounds will most likely solve specific, tactical problems.

Several theoretical attacks on blockchain have been publicized. These include the [Finney Attack](#) (a “double spend” attack), and the “[Greater than 50%](#)” attack. Still, the vast majority of organizations consider current blockchain uses to be secure and trustworthy.

Does a blockchain have to have a publicly traded token or coin?

No. While issuing coins or tokens is a common method that finance and payment systems use to drive public adoption of their specific blockchain project or cryptocurrency, private, or permissioned, blockchains do not require tokens or coins to be traded in order for the system to be secured.

Appendix B

Relevant Blockchain Research

Our nation’s colleges and universities have been a hotbed for blockchain innovation, with dozens of blockchain labs spread throughout the United States. Here is a sampling of the latest in blockchain research in higher education.

Arizona State University

[ASU Blockchain Research Lab](#) – ASU has [partnered](#) with digital currency provider DASH on their blockchain research lab.

Massachusetts Institute of Technology (MIT)

[Blockchain Papers and Projects at MIT](#) – MIT has released a selection of papers and studies being done on blockchain at MIT.

University of California at Berkeley

[Blockchain at Berkeley](#) – Berkeley hosts a users’ group focused on blockchain and cryptocurrency.

Duke University

[Duke Blockchain Lab](#) – Duke hosts a student-run organization aimed at promoting blockchain adoption.

Purdue University

[Purdue Blockchain Lab](#) – Purdue’s lab received a \$1.5 million grant from an Australian company to support blockchain research and development.

George Mason University

[Masters Course – George Mason offers a class to Masters computer science student on blockchain technologies.](#)

Appendix C

Blockchain Resources

The National Institute of Standards and Technology (NIST) has created a draft document entitled “Blockchain Technology Overview.” It is categorized as NISTR 8202. You can read the draft document at the following locations:

- <https://csrc.nist.gov/publications/detail/nistir/8202/draft>
- <https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf>

It contains an authoritative and relatively concise understanding of blockchain. You can also consult additional resources, including:

A Complete Beginner’s Guide to Blockchain (*Forbes Magazine*): <https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain>

Deloitte’s 2018 Outlook Highlights the Growth of Blockchain Technology (Nasdaq Article): <https://www.nasdaq.com/article/deloittes-2018-outlook-highlights-the-growth-of-blockchain-technology-cm897934>

Other Resources

- [Bitcoin: A Peer-to-Peer Electronic Cash System](#)
- [Digital Chamber of Commerce](#)
- [NASCIO “Blockchains: Moving Digital Government Forward in the States](#)
- [MIT](#)
- [Illinois Blockchain Initiative](#)
- [CompTIA “Understanding Emerging Technology Blockchain Research Brief](#)
- [Congressional Blockchain Caucus](#)
- [Nakamoto White Paper](#)
- [World Economic Forum “Realizing the Potential of Blockchain a Multi-Stakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies” June 2017 White Paper](#)
- [Austin Blockchain Collective](#)
- [GSA U.S. Emerging Citizen Technology Atlas](#)

Books

- Blockchain: Blueprint for a New Economy. Melanie Swan. O’Reilly publishing. ISBN: 13: 978-1491920497
- Mastering Bitcoin. 2nd Edition. Andreas M. Antonopoulos. ISBN: 978-1491954386
- Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. Mark Gates. ISBN: 1547090685

Appendix D

Glossary of Terms



Blockchain: A method for recording transactional information. Rather than keeping a record of all transactions in a central location, blockchain utilizes a distributed ledger. For a given activity, a copy of the full ledger with all transactions is kept on each node in a distributed network.



Block Height: The number of blocks connected together in the blockchain. The first block is considered the “genesis” block.



Chain Linking: Connecting two blockchains together, allowing communication and transactions to occur.



Consensus: A process used to achieve agreement on the accuracy and value of the data in a distributed ledger, while enabling the acceptance or rejection of changes across the network.



Cryptographic Hash: The digital fingerprint of data.



Cryptography: The conversion of data into a secret code for transmission over a public network.



Cryptocurrency: A digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.



Distributed Ledger: A digital system for recording, storing and sharing data across multiple nodes, with no centralized database or storage.



Node: Any computer that connects to the blockchain network and tests/validates transactions.



Permissionless, or Publicly, Distributed Ledgers: Enables all participants with a node on the network to contribute data to the network, with all participants possessing an identical copy of the ledger. Best used when there is little to no trust between the participants.



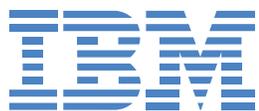
Permissioned, or Privately, Distributed Ledgers: Enables only pre-selected, trusted participants access to the ledger. Only trusted participants can verify new content. Best used for inter/intra organizational transactions.



Smart Contracts: A computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts do not need third parties to validate their accuracy or authenticity.

Acknowledgements

CompTIA would like to thank the important contributions to this guide made by the following organizations:





Public Advocacy Office

515 2nd Street, NE
Washington, DC 20002
United States

202-503-3629

CompTIA.org