OVERVIEW OF BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY FOR STATE GOVERNMENT FUNCTIONS

Distributed ledger technology is a decentralized approach to manage information and transactions. Blockchain, the distributed ledger on which the cryptocurrency Bitcoin is built, is the most notable example of distributed ledger technology. According to the National Association of State Chief Information Officers, blockchain technology is a new and growing capability for initiating, recording, and verifying transactions instantaneously.

Distributed ledger applications are used to process financial transactions, monitor supply chains, and make cross-border payments in the private sector. Several states have explored the potential of using this technology in the public sector. According to states that have studied implementing blockchain for state government functions, the technology has potential to be useful in the future, but some challenges must be overcome. Some of these challenges are related to the relative immaturity of the market for this technology, and others are technological challenges. For instance, the approaches that distributed ledgers use to verify transactions can be energy-intensive. As the size of ledgers increase, they become less useful for everyday users because of the amount of computing power they require. According to a report by the Illinois General Assembly Blockchain and Distributed Ledger Task Force, distributed ledgers need to be compatible with multiple legacy information technology systems in order to be implemented properly. Ledgers also are highly specific in their application and can make adapting blockchain for new uses challenging, if not financially and technically prohibitive. The Department of Information Resources has conducted an internal pilot of a selection of distributed ledger technologies. The agency found that the current market for distributed ledger technology has not developed sufficiently to warrant state investments at this time.

FACTS AND FINDINGS

- Distributed ledgers are decentralized and distributed data management technologies that are used to maintain a growing list of connected records and keep track of transactions. Each participant within a network has its own copy of the ledger. Any changes to the ledger are updated in all copies of the ledger.
- The phrase blockchain and distributed ledger often are used interchangeably; however, blockchain represents a specific type of distributed ledger in which the data are grouped together and organized in blocks. The blocks are linked to one another and secured using cryptography. Cryptocurrencies such as Bitcoin are familiar examples of blockchain distributed ledger applications.
- The National Association of State Chief Information Officers identified several potential applications for blockchain, including managing property deeds, professional licenses, criminal records, and vital statistics.
- A 2016 report by the State of Vermont recommended against state agencies adopting blockchain because the costs and challenges of implementing the technology outweigh any productivity gains that could be achieved.

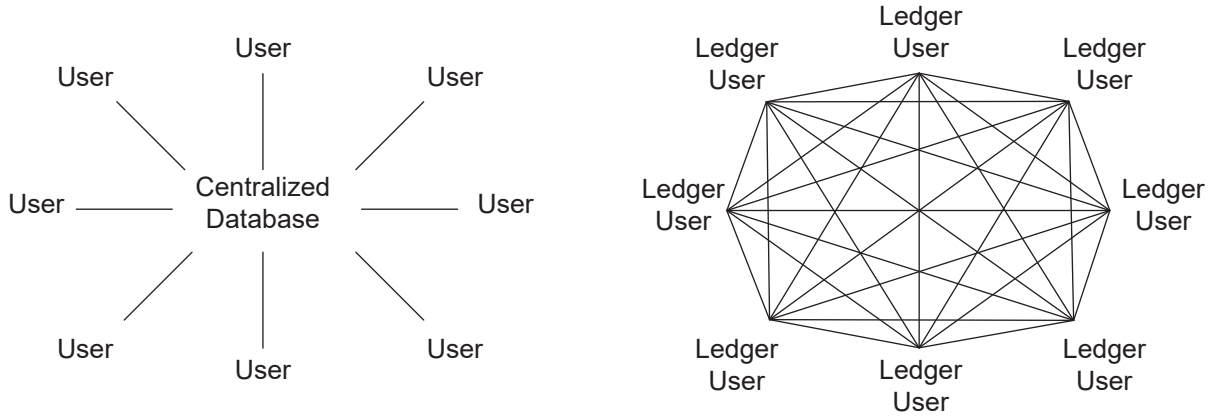
DISCUSSION

In October 2008, Satoshi Nakamoto published *Bitcoin: A Peer-to-Peer Electronic Cash System*. This white paper attempted to identify a technology solution that would enable peer-to-peer commerce with digital currency and without the need for a central authority such as a bank or financial institution to verify transactions. Without a central authority, digital peer-to-peer markets suffered from the double-spending problem. This issue is a potential flaw in a cryptocurrency or other digital cash transaction system whereby the same digital token can be spent more than once, because the token digital file can be duplicated or falsified.

Nakamoto suggested that an electronic payment system based on cryptographic proof would enable willing parties to make transactions without the need for a third party. Cryptography is the process of converting information into a form that only the intended audience can read and process. The technical solution is to develop a ledger that publicly announces each transaction to all market participants, and a system that enables participants to agree on the order in which transactions occurred. The result of this work was the distributed ledger that came to be known as blockchain and included the following components:

- development and maintenance of an electronic register of transactions;

FIGURE 1
DIFFERENCE IN STRUCTURE OF CENTRALLY ADMINISTERED DATABASES AND DISTRIBUTED LEDGERS
FISCAL YEAR 2019



SOURCE: Legislative Budget Board.

- encryption of hashes (digests) of transactions;
- verification of those transactions through a consensus protocol; and
- time-stamping those transactions.

Although the potential uses of cryptocurrencies may be limited, the distributed ledger technology upon which Bitcoin is built has generated interest among various sectors of the economy.

DISTRIBUTED LEDGER TECHNOLOGY

A distributed ledger is a type of database that is held and updated independently by each participant, known as a node, in a large network. This database is different from a standard central database that is held in a central server and to which network participants have access. Instead of networks communicating records to nodes through a central authority, each node processes each transaction independently. Each network has rules for verifying and approving transactions known as consensus protocols. When consensus is reached, the ledger is updated on each node, and the data stored are secured cryptographically. Rules established for or by the network determine whether some or all of the participants can update the ledger. **Figure 1** shows a visual representation of the difference in structure between distributed ledgers and centrally administered databases.

Distributed ledgers can be held and administered publicly or privately. A public distributed ledger is open to the public so that any user can initiate transactions on the ledger. A private distributed ledger can be updated only by members of a single organization. Public and private distributed ledgers can be permissionless or permissioned. A permissionless ledger enables any user to participate in the consensus protocol to validate transactions. A permissioned distributed ledger requires permission from a governing entity to participate in the consensus protocol. Bitcoin uses a permissionless blockchain. An application tracking health records or other confidential information that needs to comply with data protection regulations would use a permissioned blockchain.

Distributed ledgers use different consensus mechanisms to approve and authorize transactions. The Bitcoin application of blockchain uses a consensus mechanism known as proof-of-work. Proof-of-work typically involves using computing power to solve algorithms to deter negative behavior by participants in a network. Proof-of-work assumes that malicious actors will never have a majority of the computing power in a network. If malicious actors do have a majority of the computing power in a network, they can overwrite the ledger. This situation is known as the 51.0 percent problem. The proof-of-work consensus mechanism requires significant computing power and energy consumption, and it is relatively slow at processing transactions. According to testimony provided to the U.S. Senate Committee on Energy and Natural Resources by computer science professor Arvind Narayanan in August 2018, the proof-of-work consensus protocol used by Bitcoin, known as mining, accounted for an estimated 1.0 percent of the world's electricity consumption on August 21, 2018, or slightly more than the electricity

used by Ohio. Bitcoin is the first example, or use case, of a publicly distributed ledger. As a result, the term blockchain has been adopted widely to refer to technologies inspired by Bitcoin that have implemented distributed ledgers.

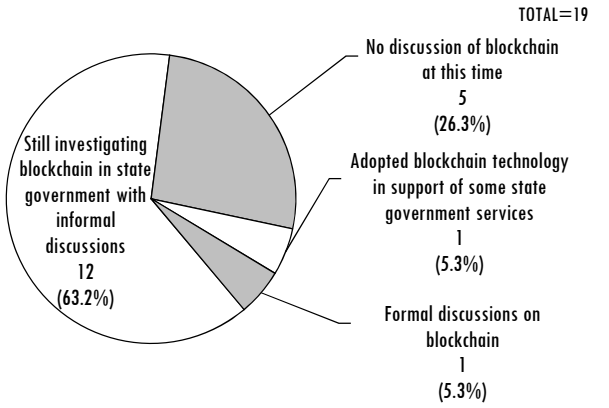
BLOCKCHAIN

Blockchain and distributed ledger often are used interchangeably; however, blockchain is a type of distributed ledger. Distributed ledger technology was intended to process transactions in a shared, trusted environment. Blockchain was intended to facilitate peer-to-peer transactions without the need for a trusted third party.

The characteristic that distinguishes blockchain from other distributed ledgers is that information about transactions—including a time stamp, a digital signature, and relevant information—is grouped together in blocks and then linked cryptographically. One benefit of blockchain is that it eliminates the risk to a centralized database posed by a hacker gaining access to the system and destroying or corrupting the data it holds. Because of this risk, centralized databases depend on administrators to maintain the security of the databases. Blockchain uses cryptographic hashing to save space. Hashing is the encryption of the contents of transactions and some metadata using an algorithm to compile a short digest of the data, known as a hash. A hash cannot be used to replicate the original document or information, but it can be used to verify the original document. Each record has a unique hash.

The blockchain data structure is append-only, which means that data cannot be removed. This structure has been called immutable or tamper-proof. However, it technically is possible to overwrite previous transactions if malicious actors can control a majority of the computing power in the network, which is known as a 51.0 percent attack. According to the management consulting firm McKinsey & Company, control of a majority of computing power in a network by malicious actors is considered largely impractical. However, there has been an increase in these types of attacks on cryptocurrencies during calendar year 2018. Although the blockchain is protected by immutable data structures and cryptography, the overall security of the blockchain system depends on the applications that are built to work with it. For example, the user interface for the system and databases are stored off-chain. Most of the software that is implemented to support a blockchain does not operate directly on the blockchain. Blockchain stores hashes, not documents. Other technology solutions are needed to work with the blockchain to store the records, which can be subject to their own, unique cybersecurity threats.

FIGURE 2
STATE CHIEF INFORMATION OFFICERS RESPONSES TO NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS SURVEY REGARDING BLOCKCHAIN ADOPTION MAY 2017



SOURCE: National Association of State Chief Information Officers.

Blockchain originally was developed as open-source software, which means that the source code was publicly available for other software developers to modify and adapt. This practice has led to many different applications being called blockchain. As a result, no standards for blockchain technologies or the networks that operate them are widely accepted, which presents challenges for assessing the quality of available blockchain solutions and determining how to integrate them. According to McKinsey & Company in 2017, although some large software companies offer blockchain solutions, many of the providers are small start-up companies. For this reason, it is difficult to assess which firms are going to be successful and remain in business long enough to support any information technology (IT) upgrades related to blockchain.

BLOCKCHAIN AND DISTRIBUTED LEDGERS IN STATE GOVERNMENT

In 2017, the National Association of State Chief Information Officers (NASCIO), a national non-profit organization that represents state chief information officers (CIO), surveyed state CIOs about the extent to which blockchain technology is part of each state's agenda. Of the CIOs who responded, a majority said that they were investigating blockchain use in state government through informal discussions. **Figure 2** shows the results of the NASCIO survey.

FIGURE 3
POTENTIAL STATE GOVERNMENT APPLICATIONS OF BLOCKCHAIN TECHNOLOGY
MAY 2017

- Managing property deeds
- Submitting healthcare providers reimbursement
- Evaluating and managing professional licenses
- Administering tickets, fines, and citations, including payments and processing
- Managing birth and death certificates
- Managing microgrid transactions in the energy section
- Managing lineage of patents, trademarks, reservations, and domain names
- Authenticating academic credentials
- Filing and managing insurance claims
- Tax calculations and payment
- Managing, updating, and transmitting criminal records
- Managing, updating, and transmitting healthcare records
- Recording and reporting financial transactions and financial statements
- Managing voting in elections

SOURCE: National Association of State Chief Information Officers.

Many of the government use cases that are being evaluated are functions in which the government serves as the trusted holder of an official record, such as a property record. NASCIO has identified several areas in which the use of blockchain technology could assist with monitoring or making transactions. **Figure 3** shows potential government applications for blockchain technology that NASCIO identified.

NASCIO suggests that governments should consider whether using blockchain is appropriate for a particular program. For example, blockchain theoretically could be useful for managing grants, but many applicants for grant programs already face technological or financial impediments that make their participation in a blockchain unlikely.

According to NASCIO, states initially should focus any blockchain or distributed ledger efforts on a permissioned network, so that a restricted number of users have the rights to validate transactions. This requires decisions about the network to be overseen through governance rather than through energy-intensive, permissionless blockchain that has limited scalability.

A 2018 report by the Brookings Institute, a nonprofit, public policy organization, assessed each state's level of engagement with blockchain technology and cryptocurrency. It found that some states, such as Illinois, envision a broader role for blockchain in their economies. Other states, including Texas, are taking a more reserved approach to research and adoption.

BLOCKCHAIN EVALUATION IN OTHER STATES

According to the National Conference of State Legislatures (NCSL), in 2018, three states—Colorado, Connecticut, and Wyoming—passed legislation; two other states, New York and Virginia, filed legislation to establish working groups to study issues related to implementing blockchain in state government. Illinois and Vermont previously had blockchain and distributed ledger working groups. The working group in Illinois has been supportive of the potential for blockchain technology. Vermont published its results in 2016 and recommended against state agencies adopting blockchain technology because the likely costs associated with adoption exceed the potential benefits.

House Joint Resolution 25, One-Hundredth Illinois General Assembly, 2017, established the Illinois General Assembly Blockchain and Distributed Ledger Task Force to study the following factors:

- opportunities and risks associated with using blockchain and other distributed ledger technologies;
- types of blockchain, public and private;
- projects and use cases from other state and national government entities that Illinois should consider;
- how current state laws could be modified to support this technology;
- encryption technology, including Illinois' digital signature infrastructure, and
- official reports and recommendations from the Illinois Blockchain Initiative.

In 2018, the Illinois task force published a report of its findings. It found that blockchain technology and its built-in encryption could facilitate highly secure methods for public interaction with government, keeping paperless records,

increasing data accuracy, and providing better cybersecurity protections for Illinois residents. The task force also found that scalability in blockchain technology must improve before government adoption can become widespread.

The task force's findings were positive overall about the potential to use blockchain technology in Illinois state government, particularly to manage real estate records. However, it also identified the following challenges associated with adopting blockchain and distributed ledgers for state functions:

- some consensus mechanisms are energy-intensive;
- as the size of ledgers increase, they become less useful for everyday users;
- ledgers must be compatible with multiple legacy IT systems to be useful, but the ledgers are highly specific in their application and lack flexibility that can make adapting blockchain for new uses challenging, if not financially and technically prohibitive;
- hundreds of blockchain technologies are unique variations on the open-source technology, of which each has its own proprietary standards and protocols that may cause compatibility issues between systems; and
- information entered onto a public ledger is permanent, and no mechanism removes information that is entered inappropriately or illegally after it is approved by the consensus mechanism.

A 2016 report by the Vermont Secretary of State, Attorney General, and Department of Financial Regulation found that blockchain provides a reliable way of confirming the party submitting a record to the blockchain, the time and date of its submission, and the contents of the record, which can eliminate the need for third-party intermediaries in certain situations. The report also found that blockchain is limited because the blockchain does not verify or address the reliability or the accuracy of the contents, nor does it provide storage for the records. The report recommended against state agencies adopting blockchain technology because the likely costs associated with adoption exceed the potential benefits.

According to the Department of Information Resources (DIR), as of May 2018, no state agencies in Texas were using blockchain or distributed ledger technology for state functions. DIR used existing agency resources to fund an internal distributed ledger pilot project to track permissions for internal applications. The goal of the project was to familiarize DIR staff with using distributed ledger technology. Although DIR is optimistic overall about the potential of distributed ledger technology, the agency advises that the current market for distributed ledger technology has not developed sufficiently to warrant state investments at this time.

DIR provides guidance to state agencies that explore blockchain applications. DIR suggests that any agency exploring the use of blockchain consider the following questions:

- Does the agency need a structured central repository?
- Are multiple entities accessing the database?
- Does the agency need to ensure trust?
- Would centralized administration be inefficient? and
- Can business rules be automated?

If the agency answers yes to each question, DIR advises the agency to consider whether transactions need to be private (permissioned) or public (permissionless).