JUNE
2019

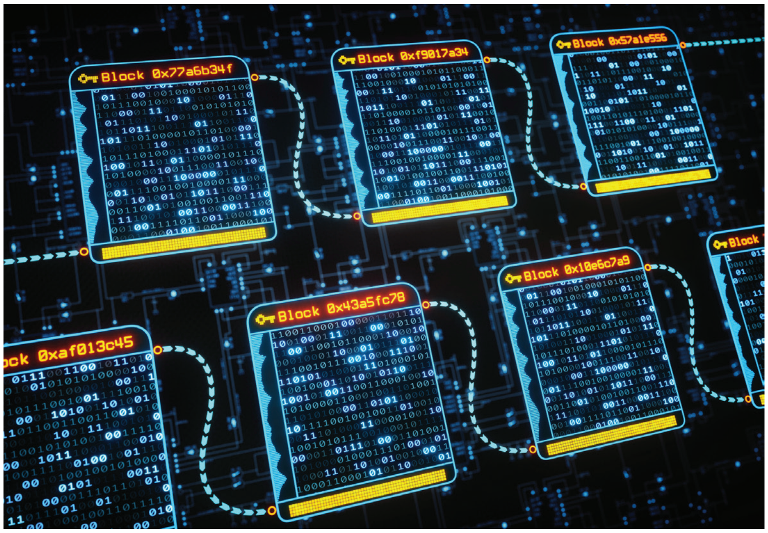
policy matters
california senate OFFICE OF RESEARCH

# ISSUE PRIMER—BLOCKCHAIN TECHNOLOGY

In 2008, a paper published online pseudonymously under the name Satoshi Nakamoto proposed a new type of currency called Bitcoin.[1] Unlike traditional currency, consisting of coins and bills backed by a central bank, the new currency would be entirely digital. It could be exchanged like any other currency, without having to rely on an intermediary. Individual users would be able to manage currency they own through a digital "wallet," a private password that proves they own the currency, while everyone would have a copy of a master ledger that keeps track of all transactions made with the currency. The supporting technology ensures that the ledger remains accurate and that no individuals can spend currency they do not have.

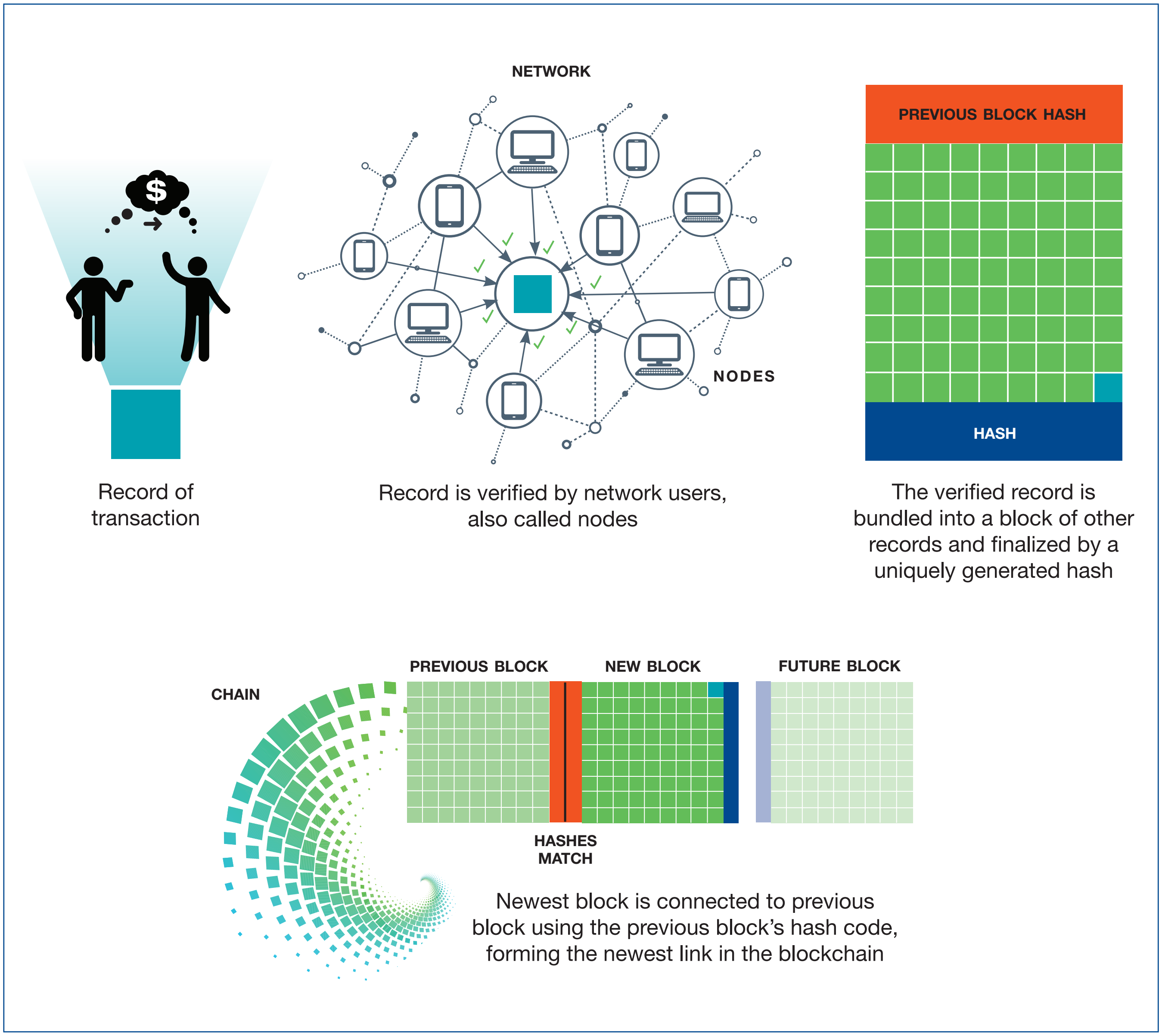
Bitcoin eventually would grow in popularity and oscillate wildly in value; however, the underlying technology that supports its existence, called blockchain, would attract attention for its potential in much more wide-ranging applications. A blockchain is a growing list of records, stored digitally using cryptography, which is virtually impossible to modify while being transparently accessible to network users. Because of this, blockchain supporters have proposed using it to transform a variety of sectors, such as energy, elections, and tax collection. At the same time, some critics of the technology have pointed out unanswered questions and concerns about its use.

As interest in blockchain has grown, some governments around the country have implemented pilot programs or begun studying its implications or potential applications for government functions, including the risks and challenges it presents. In California, legislation enacted in 2018 requires the formation of a new working group composed of public and private representatives to report to the Legislature by July 2020 with an assessment of blockchain for use by state government and California-based businesses.



As an introductory primer on blockchain technology, this brief explains what it is, how it works, some of its potential applications, and how other states are taking steps to explore the emerging technology.

## Figure 1
## How a Blockchain is Formed



Record of transaction

Record is verified by network users, also called nodes

The verified record is bundled into a block of other records and finalized by a uniquely generated hash

Newest block is connected to previous block using the previous block's hash code, forming the newest link in the blockchain

Source: Generated by the Senate Office of Research from information provided by Reuters.[2]

## WHAT IS BLOCKCHAIN, AND HOW DOES IT WORK?

Put simply, a blockchain is a database of records shared across a network of computers. As seen in Figure 1, the database is formed from single records (for example, financial transactions) that are checked and validated by the network users—called nodes. Once a transaction record is accepted by the nodes, it is bundled with other validated transactions into a block, which is given a uniquely generated hash.[i] A hash can be thought of as a block's label—each block's hash will be uniquely determined by the data contained within the block. If even one bit of data in a block is changed (for example, changing "1" to "2"), the newly generated hash will not resemble the

[i] A hash is a mathematical function that takes an arbitrary amount of data (such as text) and maps it to a string of characters of fixed length. For an ideal hash function, a user can verify that a piece of data results in a given hash, but it is infeasible to recreate that data if a user is given only the hash.

old hash in a meaningful way. The block is then added to the chain by linking to the previous block via its hash code. The next block requires the most recent block's hash code to be added to the chain, forming a database that documents the entire transaction history.

A blockchain can be public, where any users can participate in the network as long as they can pass tests to prove their ability to solve complex mathematic problems. However, a blockchain also can be private or "permissioned," wherein an administrator grants users—typically company employees or department staff—access to the network.[2]

## WHY IS BLOCKCHAIN USEFUL TECHNOLOGY?

In a conventional database, transaction records are secured in a central location such as a server. Blockchain offers an alternative to this model with a network of distributed ledgers. Instead of one central authoritative record of all transactions or information, blockchain creates an unlimited number of identical records across a network that can include users all over the world, making the records open and transparent. The decentralized aspect of blockchain makes it very difficult to hack because there is no single point of access and information cannot be gained or controlled from a single computer or server.[3]

A blockchain is very difficult to alter. After a block of data is finalized and a hash is generated, any user attempt to change a detail of the block's record—no matter how minor—would generate a new hash for the block, which breaks the connection to the next block in the chain. Essentially, a hacker would need to recalculate every hash in the chain to modify a record, which would take an enormous amount of computing power and would be evident to other nodes within the system. A potential hacker would have to take control of more than half of the computers in the network to alter a block since 51 percent of the nodes must verify

### Figure 2
### Select Actions From State Legislatures Related to Blockchain Technology

**Regulatory Legislation**

- Defines blockchain technology components, terms, and transactions (Arizona, New York, Wyoming, Vermont)
- Prohibits the regulation or taxation of blockchain technology (Illinois, Nebraska, Nevada, Wyoming)
- Prohibits mandatory electronic firearm tracking technology using blockchain (Arizona, Missouri, Tennessee)
- Defines and authorizes the use of smart contracts (Arizona, Ohio, Nebraska, New York, Tennessee)

**Record-Keeping Legislation**

- Provides specific authority to state corporations and businesses to create and maintain records using blockchain (California, Delaware, Maryland, New Jersey, Wyoming)
- Authorizes state departments to study and implement the use of cryptology and blockchain for state records (Colorado, Vermont)

**Voting Legislation**

- Directs state departments to study and evaluate blockchain technology use in various aspects of elections (Maine, New York)

See page 6 for further information about voting applications

**Supply Chain Tracking Legislation**

- Develops blockchain technology to track and certify the cultivation, manufacture, and sale of marijuana (Colorado: these bills did not pass)

**Crime Legislation**

- Expands the definitions of forgery and counterfeiting crimes to include altering a record using blockchain (Michigan)
- Expands the definitions of forgery and counterfeiting to include altering a record using blockchain (Michigan)
- Adopts a "Virtual Currency Money Laundering Act," which defines and protects blockchain technology from unlawful transactions (Nebraska)

**Legislation Establishing Working Groups**

- Several states have called for working groups to study and report on the potential implementation of blockchain technology in government operations (California, Connecticut, Hawaii, Illinois, Maine, New Jersey, New York, Vermont, Virginia, Wyoming)

Source: Generated by the Senate Office of Research from information provided by the National Conference of State Legislatures.

Figure 3

Breakdown of the 20-Person Working Group, Appointed by Secretary of Government Operations Agency, Pursuant to AB 2658

**Government**

- State Chief Information Officer (CIO)
- Director of Finance
- CIOs from three other state entities
- One member of the Senate and one member of the Assembly*

**Legal**

- Three appointees with a background in law chosen in consultation with the Judicial Council
- Two appointees from privacy organizations

**Industry**

- Three appointees from the technology industry
- Three appointees from non-technology-related industries
- Two appointees representing consumer organizations

Source: AB 2658 (Calderon), Chapter 875, Statutes of 2018.

* Appointed by Senate Committee on Rules and the Speaker of the Assembly, respectively.

that the resulting record change is valid.[4]

While blockchain's immutability is beneficial as a defense against malicious changes, it also is very difficult to change information for a valid reason, such as an input error. Additionally, security vulnerabilities could be introduced at the point in which the blockchain interfaces with the real world, such as third-party applications. If an app that manages user access to a blockchain ledger or a user's personal key is compromised, few avenues are available to address any fraudulent activity that may occur.

In addition to security, blockchain has potential privacy benefits. In contrast to a traditional system in which a central authority verifies transactions, network users validate the transactions in a blockchain, replacing the need for third-party institutions to provide trust. Since an intermediary is not verifying the transaction, the data from the transaction is not shared with advertising companies, social media networks, or even credit bureaus.[5]

## WHAT ACTIONS HAS CALIFORNIA TAKEN?

The California Legislature has recognized the potential impact of blockchain technology and in 2018 passed two bills addressing the technology. SB 838 (Hertzberg), Chapter 889, Statutes of 2018, provides statutory authority for corporations formed in California to use blockchain to create and maintain corporate records, including the corporation's stock ledger. AB 2658 (Calderon), Chapter 875, Statutes of 2018, is a broader bill that defines blockchain for purposes of state law and establishes a working group (see Figure 3) to evaluate the potential uses of blockchain by state government and California-based businesses, as well as risks, privacy concerns, and legal implications. The working group is expected to be appointed in the summer of 2019 and must report its findings to the Legislature on or before July 1, 2020.

Additionally, local governments have implemented initiatives to utilize blockchain technology to transform traditional services. In May 2018, the Berkeley City Council voted to direct the city manager to evaluate the potential benefits of a pilot program in which the city would issue municipal microbonds using blockchain technology.[6] Supporters of the measure argue that the lower denominational costs of microbonds (typically less than $5,000), combined with the increased transparency of blockchain technology, which would cut out Wall Street middle-men, could allow local citizens to invest directly in their communities in a manner often infeasible with traditional municipal bonds. In the Sacramento–San Joaquin River Delta, a partnership between the nonprofit Freshwater Trust and IBM is piloting a program that combines remote groundwater sensors with blockchain technology to measure and track groundwater usage.[7] Individual water users, such as farmers, would then be able to buy and sell groundwater credits via the blockchain ledger.

# WHAT CAN BLOCKCHAIN DO?

Blockchain's promise of a highly secure distributed digital ledger has led to a number of proposed applications for the technology, some of which already have been adopted in both the public and private sector.

## Current Applications

***Cryptocurrency.*** As discussed in the introduction, blockchain initially was proposed as the underlying technology for the cryptocurrency Bitcoin, the most well-known application of blockchain. Historically, currency has been backed either by a physical commodity, such as gold or silver, or issued and regulated by a central authority such as a central bank, in which case it is known as fiat currency. Fiat currency generally is seen as more stable than commodity-backed currency since the inherent value of a commodity could fluctuate based on its reserves.

Cryptocurrency employs blockchain technology to maintain a distributed ledger that tracks all transactions. Therefore, anyone on the network has a copy of the ledger and can view the full history of currency transactions without relying on a central bank to house and verify it. The transactions are bundled into blocks, each of which contains information on the amount of currency sent and received, as well as the digital signatures of the involved parties, which are used to validate the transaction. When a new block is created, computers across the network confirm its validity. In the case of Bitcoin and many other cryptocurrencies, the validity of the blockchain is maintained by employing a competitive process called "proof of work."

In a "proof-of-work" blockchain, network users compete to validate the newly formed block and add it to the existing chain. Individual users race to solve a complex cryptographic problem that requires a large amount of computing power. The first user to successfully solve it adds the new block to the chain and earns a reward, typically a small amount of coin. This process, called "mining," is the method by which new currency is added into the system. Users without the computing resources to mine new coin must use other currency to buy coin. The total amount of currency available to be mined is capped, and the rewards for mining diminish as the blockchain grows longer, until miners no longer receive new currency for successfully creating new blocks.[ii] In the case of Bitcoin, the proof-of-work algorithm periodically adjusts the difficulty of the cryptographic problem, ensuring that a new block is created approximately every 10 minutes. As the difficulty increases, the amount of computing resources needed to create a new block also increases, effectively restricting the ability to mine Bitcoin to those with access to serious computing power.

Of particular importance when considering the adoption of cryptocurrency is the volatility in value. Using Bitcoin as an example, in January 2017, the value in U.S. dollars of a single Bitcoin was $800 to $900. By the year's end, the value had skyrocketed to an all-time high, hitting its peak value of $19,970.62 on December 17, 2017. Since then, the value of Bitcoin has declined significantly, experiencing several sharp drops in the span of days and weeks, and its value sits at approximately $5,000 per coin as of April 2019.[8]

[ii] While no new currency is added to the system after the maximum amount of currency is mined, successfully creating the new block would still result in the miner receiving transaction fees associated with the transactions bundled in the block.

***Corporate Records.*** At least five states, including California, recently enacted legislation that allows certain corporations registered in those states to maintain corporate records via blockchain technology under specified conditions.[9] Corporations typically are required to maintain a stock ledger that contains records of stockholder names, the number of shares registered to the stockholder, and any issuances or transfers of stock. The security offered by blockchain could help ensure the accuracy of the stock ledger and the appropriate recording of stock transactions.

***Smart Contracts.*** A smart contract is a self-executing agreement in which the terms are programmed into the blockchain itself, where they sit until the contract provisions are met. Once the provisions occur, the nodes validate the terms of the contract and record the result. For example, if person A wants person B to edit her paper, both create a smart contract that will reward person B with payment from person A's wallet upon delivery of edits. The network will enforce the contract without a third party, but the two people involved also can build in a provision that would enlist others in the network to resolve disputes for a fee.[10] As another example, if a father wants to transfer a sum of money to his son's account when his son turns 18, the smart contract would be built based on the son's birthday and the set amount of money to transfer. The system nodes will validate the son's birthday based on a birth certificate, certify when the date of his 18th birthday occurs, and then transfer the money.

## In Development

***Voting.*** The potential security benefits of blockchain technology have led to several proposals to apply it to an array of voting applications, from securely storing voter rolls to allowing voters to record their votes remotely through an app. Ideally, a voting system should be secure from interference from hostile third parties or election administrators and allow voters and auditors to verify the election's outcome. In theory, blockchain's distributed, difficult-to-edit ledger could satisfy the requirements. This is being implemented practically by supplementing the blockchain with biometric identification, using voters' smartphone fingerprint readers and facial recognition to verify votes.

In 2018, West Virginia became the first state to allow certain voters to submit their ballots using blockchain technology. Pursuant to a pilot project initiated by the secretary of state, eligible military personnel registered to vote in two West Virginia counties were able to vote in the 2018 primary election using an app called Voatz, which stores the records using a privately maintained blockchain ledger.[11] After successful postelection security audits, the secretary of state expanded the pilot to eligible military personnel in 24 counties for the 2018 midterm election.[12] According to the West Virginia Secretary of State's Office, 144 eligible individuals voted via Voatz.[13]

Cybersecurity and election experts, however, have expressed skepticism, saying the online platforms are no more secure than other online ballots. They are concerned that blockchain addresses only the security of a cast ballot but does not help to authenticate voters or the security of voters' devices. Others have raised concerns that Internet voting systems cannot be audited with a level of confidence comparable to physical polling places.[15]

***Taxes/Taxation Mechanisms.*** A survey by the World Economic Forum estimated that by 2025 the first government will use blockchain to collect taxes.[16] A blockchain-based tax solution would utilize smart contracts to automate the calculation and payment of certain taxes, with the hope of reducing inefficiencies and the resources required to process these taxes.[17] This is particularly applicable to taxes where self-reporting can be burdensome, such as payroll, employment, or—in the case of most countries outside the United States—value-added taxes (commonly called VATs). While there are great potential benefits in such a system, implementing it would require, among other things, integrating a number of IT systems and reforming laws related to databases and identity.

In November 2018, Ohio became the first state to allow businesses to pay certain taxes using cryptocurrency.[18] The process works by businesses registering on the state's online portal and then paying their applicable taxes using funds in their cryptocurrency wallets. Ohio uses a third party to process the payments and convert the cryptocurrency into dollars, which are then deposited into the state's accounts.[19] Online retailer Overstock stated in January 2019 that it planned to pay its Ohio state business tax using this method of payment.[20] To protect against cryptocurrency's potential volatility, Ohio's processor sets an exchange rate that is valid for 15 minutes for each transaction. This process benefits businesses because the transaction fee is 1 percent versus the 2.5 percent fee assessed on credit cards.[21] Ohio plans to extend this service to individuals in the coming years.

***Digital Identity/Personal Records.*** In a time when massive online data breaches are becoming more common, many are looking to blockchain technology as a potential solution for personal identity management. In theory, individuals could store personal identifying documentation, such as a birth certificate or a driver's license, on a blockchain. Access to the information would then be controlled by the individual, who could give permission to other entities to verify the information. While the security of blockchain would be a main advantage of this approach, the decentralized nature of the technology would be at odds with the need for third-party authorities (i.e., the government) to ultimately validate the information. However, the technology is already being tested in instances where individuals lack any form of identification, such as in refugee camps in Jordan.[22] Beyond traditional identification documents, some companies are developing blockchain platforms to manage medical records, allowing patients to have complete control of their electronic medical records while letting them safely and securely share the information with doctors and hospitals as needed.[23]

***Supply Chain.*** Modern supply chains have become increasingly widespread and complex, leading some to propose blockchain as a potential tool for managing and tracking them. Replacing a traditional supply chain database with a blockchain ledger could increase efficiency and transparency.[24] While modern supply chain management systems can handle the complexities, the greatest potential advantage of blockchain in the supply chain is in traceability, particularly in the food and produce sectors, where the ability of a company to trace a product accurately and react efficiently in the event of contamination is vitally important. For example, in the wake of a large-scale E. coli outbreak in 2018, Walmart began requiring lettuce and spinach suppliers to utilize a blockchain to track the origins of their produce.[25]

***Energy and Grid Management.*** Finally, blockchain advocates have proposed a number of potential applications of the technology in the energy sector, particularly as a way to support the deployment and management of renewable energy. For example, when a renewable energy plant generates a unit of electricity, it is issued a renewable energy certificate from an accrediting body, which can be sold on the energy market, allowing for the tracking of renewable electricity once it is fed into the grid and mixes with electricity generated from other sources. A blockchain ledger potentially could be used to track the issuance and trading of renewable energy certificates, preventing double counting and increasing transparency in the energy market.[26]

Blockchain also has been proposed as a tool to assist with the management of microgrids. Microgrids are small networks (e.g., building complexes or neighborhoods) of distributed energy generation resources, such as fuel cells, solar panels, and energy storage, which can operate both in conjunction with the larger grid or as an independent island. Blockchain offers a way for electricity generators and users on a microgrid to buy and sell without relying on a centralized authority, reducing the costs and time associated with performing the transactions. Additionally, blockchain potentially could offer a way to track energy generation and consumption when microgrids interact with the national grid. While blockchain microgrids are still being developed as a concept, a pilot program is being run in Brooklyn, New York, in which neighbors can buy and sell excess energy from one another in peer-to-peer transactions supported by blockchain.[27]

## Conclusion

The state and Legislature may consider several potential applications to enhance or improve the delivery of services to Californians. However, blockchain is still a new technology and needs to be monitored for limitations or complications. As noted earlier, California's blockchain working group, as mandated by AB 2658, is required to complete its assessment and report its findings to the Legislature by July 2020. Upon receiving this information, the Legislature will in a better position to consider any future large-scale blockchain initiatives.

# Endnotes

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008, https://bitcoin.org/bitcoin.pdf.

[2] Maryanne Murray, “Blockchain Explained,” Reuters Graphics, June 15, 2018, http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html.

[3] Curtis Miles, “Blockchain Security: What Keeps Your Transaction Data Safe?” IBM, December 12, 2018, https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/.

[4] Lotte Schou-Zibell and N. Phair, “How Secure is Blockchain?” *World Economic Forum*, April 20, 2018, https://www.weforum.org/agenda/2018/04/how-secure-is-blockchain/.

[5] Steven Johnson, “Beyond the Bitcoin Bubble,” *New York Times*, January 16, 2018, https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html?auth=login-smartlock.

[6] Romy Varghese, “Blockchain Municipal Bond Plan Inches Forward With Berkeley Vote,” *Bloomberg*, May 2, 2018, https://www.bloomberg.com/news/articles/2018-05-02/blockchain-municipal-bond-plan-inches-forward-with-berkeley-vote.

[7] “State of California Tackles Drought with IoT & Blockchain,” February 8, 2019, https://www.prnewswire.com/news-releases/state-of-california-tackles-drought-with-iot--blockchain-300792331.html.

[8] Bitcoin prices were pulled from historical data available on *Yahoo! Finance*, on March 27, 2019, https://finance.yahoo.com/quote/BTC-USD?p=BTC-USD.

[9] National Conference of State Legislatures, “Blockchain State Legislation,” July, 10, 2018, http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx#2018Legis.

[10] U.S. House of Representative, “2018 Joint Economic Report,” ch. 9, p. 214, https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf.

[11] Office of the West Virginia Secretary of State, September 20, 2018, https://sos.wv.gov/news/Pages/09-20-2018-A.aspx.

[12] Office of the West Virginia Secretary of State, https://sos.wv.gov/elections/Pages/MobileVote.aspx.

[13] Office of the West Virginia Secretary of State, https://sos.wv.gov/news/Pages/11-15-2018-A.aspx.

[14] Jesse Dunietz, “Are Blockchains the Answer for Secure Elections? Probably Not,” *Scientific American*, August 16, 2018, https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/.

[15] Terry Nguyen, “West Virginia to Offer Mobile Blockchain Voting App for Overseas Voters in November Election,” *Washington Post*, August 10, 2018, https://www.washingtonpost.com/technology/2018/08/10/west-virginia-pilots-mobile-blockchain-voting-app-overseas-voters-november-election/?utm_term=.a7be97fb8341.

[16] Global Agenda Council on the Future of Software and Society, “Deep Shift: Technology Tipping Points and Societal Impact,” *World Economic Forum*, September 2015, p. 7, http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[17] “Blockchain Technology and Its Potential in Taxes,” *Deloitte*, https://www2.deloitte.com/pl/en/pages/tax/articles/blockchain-technology.html.

[18] Paul Vigna, “Pay Taxes with Bitcoin? Ohio Says Sure,” *Wall Street Journal*, November 26, 2018, https://www.wsj.com/articles/pay-taxes-with-bitcoin-ohio-says-sure-1543161720.

[19] Office of the Ohio State Treasurer, Cryptocurrency Tax Payment Portal, https://ohiocrypto.com.

[20] http://fortune.com/2019/01/03/ohio-bitcoin-overstock/.

[21] Office of the Ohio State Treasurer, Cryptocurrency Tax Payment Portal, Frequency Asked Questions, https://ohiocrypto.com/faq.

[22] Rajaa Elidissi, “Here’s How Bockchain May Replace IDs in the Future,” *CNBC*, May 13, 2018, https://www.cnbc.com/2018/05/10/blockchain-refugees-identity-wfp.html.

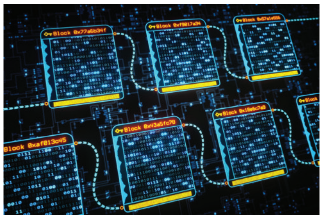
[23] Mike Miliard, “Blockchain Use Case: Electronic Health Records,” *Healthcare IT News*, December 14, 2018, https://www.healthcareitnews.com/news/blockchain-use-case-electronic-health-records.

[24] Bernard Marr, “How Blockchain Will Transfer the Supply Chain and Logistics Industry,” *Forbes*, March 23, 2018, https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#6fab35035fec.

[25] Michael Corkery and N. Popper, “From Farm to Blockchain: Walmart Tracks its Lettuce,” *New York Times*, September 24, 2018, https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html.

[26] Mike Orcutt, “How Blockchain Could Give Us a Smarter Energy Grid,” *MIT Technology Review*, October 16, 2017, https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid/.

[27] “Brooklyn Microgrid: Blockchain-Enabled Community Power,” *Power Technology*, April 11, 2017, https://www.power-technology.com/digital-disruption/blockchain/featurethe-brooklyn-microgrid-blockchain-enabled-community-power-5783564/.



**Written by Sara Noceto and John Thompson.** The California Senate Office of Research is a nonpartisan office charged with serving the research needs of the California State Senate and assisting Senate members and committees with the development of effective public policy. The office was established by the Senate Rules Committee in 1969. For more information, please visit **sor.senate.ca.gov** or call **(916) 651-1500**.