FEBRUARY 2017

DIGITAL MCKINSEY

Using blockchain to improve data management in the public sector

It's not just for financial institutions; government agencies can use this digital ledger technology to protect trusted records and simplify interactions with citizens.

Steve Cheng, Matthias Daub, Axel Domeyer, and Martin Lundqvist

An important function of government is to maintain trusted information about individuals, organizations, assets, and activities. Local, regional, and national agencies are charged with maintaining records that include, for instance, birth and death dates or information about marital status, business licensing, property transfers, or criminal activity. Managing and using these data can be complicated, even for advanced governments. Some records exist only in paper form, and if changes need to be made in official registries, citizens often must appear in person to do so. Individual agencies tend to build their own silos of data and information-management protocols, which preclude other parts of the government from using them. And, of course, these data must be protected against unauthorized access or manipulation, with no room for error.

Blockchain technology could simplify the management of trusted information, making it easier for government agencies to access and use critical public-sector data while maintaining the security of this information. A blockchain is an encoded digital ledger that is stored on multiple computers in a public or private network. It comprises data records, or "blocks." Once these blocks are collected in a chain, they cannot be changed or deleted by a single actor; instead, they are verified and managed using automation and shared governance protocols. (See sidebar "Capturing value from blockchain technology.")

So far, banks, payment-service providers, and insurance companies have shown the highest level of interest and investment in blockchain.[1] But we believe government agencies have just as much to gain from experimenting with this technology and deploying it strategically through pilot projects. Over time, blockchain can help agencies digitize existing records and manage them within a secure infrastructure, allowing agencies to make some of these records "smart." IT departments in government agencies may be able to create rules and algorithms, for instance, that allow data in a blockchain to be automatically shared with third parties once predefined conditions are met. In the longer term, the technology may even allow individuals and organizations to gain direct control over all the information the government keeps about them. This level of transparency could, in turn, make it easier for agencies to achieve buy-in for the creation of networked public services.[2]

Finding advantages in blockchain

There are a number of blockchain tools and technologies that government agencies can implement today to protect critical data and improve the management of records associated with property ownership and incorporation. In the long term, as blockchain matures, governments may also use it to enable networked public services.

Managing data and digital assets

Protection of critical data. Anyone who uses public services is rightly worried that, despite agencies' best efforts to protect their systems, criminals might gain access to government databases and steal or manipulate records.

Capturing value from blockchain technology

The core innovation of blockchain is that it allows for decentralized verification of any information added to an encoded digital ledger. The ledger extends across a network of computers and servers. There is no central agent that decides if a change to the blockchain is legitimate. Instead, all the computers in the network follow a protocol to independently verify transactions and generate automated consensus on the acceptance or rejection of a change.

This verification process, along with modern encryption methods, can effectively secure the data on blockchain ledgers against unauthorized access or manipulation. Because the existing "blocks" in the chain can never be overwritten, users always have access to a comprehensive audit trail of activity. Additionally, decentralized storage of information reduces the risk that users will not be able to get the data they need when they need it—there is no single point of failure.

Of particular interest to public-sector agencies, the use of blockchain may result in the following:

Tamperproof records. Users of a blockchain database could easily reconstruct when a change to the ledger occurred, what information was modified, and where in the network the change originated.

Digital ownership and transfer of assets. Agencies could forego paper documents and set up an efficient digital infrastructure to record asset ownership and provide the means to easily transfer information about bills of sale, deeds, and the like.

Smart contracts. Blockchain ledgers can also store contracts in software code, so when predefined external conditions are met, online transactions can kick in. The high level of security afforded through blockchain allows the contracting parties to trust a decentralized execution engine to implement the terms of agreement.

In 2015, for instance, hackers obtained personal details, Social Security numbers, fingerprints, employment history, and financial information for about 20 million individuals who had been subject to a background check by the US government. Encryption methods can never be 100 percent safe, but blockchain technology can make similar breaches a great deal more difficult to achieve.

The nation of Estonia, for example, is rolling out a technology called Keyless Signature Infrastructure (KSI) to safeguard all public-sector data. KSI creates hash values, which uniquely represent large amounts of data as much smaller numeric values. The hash values can be used to identify records but cannot be used to reconstruct the information in the file itself. The hash values are stored in a blockchain and distributed across a private network of government computers. Whenever an underlying file changes, a new hash value is appended to the chain, and this information can no longer be changed. The history of each record is fully transparent, and unauthorized tampering from within or without the system can be detected and prevented. KSI allows government officials to monitor changes within various databases—who changes a record, what changes are implemented, and when they are made. The electronic health records of all Estonian citizens are managed using KSI technology, and the country is planning to make KSI available to all government agencies and private-sector companies in the country.

Digital property ownership. The process of owning and transferring assets—whether physical property or financial instruments—typically involves multiple interactions and a long paper trail. Government agencies could meaningfully cut down on both by digitizing information about asset ownership and storing it on blockchain registers. Consider the emerging use of blockchain technology by the Swedish government. When it comes to real-estate transactions in Sweden, the stakes are high. The cumulative value of all properties in the country is currently more than 11 trillion Swedish Krona, or roughly three times the value of Sweden's GDP. Yet the registration and transfer of properties remain onerous tasks. The country's land-registry authority, Lantmäteriet, is exploring ways to digitize the process. It is prototyping a mobile app that would provide transaction space for sellers and buyers as well as their real-estate agents and banks. A blockchain would record detailed information on the properties being sold as well as each step in the sales transaction. Communications among all the parties in the sale would become more transparent. Paper documentation—typically hundreds of pages long—would become superfluous. When implemented, the app is expected to reduce the time needed to complete a sale from three-to-six months to just a few days, in some cases even hours. (See sidebar "Toward faster real-estate transactions in Sweden.")

The republic of Georgia has indicated that it will test a similar technology, allowing citizens and companies to use a smartphone application to acquire and transfer property titles within a short period of time and at limited cost. The current property-transfer process is manual; applicants can spend up to a day waiting in line at a public registry and pay between $50 and $200 to complete a transaction. According to our analysis of real-estate transactions across all countries in the Organisation for Economic Co-operation and Development, buyers pay at least $3.5 billion a year in administrative fees to register

Toward faster real-estate transactions in Sweden

The Swedish government is piloting a blockchain database intended to significantly streamline real-estate transactions. The database would allow for trusted digital verification of purchasing contracts, bills of sale, mortgage deeds, and other critical documents. It could also shorten the time between the writing of a purchase contract and the final registration of the asset transfer from months to days, and, in some cases, hours, while also reducing the risk of errors and fraud.

Lantmäteriet, the Swedish land-registry authority, would provide a mobile app that all the parties to a real-estate transaction could use to exchange information, sign legally binding documents, and perform necessary property checks—all organized into a work flow that can be completed quickly. The application would communicate with blockchain-enabled databases on the back end of the land-registry authority's IT architectures. The digital ledger would record each step of a real-estate transaction as well as the property titles themselves. Bank representatives and real-estate agents would have direct access to Lantmäteriet systems; and secure information would always be up to date and just a click away. This would help reduce processing time and legwork.

Because contracts and other critical documents would be rendered in digital form and signed digitally, there would be no need to create multiple paper copies, mail them, and then wait for signatures and responses. Everyone involved could retain a copy of the purchase agreement on their mobile phones; each copy would have a verification code registered in the blockchain. Since digital signatures would be provided with the same application at several instances, the risk of errors and fraud would be reduced. And Lantmäteriet would be involved in the purchase process throughout, rather than intermittently or at end stages—which could create greater confidence and transparency.

their purchases. Digital processing could significantly decrease the cost of this service to governments; in turn, agencies could pass the savings on to citizens.

An additional benefit of using blockchain to keep track of property ownership is that insiders, too, could be held in check; it would be that much harder for unauthorized government employees to manipulate information. This could lead to more secure property rights in parts of the world where the rule of law is weak and abuse of power is high.

Smart incorporation. The US state of Delaware is in the early stages of creating incorporation services based on blockchain records and smart contracts, rather than paper-based exchanges. The process of incorporation, of course, involves filing the appropriate documents, establishing a separate legal entity, holding organizational meetings, issuing shares, adopting bylaws, and so on. A digital approach to incorporation would benefit, in particular, the growing number of private companies with complicated equity structures, where different shareholders have different rights and obligations. The rules associated with particular investments in a business could be formulated as smart contracts embedded in a blockchain. This blockchain might then be used to automate voting procedures or ensure compliance with rules regarding when and how investors can sell their shares.

Building networked public services

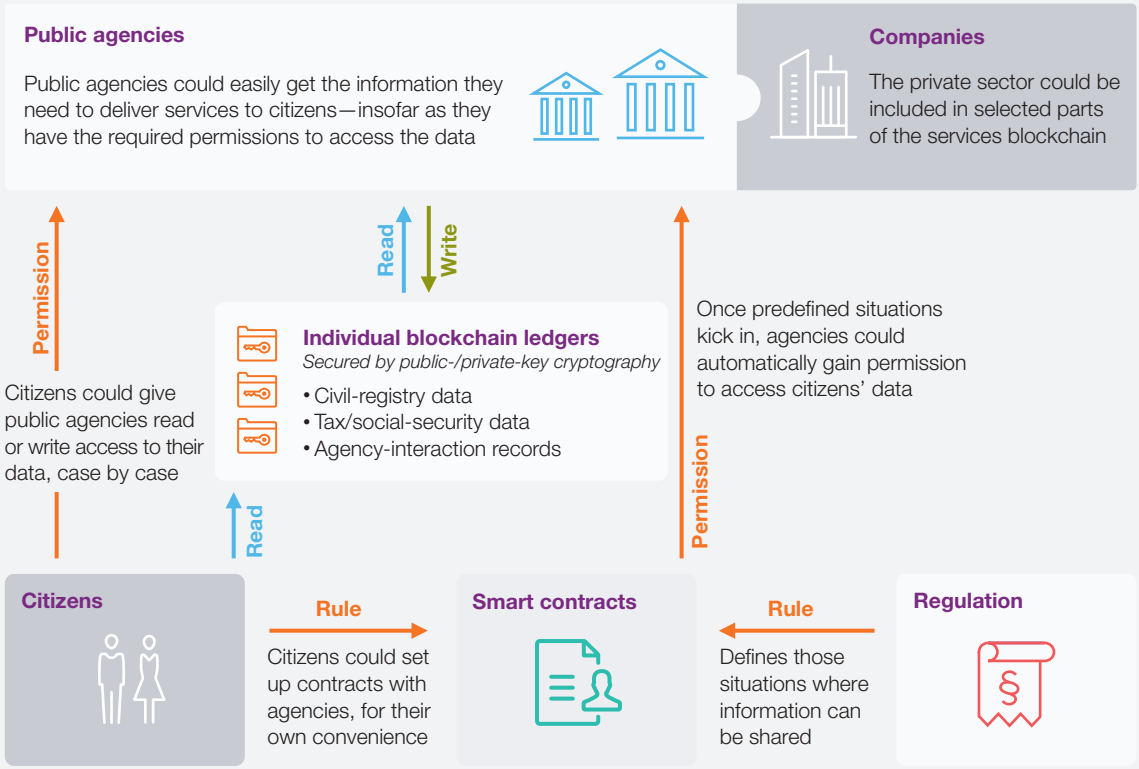
Governments normally know a lot about individuals and organizations because of all the data they collect. Because this information exists in agency and department silos, however, it is often not used to the fullest possible extent.

Agencies that provide social services typically have little or no direct access to information about interactions that a client may have had with other public authorities. And collecting such information can be a painstaking effort, requiring lots of time and legwork. In one Scandinavian country, for instance, civil servants who are responsible for planning rehabilitation programs for convicted criminals spend more than half of their workdays trying to get information about these individuals from different government agencies.

From a technical perspective, there is no good reason for keeping data in silos. With some effort, many governments could create central repositories or enterprise systems for sharing information across agencies. A critical sticking point, however, is security—like their counterparts in the private sector, public agencies cannot, under any circumstances, make sensitive data accessible indiscriminately. What's required is an environment in which data can easily be shared across systems but in which individuals and organizations can take back ownership of their data and control the flow of personal information—who sees it, what they see, and when.

Emerging blockchain technology may support such a scenario (exhibit). Each

Exhibit **Individual blockchain ledgers could let public agencies deliver networked services and citizens control their own data.**



Source: McKinsey analysis

person or organization would have all relevant data about them (basic personal information, for instance, or records of previous interactions with government agencies) stored in a dedicated ledger within an encrypted blockchain database. Individuals or companies could access these ledgers through the Internet. End users could then give government agencies the authority to read or change specific elements of their individual ledger using public- and private-key cryptography.[3] They could use public keys to selectively share information relating to a particular service transaction with agencies. Or they could issue private keys to agencies for one-time "write" access to their data.

In certain situations, smart contracts could expose certain information to designated agencies if predefined conditions are met. If recipients of unemployment benefits are imprisoned, for instance, that information could be transmitted to the labor agency so payments can be stopped for the duration of the sentence. Agencies would be able to use a specific piece of information for the purpose at hand but would not have unlimited access to all of an end user's data.

The use of blockchain ledgers would reduce the risk of unauthorized access (through strong encryption) and data manipulation (through tamperproof audit trails). Indeed, public services could become truly networked, without infringing unduly on privacy rights. Individuals and companies would no longer need to spend a lot of time filling in forms with information they had already provided to the government. And agencies could tailor their services to meet individuals' needs, rather than deploying a one-size-fits-all approach.

Understanding and addressing risks and challenges

Government IT departments that want to adopt blockchain solutions must deal with an industry that is evolving quickly. Venture-capital funds have invested more than $1.2 billion into blockchain start-ups over the past two years alone; about 50 of those start-ups have received more than $1 million each.[4]

Such fast growth presents challenges for IT decision-makers in government. First, there are no widely accepted standards for blockchain technologies or the networks that operate them. Government IT organizations—like everyone else—may therefore have a hard time assessing the quality of available solutions and determining how best to integrate them within their existing IT landscapes. Second, because many blockchain providers are small start-ups, it may be difficult for IT and procurement departments to identify partners with staying power—that is, companies that can offer cutting-edge products but are stable enough to see projects through to implementation.

At the same time, privacy risks will require constant attention. Even if governments could deploy blockchains that share data across public networks (as in the "networked services" scenario described earlier), they would still need to ensure that current and future encryption methods are strong enough to ensure user privacy. Leaders in government agencies will need to understand the legal and regulatory implications of blockchain, among them: To what degree will smart contracts be binding? Can blockchain audit trails be used as evidence in court? Should the use of blockchain be mandatory in certain fields?

How can governments take advantage of the rapid pace of innovation in the blockchain

ecosystem, while dealing with these risks and challenges? One way is by adopting an incubator approach to change. That is, they can establish a small team that *scans* and *prioritizes* opportunities for blockchain pilots and then selects the right *partners* for implementation. This group could be within a government's central digitization office or within the individual authorities that stand to benefit most from blockchain deployment.

An incubator team at the monetary authority of Singapore, for instance, invited scores of blockchain start-ups to present their offerings and capabilities; a handful of these applications were then selected for pilot testing—among them, a payment infrastructure based on blockchain technology that would allow immigrants to send remittances home more quickly and at a lower cost. Lessons from pilot projects can help government agencies address standardization, security, and regulatory issues.

Scan

The incubator team could begin by reviewing ideas for the use of blockchain technology in public administration. The team's scan could focus on processes that, with improvement, could result in a better citizen experience—for instance, streamlining interactions that involve too many manual tasks, cost too much, or take too much time.

Prioritize

The incubator team should investigate the incremental benefits that the use of blockchain technology might provide in each potential area of application. Using blockchain to record votes in an election, for instance, might be more tamperproof than existing digital and traditional voting methods. However, the incremental benefit of switching may not always be big. The team's focus should be on applications that can yield immediate, meaningful results that may prompt more buy-in for blockchain.

Partner

Once priorities have been set, the incubator team can explore partnerships with blockchain providers to create pilot programs. Through these relationships, technology companies have an opportunity to showcase and road-test products while public agencies accelerate their learning about blockchain without having to significantly add internal resources.

Once pilot programs are in place, governments should think about how to build on them. A national road map, for instance, could provide clear guidance to public agencies and blockchain-technology providers alike, about technical standards and interoperability norms. It could include best practices for building capabilities across government agencies and funding the rollout of those blockchain applications that have shown potential in pilot phases. Governments could extend these conversations to include international partners—for instance, setting up a forum like the financial industry's R3 consortium to share lessons from pilot studies, exchange technical templates, or promote global technical standards.

Blockchain technology shows promise for those government bodies that are looking for better ways to manage and protect trusted information. It offers an enticing path toward more efficient operations, more responsive service, and enhanced data security. As early adopters in financial-service industries can attest, however, it will take time for the technology to fully mature. Now is the time for experimentation. By including blockchain in their innovation

agendas—establishing it as a critical component of enterprise architecture—governments will learn what works in practice and how to unlock the full potential of data-driven service. ■

[1] For more, see *Blockchain in insurance—opportunity or threat?,* July 2016, McKinsey.com; and *Beyond the hype: Blockchains in capital markets,* December 2015, McKinsey.com.

[2] This article focuses on the use of blockchain to improve records management. Governments might also use the technology to implement digital currencies and payments.

[3] Public- and private-key cryptography systems use pairs of keys to authenticate and encrypt information that travels between two parties.

[4] *Blockchain: Putting theory into practice,* Goldman Sachs Global Investment Research, May 2016; McKinsey's Panorama FinTech database.

Steve Cheng is a partner in McKinsey's New York office; **Matthias Daub** is a partner and **Axel Domeyer** is a consultant in the Berlin office; **Martin Lundqvist** is a partner in the Stockholm office.

The authors wish to thank Sam Saatchi as well as Matt Higginson, Giuseppe Lacerenza, Dimitri Obolensky, and Peter Braad Olesen for their contributions to this article.