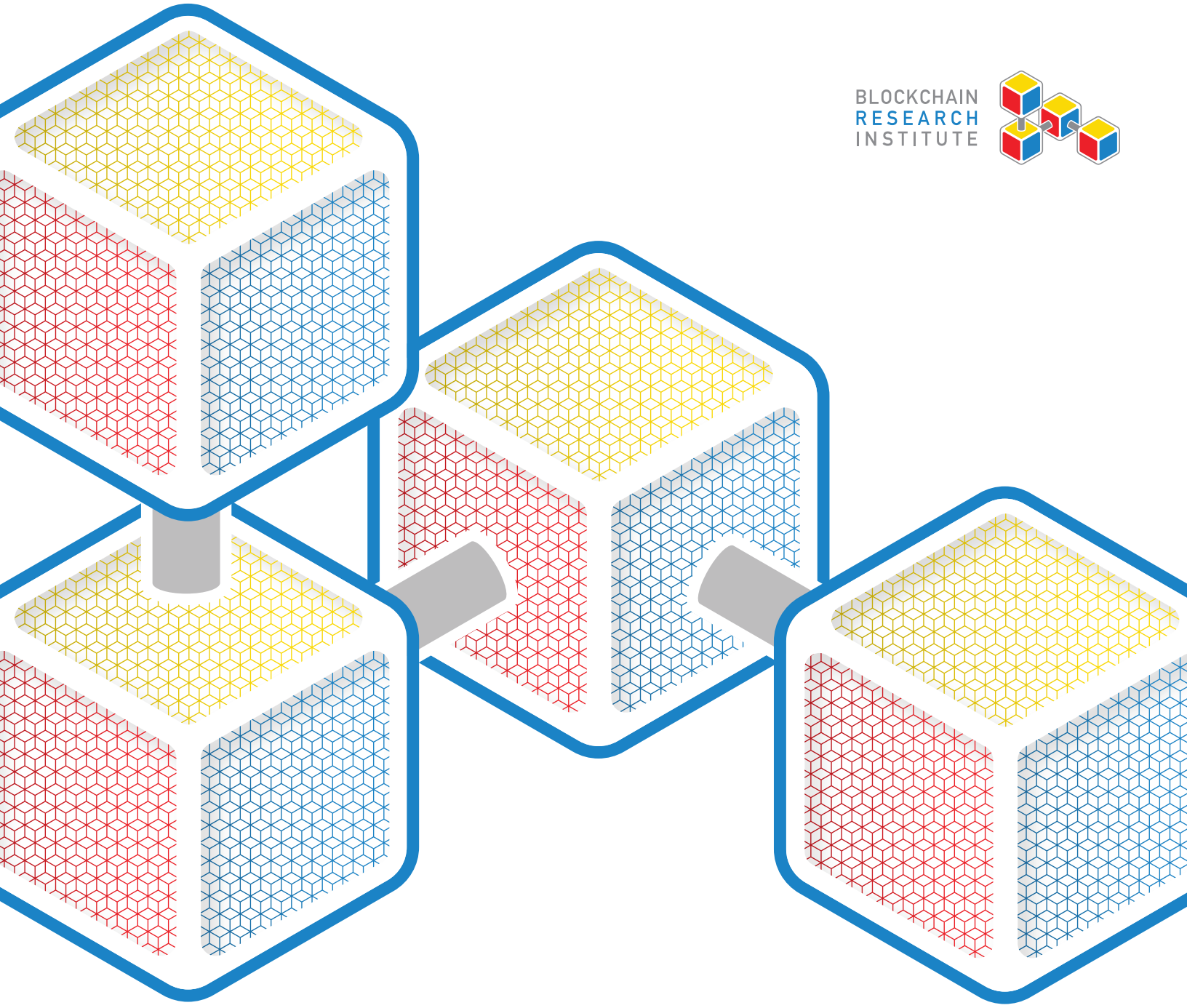
BLOCKCHAIN RESEARCH INSTITUTE



CONSOLIDATING MULTIPLE LEDGERS WITH BLOCKCHAIN

A Single Digital Ledger for the Government of Canada Accounts

Anthony Williams
DEEP Centre

November 2018

A BLOCKCHAIN RESEARCH INSTITUTE LIGHTHOUSE CASE STUDY

Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, "the digital economy," with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

Don and Alex Tapscott launched the Blockchain Research Institute to help realize the new promise of the digital economy. We research the strategic implications of blockchain technology and produce practical insights that will guide our members in achieving success.

Our global team of blockchain experts is dedicated to exploring, understanding, documenting, and informing leaders of the strategies, market opportunities, and implementation challenges of this nascent technology. Research projects are underway in the areas of financial services, manufacturing, retail, energy and resources, technology, media, telecommunications, healthcare, and government as well as in the management of organizations and the transformation of the corporation.

Our findings, conclusions, and recommendations are initially proprietary to our members and are ultimately released under a Creative Commons license to help achieve our mission. Each research publication includes a video introduction by Don and an infographic for members' use in communicating these ideas throughout their organizations. To find out more, please visit www.blockchainresearchinstitute.org.

Leadership team

Don Tapscott – Co-Founder and Executive Chairman
Alex Tapscott – Co-Founder
Joan Bigham – Managing Director, International
Hilary Carter – Managing Director, Canada
Kirsten Sandberg – Editor-in-Chief
Jane Ricciardelli – Director of Marketing
Wayne Chen – Director of Business Development
Maryantonett Flumian – Director of Client Experience
Luke Bradley – Director of Communications

Contents

Foreword

Old models of government are outdated and unacceptable. Engaged citizens expect to be heard and informed—indeed, to be active collaborators rather than passive recipients. They expect elected officials to honor their campaign promises and to spend taxes funds wisely. Blockchain technology makes these goals easier to accomplish.

This case study explores how blockchain can simplify and improve government services in Canada by providing a single digital ledger for all accounts. It assesses the current general ledger system, compares it with best practices in places like Estonia and Sweden, and lays out a proposed blockchain-based solution. The analysis is not cheerleading; it lays out the relevant challenges and implementation costs including managing risk and connecting with existing policies and procedures.

This is the second Blockchain Research Institute document authored by Anthony Williams. Members should also read his "Diamonds on the Blockchain: Building a Global Digital Ledger for Valuable Assets." Anthony and I co-authored two books relevant to the transformation of government and its relationship to citizens: *Wikinomics: How Mass Collaboration Changes Everything* showcased how large groups could mobilize and initiate change; and *Macrowikinomics: New Solutions for a Connected Planet* described how to revive the public square. This project continues those conversations.

DON TAPSCOTT
Co-Founder and Executive Chairman
Blockchain Research Institute

Concept in brief

- From global financial markets to healthcare delivery, blockchain technology is fundamentally changing how we collect, manage, and record information. It is simplifying complex ecosystems, creating trusted and secure repositories of data, and supporting complementary technologies, such as smart contracts and artificial intelligence.
- From Estonia to the United States, jurisdictions are deploying blockchain (also referred to as *distributed ledger*) to power innovations in business registration, identity management, evoting, healthcare services, and international trade.
- This study explores the use of blockchain to consolidate the Government of Canada's multiple ledgers into a single distributed ledger that would increase the integrity of its accounts, boost the efficiency of auditing functions, and reduce its transaction costs.

This study explores the use of blockchain to consolidate the Government of Canada's multiple ledgers into a single distributed ledger.

- As transactions recorded onto the ledger would be instantly searchable and publishable, the blockchain-based ledger could also boost public transparency, fulfill and expedite the receiver general's auditing requirements, and improve the integrity of Canada's accounts.

Overview of receiver general ledger system

The receiver general for Canada is responsible for managing the government-wide treasury, accounting, and reporting functions of the federal government. These activities include controlling all monies drawn from or deposited to the *consolidated revenue fund* and ensuring that all of these transactions are accounted for in the accounts of Canada—Canada's general ledger—and producing the public accounts of Canada.

To ensure that all transactions are reflected in the accounts of Canada, the receiver general implements a control framework, which sees government departments submit monthly, aggregated financial information (including all expenditures and revenues), which the receiver general reconciles against the general ledgers. The control framework is largely based on legacy applications that require human intervention, such as file uploads, verifications, and data refreshing. Some of these operations are highly time-sensitive, and any snag in the process can have severe repercussions.

What follows is a brief overview of the key components of the receiver general control framework, including the central financial management reporting system, the receiver general-general ledger, and the account balance concept.

Central financial management reporting system

The Government of Canada uses a central financial management reporting system to maintain its accounts.

The Government of Canada uses a *central financial management reporting system* to maintain its accounts. This central reporting system compiles a general ledger from the certified trial balances submitted by government departments and agencies at the end of every month. These monthly departmental trial balances contain opening and closing balances for each unique combination of *government-wide coding*, a standardized input record layout needed to maintain Canada's accounts.

The central system performs several key functions:

- Verifying account balances of the control accounts for all departments against the corresponding control accounts in *receiver general-general ledger* (RG-GL) and *payroll systemgeneral ledger* (PS-GL)
- Ensuring that all payroll-related transactions, payments, and money received by departments, including interdepartmental settlements, are accounted for in the books of Canada
- Validating codes submitted by departments in the chart of accounts
- Providing information to central agencies through an ad hoc reporting function.

Receiver general-general ledger

Every day, the receiver general-general ledger provides departments with an electronic file containing all payment and deposit transactions recorded against the control accounts.

The *receiver general-general ledger* (RG-GL) is maintained using the *common departmental financial system* (CDFS). The RG-GL maintains control account balances for all payments, interdepartmental settlement transactions, and deposits processed by the treasury systems for all departments. Every day, the RG-GL provides departments with an electronic file containing all payment and deposit transactions recorded against the control accounts.

Account balance concept

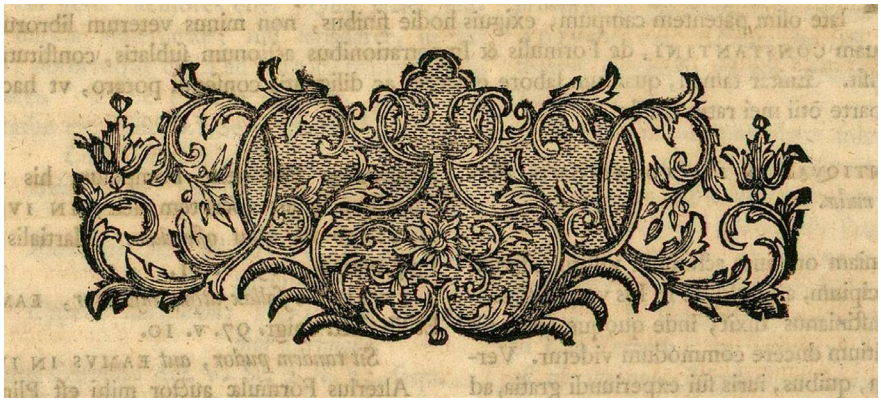
The control account balances maintained by the RG-GL and the PS-GL are a key component of the account balance concept. The RG-GL control account totals are based on data received from the treasury systems and internal journal vouchers for adjustments not processed through the treasury systems. The PS-GL control account totals are based on pay data received from Canada's Phoenix public service payroll system and from internal journal vouchers for adjustments not processed through Phoenix.

Departments are required to perform a periodic reconciliation between the control account balances in the *departmental financial management systems* (DFMS) and the daily control account totals received from the RG-GL and PS-GL. For example, departments receiving internal journal vouchers affecting their control accounts are required to manually upload the data into the related accounts in their DFMS and reconcile their DFMS account balances with the daily control account totals received from the RG-GL and PS-GL.

At month's end, the RG-GL and PS-GL send a final control account balance report to departments, which includes reports and data files containing control data and control account balances.

At month's end, the RG-GL and PS-GL send a *final control account balance report* to departments, which includes reports and data files containing control data and control account balances. Departments must reconcile the control account balances with the corresponding account balances recorded in their DFMS.

The receiver general uses the reconciled trial balances to produce the *monthly statement of financial operations* (MSFO) and the annual public accounts of Canada. If there are errors, omissions, or inappropriate coding in departmental trial balance data that will have a material impact on the results of the MSFO, the receiver general will make the appropriate changes and request that the departments adjust the following month.



Barnabé Brisson, "De formulis et solennibus populi Romani verbis libri VIII," 1755 [SICD] by Paul K, 2008. Used under CC BY 2.0.

Public sector applications of blockchain

A blockchain is an encoded digital ledger stored on multiple computers in a public or private network.

A blockchain is an encoded digital ledger stored on multiple computers in a public or private network. It consists of data records, or "blocks," aggregated into time-stamped chains that cannot be changed or deleted by a single actor; instead, they are verified and managed through automation and shared governance protocols. As a result, blockchain provides an immutable, transparent record of the truth.

Use cases tend to focus on financial services. Government agencies could use blockchain not just for conducting financial transactions and collecting taxes, but also for registering voters, identifying

recipients of healthcare, financial support, and emergency aid; issuing passports and visas; registering patents and trademarks; recording marriage, birth, and death certificates; and maintaining the integrity of government records.

Governments are already exploring blockchain applications for land registry (Sweden), digitizing all public documents (Dubai), and bolstering cybersecurity for identity management and e-voting (Estonia). The US General Services Administration now uses blockchain to automate its public procurement process, and the State of Delaware introduced legislation to allow companies to incorporate using blockchain. This case study explores the deployment of distributed ledger technology for public sector accounting, these use cases are all exercises in simplifying and improving data management in government.

Governments are already exploring blockchain applications for land registry, digitizing all public documents, and bolstering cybersecurity for identity management and e-voting.

Identity management in Estonia

Formed as an independent nation in 1991—just as the public Internet was born—Estonia is a true digital native. Its lack of legacy infrastructure has freed it to build a digitally enabled society and economy from the ground up. Today, the normal services of government—legislation, voting, education, justice, healthcare, banking, taxes, policing, and so on—have been digitally enabled across one platform, wiring up the nation into the most ambitious project in technological statecraft on the planet.

Among the hallmarks of e-Estonia is the blockchain-enabled Estonia ID card, a cryptographically secure digital identity card that unifies access to a mindboggling array of services. Citizens can order prescriptions, vote, bank online, review school records, apply for state benefits, access medical and emergency services, file their taxes, submit planning applications, upload their will, apply to serve in the armed forces, travel within the European Union without a passport, and fulfill around 3,000 other functions with their Estonia ID. Businesses owners can use the ID card to file their annual reports, issue shareholder documents, apply for licenses, and so on. Government officials can use the ID card to encrypt documents; review and approve permits, contracts, and applications; and submit information requests to law enforcement agencies.

Estonia's lack of legacy infrastructure has freed it to build a digitally enabled society and economy from the ground up.

The day-to-day efficiencies for citizens are considerable. Estonia's "once only" data policy dictates that no single piece of information about its citizens should be entered twice. Instead of having to "prepare" a loan application, applicants have their data—income, debt, savings—pulled from elsewhere in the system. There's nothing to fill out in doctors' waiting rooms, because physicians with permission can access their patients' medical histories. When a child is born in the hospital, his or her parents are automatically registered for family benefits. Citizens requiring long-term medication get a digital prescription slip on their medical record, which reduces queues at doctors' offices and hospitals.

In 2016, around 68 percent of the adult population in Estonia used the Internet to send filled forms to the public authorities, which is almost twice the OECD (Organization for Economic Cooperation and Development) average (35.6%).[1] While citizens evidently like the convenience of online services, the savings for government are also significant. Digitizing processes reportedly saves the state two percent of its gross domestic product a year in salaries and expenses.

In 2016, around 68 percent of the adult population in Estonia used the Internet to send filled forms to the public authorities, which is almost twice the OECD average (35.6%).

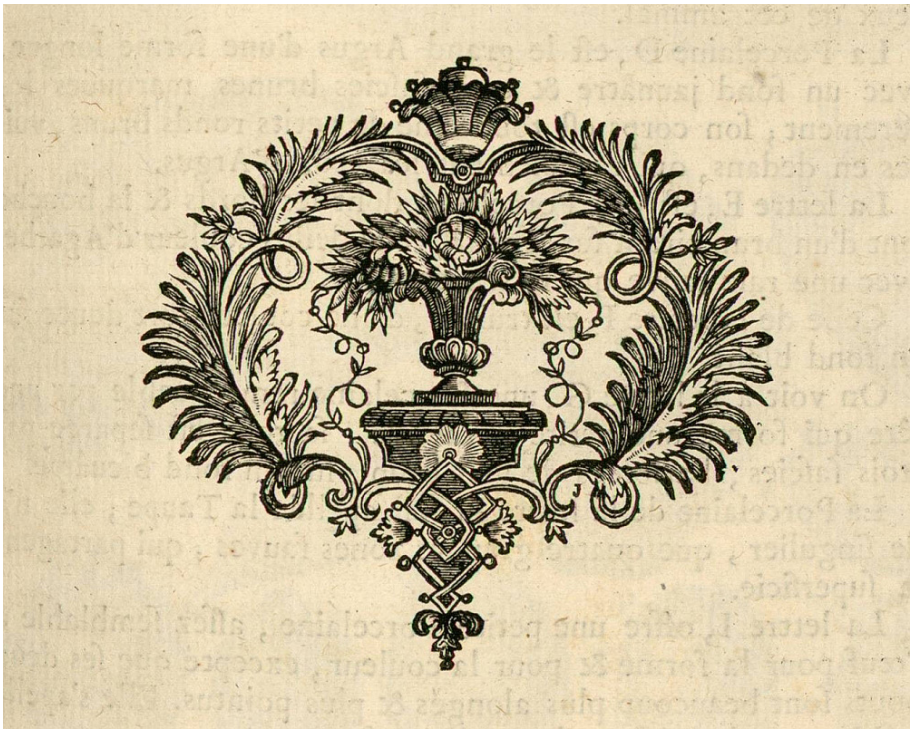
Confident that it could extend these benefits beyond its physical borders, Estonia launched a digital "e-residency" program in 2014, which allows non-resident foreigners to partake of some Estonian services as if they were living in the country. A €100 fee and a successful security check will get users an identity card, a cryptographic key, and a *personal information number* (PIN) to access e-services like business incorporation and banking. Estonia hopes its e-residency program will appeal to entrepreneurs and encourage international start-ups to put down virtual roots. Estonia has the lowest business tax rates in the European Union and has become known for liberal regulations around tech research. As of January 2018, 28,000 people had applied for e-residency (approx. 500 people apply each week), and e-residents own more than 3,200 companies.[2]

Estonia's e-Business initiative has made it easy for both resident and e-residents to start and operate a business in the country: Estonia has one of the fastest growing start-up populations in the world, with 31 start-ups per 100,000 inhabitants, which is six times higher than the European average.[3] Once companies are up and running, they can connect their financial management application programming interfaces (APIs) to the government online, automate reporting for annual tax filings, and reduce the administrative burden on businesses and the public sector.

Blockchain-enabled ledgers provide the underlying data management and security technology for much of Estonia's digital public services. The Estonian ID card, for example, records every piece of data with proof of time, identity, and authenticity—providing a verifiable guarantee that records have not been altered. The Estonian government said the *keyless signature infrastructure* (KSI) that blockchain requires ensures the authenticity of the electronic data stored on its citizens. No one—not hackers, system administrators, and or even the government itself—can manipulate the data and get away with it.

Leveraging the blockchain infrastructure means distributing storage of data, thus reducing the chance of major breaches of centralized databases.

Leveraging the blockchain infrastructure means distributing storage of data, thus reducing the chance of major breaches of centralized databases. Instead, the government's data platform, X-Road, links individual servers through end-to-end encrypted pathways. Information resides locally: hospitals, educational institutions, banks, and government agencies all maintain their own data sets. When a user requests a datum, the system delivers it like a boat through a canal—via locks.



Dezallier d'Argenville, Antoine-Joseph, "Histoire naturelle éclaircie dans deux de ses parties principales, la lithologie et la conchyliologie," Paris, 1742 [SICD] by Paul K, 2009. Used under CC BY 2.0.

A strict system of permissions and privacy safeguards ensures that citizens control who sees or may not see their data. Teachers, for example, can enter student grades but cannot access a student's entire academic history. A file accessible to one medical specialist need not be accessible to other doctors if a patient deems it unnecessary. Few people are able to say exactly who has looked at their medical records. But Estonians can log into their records and see exactly what medical professionals have viewed and acted on. Citizens could challenge and justice departments could prosecute any government official who accessed a citizen's data without permission or a legally valid reason.

Estonia's advances are so well regarded that other governments are importing its innovative models for e-governance.

Estonia's advances are so well regarded that other governments are importing its innovative models for egovernance. Its experts have consulted on Georgia's efforts to set up its own digital registry. Estonia is also building data partnerships with Finland and sharing its methods elsewhere in Europe. "The vision is that I will go to Greece, to a doctor, and be able to get everything," said Sandra Roosna, a member of Estonia's E-Governance Academy and the author of the book *e-Governance in Practice*. "I think we need to give the European Union two years to do cross-border transactions and to recognize each other digitally."[4] Nations as disparate as Moldova and Panama have adopted the Estonian platform. What started in a small Baltic state could soon provide the digital platform for e-governance across Europe.

US GSA and FASt Lane

In fiscal year 2017, the US General Services Administration (GSA) procured over $15 billion in IT equipment, software, and services from more than 5,000 companies on behalf of federal, state, and local government buyers.[5] On average, the GSA took 110 days to onboard a scheduled contractor to deliver services—an exceedingly long time to wait for IT products in today's environment.

A crucial element was to change two steps of the vendor selection and onboarding process: the review of vendor-submitted financial statements and the preparation of pre-negotiation letters.

In recent years, GSA has worked to shave time off the procurement process using a new approach the agency calls FASt Lane, a mash-up of Federal Acquisition Services (FAS) and Integrated Technology Services (ITS). According to Jose Arrieta, director of the General Services Administration's Schedule 70 (IT products and services) operation, "The FASt Lane process can award contracts within 40 days, but only when the requirements are very clear."[6] In 2018, GSA initiated a blockchain-enabled pilot in an attempt shave even more time off the process. The agency anticipates its proof of concept (POC) will bring the FASt Lane review process down to fewer than 10 days.

Currently moving through both the design and proof-of-concept phases, GSA is looking to use blockchain to intelligently automate the most time- and labor-intensive aspects of the FASt Lane contract review process. The agency expects that automation will reduce the amount of human interaction required to review new proposal documents, improving the user experience and speeding the awarding of contracts and onboarding of companies.

A crucial element of GSA's proof of concept was to change two steps of the vendor selection and onboarding process: the review of vendor-submitted financial statements and the preparation of prenegotiation letters.

On the financial review, the traditional process involved a staffer extracting financial information from material the vendor provided and calculating the firm's financial viability. This alone could take up to a month. The blockchain POC accelerated that process so that, in most cases, an automated review is nearly instantaneous. Offers that pass are moved to the next step in the workflow; those flagged are routed to a human reviewer for further analysis.

Automation will not only save time and money but it will free up staff for more valuable activities.

A pre-negotiation letter, meanwhile, is a document listing issues for the GSA to raise in negotiations with a vendor. The blockchain became the system of record for an entire offer, replacing multiple emails back and forth between the government and vendor, and back and forth with the contracting officer checking multiple systems. It has reduced preparation time from 15 to 30 days to fewer than 10 days.

Automation will not only save time and money—possibly lowering the direct costs of analyzing a proposal by close to 80 percent, according to Arrieta—but it will free up staff for more valuable activities. "By automating these business processes, we can lessen the burden on our industry partners, and allow the contracting professionals to focus more on critical thinking tasks rather than the process tasks associated with interacting with multiple systems," said Arrieta.[7]

Accuracy and data integrity are further benefits of using blockchain to mediate transactions, especially when (as GSA does) mediating between thousands of IT vendors and thousands of local, state, and federal buyers. Blockchain provides a cheaper, more flexible, and more accurate platform for handling the procurement process than the traditional system, which required multiple databases. Arrieta said,

Blockchain provides a cheaper, more flexible, and more accurate platform for handling the procurement process than the traditional system, which required multiple databases.

> *In the old system, we had multiple databases with specific data elements and operations that can be performed on them. If one wished to introduce new data elements or new ways to analyze some data, we had to modify the databases. Multiple databases also create risks for errors in data transfer from one database to another.*[8]

With the blockchain solution, vendors and purchasers enter their information once instead of logging onto multiple systems, and there is only one shared ledger and an open application programming interface connecting any user. The applications that leverage the API for any given user's needs can be modified as appropriate without needing to modify the ledger itself. Also, having only one ledger eliminates errors that can creep in when transferring data from one database to another.

Another big benefit of using blockchain is transparency. All of the government's interactions with vendors, such as requests for proposals, recommendations, and decisions, are recorded on the blockchain and viewable by permissioned parties. If an offer is rejected, for example, the information affecting that decision is available for protests and audits. Transparency also offers vendors access to the information in the ledger about them, so that they can detect and report any errors. "We're not going to share multiple industry partners' information with each other," said Arrieta. So-called permissioned blockchains allow distributed ledger managers discretion over who may view data. "But it's one transparent view that multiple stakeholders can see in real time, and it provides a trusted record of all of the interactions with one another."[9]

State of Delaware's blockchain initiative

State officials believe the blockchain ledger has enormous advantages for government and the companies registered in Delaware.

Home to 1.2 million incorporated business entities, a well-established body of corporate law, and a sophisticated business court, the State of Delaware is widely regarded as the corporate capital of the United States, if not the world.[10] In 2016, 81 percent of all new US *initial public offerings* (IPOs) chose to incorporate in Delaware. The state remains the chosen home for more than half of all US publicly traded companies and 67 percent of Fortune 500 companies.[11]

On 1 August 2017, Delaware passed legislation that allowed corporations to use distributed databases and smart contracts to maintain a registry of stock issuances and transfers. State officials believe the blockchain ledger has enormous advantages—cost savings, error avoidance, accuracy of ownership records, and automation of administrative functions—for government and the companies registered in Delaware.

Corporate records will be easy to track and verify, allowing corporations to save significant time and money and avoid costly litigation.

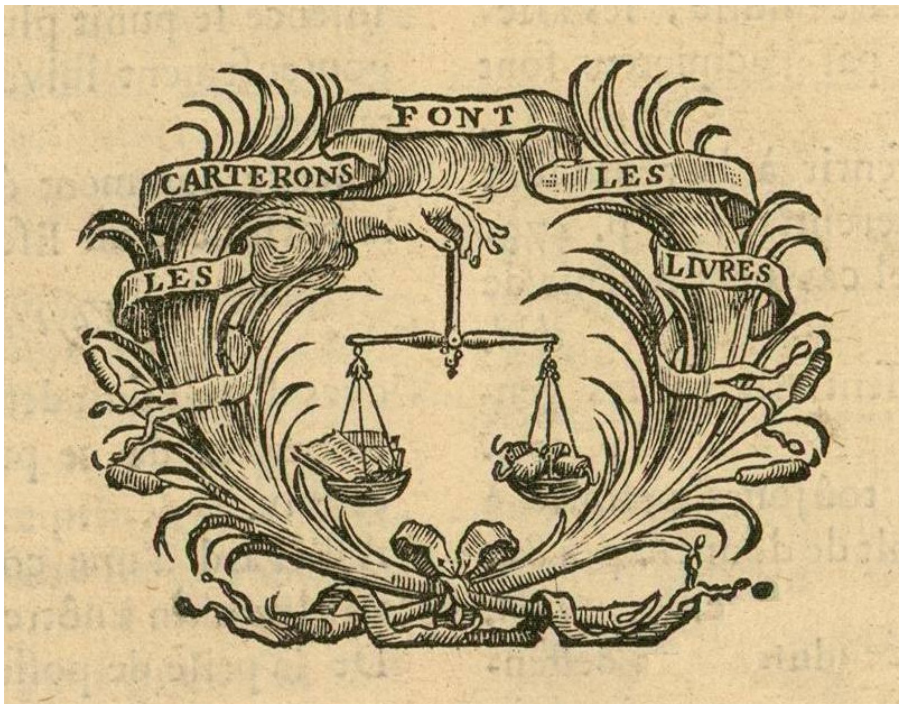
Under the old system, a corporate secretary or transfer agent maintained stock ledgers, manually updating them when shares changed hands. This paper-based system made tracking stock ownership burdensome, particularly as companies grow and change over time. Legal expert John Williams said, "It is a challenge to reconstruct the stockholders at any given point in time, including the exact number of shares held and any restrictions or agreements that apply to those shares, which impacts shareholder voting."[12]

The new Delaware legislation will allow existing corporations to convert their paper-based shares to distributed ledger shares, and new corporations will use electronic records from the outset. Corporate records will be easy to track and verify, allowing corporations to save significant time and money and avoid costly litigation.

How, specifically, will blockchain-based ledgers improve on current practice? The answer lies in the security, immutability, and efficiency of blockchain ledgers.

Currently, most corporate stock ledgers are stored on servers or "in the cloud" on a server network. This makes them vulnerable to hacking by outsiders and to manipulation/data entry error by insiders. Because this system results in a record that is less than fully dependable, companies are required to keep paper copies of documents to mitigate the risks.

In contrast, blockchain technology allows companies to store, manage, and share encrypted data on a distributed database. The



Dantoine, Jean-Baptiste, "Les règles du droit civil," Lyon, 1710 [SICD] by Paul K, 2008. Used under CC BY 2.0.

system uses a vast network of encrypted servers, called nodes, to hold documents or digital signatures of encrypted documents. There is no central repository; instead, the digital assets are widely dispersed on a spiderweb of servers, and available only to those holding encryption keys.

The distributed ledger cannot be edited, even by an individual who holds all of the access keys.

The distributed ledger cannot be edited, even by an individual who holds all of the access keys. The stockholder record can be appended, but retroactive adjustments to the record cannot be made. This process generates a highly dependable audit trail that clearly—and indisputably—indicates how each stockholder acquired stock and from whom. That trail would be essential in court of law, should a plaintiff dispute who the stockholders were at a given moment.

Eliminating paper records is a significant win, but there are potentially even greater efficiencies to be gained by speeding up incorporations, mergers, acquisitions, IPOs, and other sophisticated commercial transactions. Blockchain-based smart contracts, for example, will make it possible to update, delete, and act automatically upon records when specific conditions are met, like option expirations. Other possibilities include automatic updates to reflect name and address changes and amendments to collateral descriptions and secured parties.

Early adopters of blockchain stock ledgers include Medici Ventures and Overstock.com, and there are supporters in the legal community as well. "The technology is potentially incredibly powerful," said John Mark Zeberkiewicz, a partner at Delaware-based law firm Richards, Layton, and Finger. "It can be used to create an immutable record of any number of transactions, not limited to the issue and transfer of shares, but theoretically any transaction that implicates or touches upon in any way the internal affairs of the corporation."[13]

Sweden's land registry

For most countries, keeping track of who owns what pieces of land is still a low-tech affair, involving mountains of hand-signed documents and expensive lawyers.

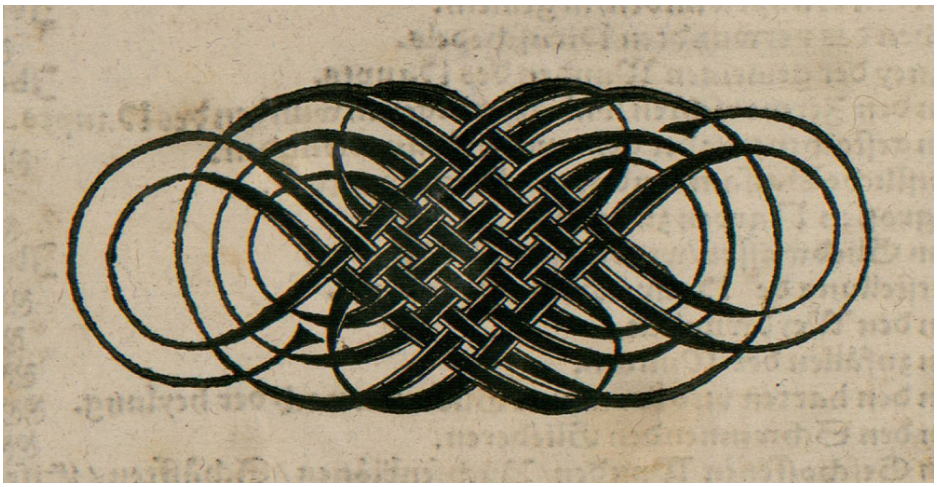
For most countries, keeping track of who owns what pieces of land is still a low-tech affair, involving mountains of hand-signed documents and expensive lawyers. That is, if a country is lucky enough to have a functioning land registry. The World Bank estimates that 70 percent of the world's population lacks access to land titling.[14] Getting everyone to agree on every stage of a property transaction and to record it permanently somewhere, is a feat of security, coordination, and trust.

Sweden is the country furthest in putting land registries on a blockchain. Since June 2016, Sweden's land registry authority (the *Lantmäteriet*) has been testing how to record property transactions on a blockchain, thereby saving Swedish taxpayers over €100 million ($106 million) a year by eliminating paperwork, reducing fraud, and speeding up transactions, according to Kairos Future, a consultancy in the project.[15]

Whereas the first phase essentially presented the technology's potential, the second phase (concluded in March 2017) involved the creation of a pilot blockchain registry and a set of smart contract templates that automate transactions. Each property registered on the blockchain was uniquely coded and linked to a smart key held only by the owner. When a land title changed hands, each step of the process was verified and recorded on the blockchain. Instead of the parties' signing a bill of sale at the agent's office, the pilot project demonstrated how they could use digital signatures verified automatically. This phase involved the telephone company Telia and two Swedish banks.

Each property registered on the blockchain was uniquely coded and linked to a smart key held only by the owner.

Mats Snäll, the Lantmäteriet official in charge of the project, said, "Blockchain technology offers real digital trust. It's the only solution so far that handles digital originals, verifies both legal actions and processes, and secures transparency."[16] However, Sweden must resolve legal issues, like the validity of digital signatures, and so it will not likely put the new system in place before 2019.



Gersdorff, Hans von, "Feldtbuch der Wundt Artzney," 1551 [SICD] by Paul K, 2008. Used under CC BY 2.0.

According to the World Bank, a digital land registry could be the most cost-efficient and fastest way to increase gross domestic product in the medium term.

While Sweden's land registry is out in front, counties where land holdings have less certain ownership and fraud is more common will likely enjoy the greatest benefits of blockchain-based systems. Although blockchain does not eliminate the entry of incorrect data and the requirement for trusted inputs, countries with limited or no centralized land recording will see blockchain registries as effective means of securing property ownership. According to the World Bank, a digital land registry could be the most cost-efficient and fastest way to increase gross domestic product in the medium term. It will serve as a foundation for better investments in land, enable the development of mortgage and credit markets, and become an institution for trust in one of the most fundamental parts of an economy: land and real estate.

A single ledger for the accounts of Canada

Most organizations maintain various trial balances, journal entries, sub-ledger extracts, account reconciliations, and supporting spreadsheet files in both electronic and manual formats.

Organizations have traditionally recorded transactions in ledgers, kept under lock and key. Those ledgers are typically isolated to protect their accuracy and sanctity, and when conducting business, each organization maintains its own separate record, to verify information independently. Most organizations—including the Government of Canada—maintain various trial balances, journal entries, sub-ledger extracts, account reconciliations, and supporting spreadsheet files in both electronic and manual formats.

In the maintaining the accounts of Canada, the receiver general must consolidate the financial ledgers of 102 departments, each with its own financial system. In preparing summary trial balances, departments aggregate their detailed financial information to government-wide coding; the receiver general does not have visibility into the operations required to perform this amalgamation nor the actual detailed information itself. Mistakes and missing data are costly and labor-intensive to rectify. A lack of visibility into departmental data also limits public scrutiny and analysis of government spending and revenue streams.

With the proposed blockchain-enabled solution, Canada could consolidate multiple independent and isolated departmental ledgers into a single shared ledger that would retain a complete, indelible, and authoritative history of all transactions executed by the Government of Canada. Departments would no longer submit aggregate financial statements, as the blockchain would instantaneously encode each department's accounting entries into the single shared ledger managed by the receiver general.

Using a permissioned blockchain would ensure that the ledger is trusted and secure, while remaining easily accessible to key participants across the government.

Using a permissioned blockchain would ensure that the ledger is trusted and secure, while remaining easily accessible to key participants across the government. Such a system would eliminate layers of redundancy, increase the integrity and granularity of data, expedite auditing requirements, and enable the receiver general to refocus its energies on activities that would boost the efficacy and transparency of the government's accounting and reporting functions.

Solution approach

The proposed solution for the receiver general would take the form of a distributed blockchain ledger. Although the terms, "distributed ledger" and "blockchain," are often treated as synonyms, blockchain is a specific type of distributed ledger. Blockchain is most often deployed for situations where parties to a transaction might not fully trust each other to agree on ledger updates (e.g., one user will not accept the "truth" as reported by another user). Instead of using a central third party or an offline reconciliation process, blockchain uses peer-to-peer (P2P) protocols.

On a blockchain, nodes participating in the network arrange transactions in groups or batches called *blocks*. When parties broadcast their transactions to the network, various nodes on the network verify that the transaction data obey the rules and standards of that individual blockchain network and that the existing data maintain integrity. Once a majority of the nodes agrees that the data are valid, all nodes in the network store the data as a new block in a chronological chain.

Once a majority of the nodes agrees that the data are valid, all nodes in the network store the data as a new block in a chronological chain.

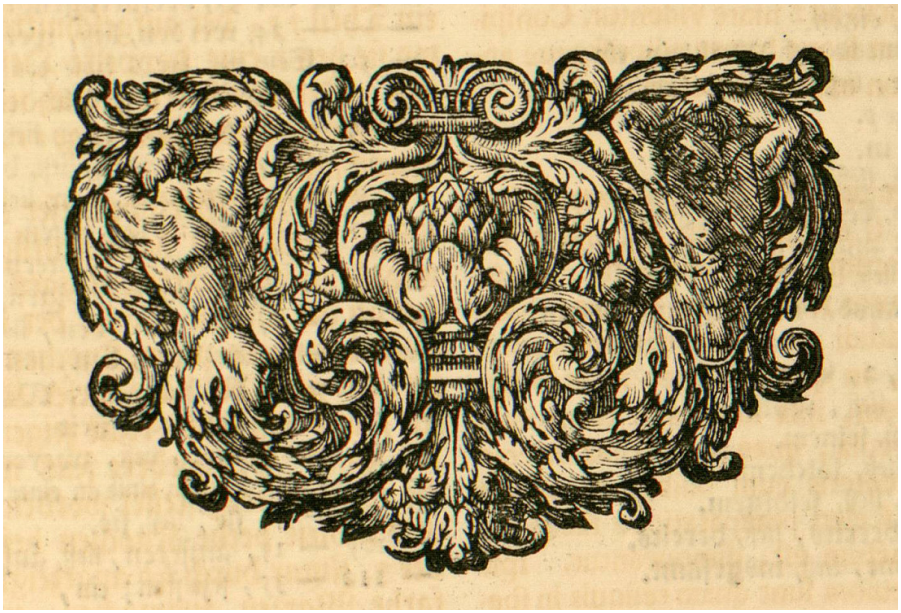
Cryptographic hash functions allow for data on the blockchain to be "hashed" in each block, which results in the persistence of a mathematical fingerprint representing the stored information. When a new block is assembled, the hashed value of the previous block is used to calculate the hashed value of the new block, creating a link between the blocks. Each block refers to the previous block, which forms a cryptographically linked chain—hence the name, *blockchain*. The chain's stored data and data references serve as a multilaterally accepted common repository for members of the blockchain network. Parties can update data only by appending new information to the ledger record.

We can visualize blockchains as databases with sets of validations not stored in central locations or managed by a few administrators. They are P2P networks that exist simultaneously on multiple nodes (computers): any interested or permissioned party can maintain a copy. They are distributed and redundant by design.

Solution architecture

In the proposed solution (Figure 1), blockchain technology would enable departments to record and verify their transactions using a single shared ledger that would fulfill all of the accounting and

We can visualize blockchains as databases with sets of validations not stored in central locations or managed by a few administrators.



August Johann Roesel von Rosenhof, "Historia naturalis ranarum nostratium," Nürnberg, 1758 [SICD] by Paul K, 2008. Used under CC BY 2.0.

auditing functions of the receiver general. Entries would be instantly hashed and time-stamped, creating an immutable record for each entry.

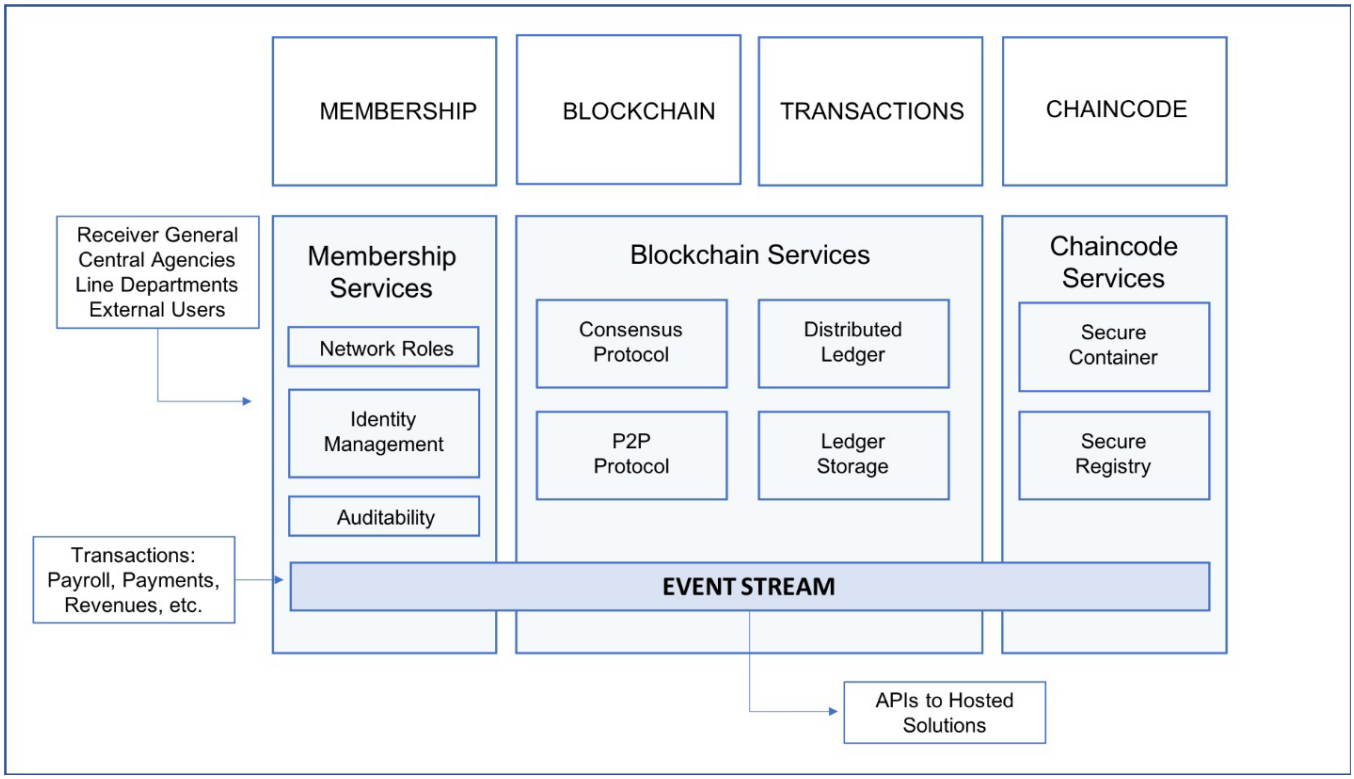
We can set up blockchains with varying degrees of access control.

We can set up blockchains with varying degrees of access control. The creators of public blockchains, including Bitcoin, Ethereum, and most cryptocurrencies, designed them to be accessible by anyone with a computer and Internet access. These public blockchain platforms eliminate the need for intermediaries in any exchange value using P2P protocols.

Private blockchains, by contrast, essentially redefine the intermediary. Nodes in a private blockchain network require invitations and must be validated by the network administrator or a set of protocols that govern it. The access control mechanism may vary: existing participants could decide future entrants, a regulatory authority could issue licenses for participation, or a consortium could determine whom to include in the network.

Depending on the architecture of the blockchain, there can be varying tiers of access and participation within the network as well. Nodes that have access to read the ledger, for example, may not also receive permission to write to it or create new entries. Operators can allow only certain nodes to perform the verification process, and these trusted parties would be responsible for communicating newly

Figure 1: Potential architecture of government blockchain



Source: "Introduction: Release 2.0," Hyperledger Fabric Documentation, Hyperledger, 2017, accessed 20 March 2018. Adapted by Anthony Williams under CC BY 4.0.

verified transactions to the rest of the network. The responsibility for securing access to these nodes, including determining when and for whom to expand the set of trusted parties, rests with the blockchain system operator.

The benefits of a private blockchain include faster transaction verification and network communication, the ability to fix errors and reverse transactions, and the ability to restrict access and reduce the likelihood of outsider attacks.

The receiver general could set up a permissioned distributed ledger and allow access to identical copies of the ledger to each federal department. Broadly speaking, the benefits of a private blockchain include faster transaction verification and network communication, the ability to fix errors and reverse transactions, and the ability to restrict access and reduce the likelihood of outsider attacks.

Using a permissioned network, the receiver general could assign differing roles to different departments (Table 1). Hyperledger Fabric, for example, allows different classes of network participants: network proprietors, owners, members, users, and auditors.

Public versus private blockchain consensus mechanisms

On public blockchain, participants submit transactions to the blockchain but no new data is accepted without consensus. The process by which a network of nodes verifies new transactions is known as a consensus protocol. In the public blockchain system, all users follow an algorithm that verifies transactions by committing software and hardware resources to solving a problem by brute

Table 1: Potential roles, rights, and responsibilities assigned to different government actors

Government office	Network role	Rights and responsibilities
Receiver general	Network proprietor	Proprietors set up and define the purpose of a chain network. After launching a network, they become network owners and can validate transactions and invite other business partners to use or co-own the network.
Central agencies (treasury board, finance)	Network owners	Network owners are stakeholders of a network that can both initiate and validate transactions, invite new members or users to the network, and approve new owners.
Line departments	Network members	Members are participants of a blockchain network that cannot validate transactions but can initiate new transactions on the network.
Government auditors	Network auditors	These individuals or organizations have permission to interrogate transactions.
Citizens, businesses, suppliers, researchers	Network users	End users of a network can read and initiate transactions on a chain network through applications. Unlike network owners and members, users do not own nodes. They transact with the network through a member or owner node.

force (i.e., by solving the cryptographic puzzle). The user who finds the solution first is rewarded, and each new solution, along with the transactions used to verify it, forms the basis for the next puzzle.

This process is designed to take time, currently around 10 minutes. Transactions are not considered fully verified for about one to two hours, after which point they are sufficiently deep enough in the ledger that introducing a competing version of the ledger, known as a fork, would be computationally expensive. This delay is a vulnerability of the system, in that a transaction that initially appears verified may lose that status later. It is also a significant obstacle to adoption by financial traders, devices on the Internet of Things, and any participant relying on fast-paced transactions.

Centralization is inimical to a truly robust network, and so a stakeholding approach is not a natural fit for this use case.

The most widely adopted approach to adding new block to a chain is the *Nakamoto consensus protocol*. In this instance, the rate at which blocks can be created is limited, often by using a proof-of-work mechanism, whereby a processing node can only add a new block by demonstrating that a difficult computational task has been completed. Proof of work is widely used, but the auxiliary effort required to complete the difficult task can be economically inefficient and would not be justified in receiver general context.

Another option is a *proof of stake*, in which the processing node that can add a new block in the next round is determined by the size of its stakeholding in the global blockchain and/or in that round. Proof of stake can be more computationally efficient, but it has not yet been widely adopted because of concerns that rewarding those who already are most deeply involved in the network inherently creates an increasingly centralized system. Centralization is inimical to a truly robust network, and so a stakeholding approach is not a natural fit for this use case.

Instead of Nakamoto consensus, private blockchains such as the one proposed here can use conventional replication algorithms. For example, Hyperledger, Stellar, and Ripple use *practical Byzantine fault tolerance*, which provides stronger guarantees about the completion of transactions, is more computationally efficient, and supports fewer processing nodes, all of which must be trusted actors.

How practical Byzantine fault tolerance works

When a node in the blockchain receives a message, it uses the message in conjunction with its internal state to run a computation or operation. This computation informs the node's interpretation of that message (e.g., whether to accept a transaction as valid). The node then shares its decision with all other nodes in the network. The blockchain updates according to the consensus decision determined by the total decisions submitted by the nodes—that is, a majority vote of validating nodes on the network.

For the receiver general's single ledger, departments would initiate transactions (e.g., payments to employees or vendors)

and the receiver general (and possibly other federal entities) would interrogate the transactions to ensure they are valid. The government could customize its approach to validating transactions. For example, Hyperledger Fabric uses an endorsement policy to define which network members must agree on the results of a transaction before they add it to the ledger. Fabric includes a small domain-specific language for endorsement policies, such as:

> *Government of Canada peers A, B, C, and F must all endorse transactions of type P (e.g., payroll transactions)*
>
> *A majority (51%+) of peers in the network must endorse transactions of type V (e.g., payments to vendors)*
>
> *At least three peers of A, B, C, D, E, F, and G must endorse transactions of type R (e.g., departmental revenues)*

Once network members reach consensus, the transaction data are time-stamped and their corresponding metadata are appended to the ledger and replicated to all other nodes (members) on the network.

Regardless of the protocol used, once network members reach consensus, the transaction data are time-stamped and their corresponding metadata are appended to the ledger and replicated to all other nodes (members) on the network. In this instance, the network would add validated transactions to the Government of Canada's ledger and update the DFMS.

User experience

A blockchain ledger would introduce several advantageous changes to the user experience for government departments, the receiver general, and government auditors.

Automation of reconciliation and reporting. The ability of departments to enter and verify transactions directly on the blockchain in near real-time would eliminate the need for time-intensive offline or batch reconciliation processes between the RG-GL and the departmental financial management systems. Rather, verified transactions in the blockchain would be used to update the receiver general's ledger and the DFMS simultaneously.

Transparency and granularity. The receiver general and government auditors would gain near real-time visibility into individual transactions (i.e., revenues and payments) conducted across the network of federal departments. Under the current system, the information received on a monthly basis is a summary-level trial balance prepared by all departments by aggregating their detailed financial information to government-wide coding—information the receiver general cannot access otherwise. Since transactions recorded on a blockchain could be coded, a shared blockchain ledger could amalgamate transactions for producing the public accounts of Canada without losing the granularity of transaction data, which would reside in the shared ledger.

A blockchain solution would ensure that the government's financial records are tamper-proof.

Reduced fraud. A blockchain solution would ensure that the government's financial records are tamper-proof and would

A blockchain ledger would allow government auditors to verify a large portion of the most important data behind the financial accounts of individual departments automatically.

Johann Friedrich Mayern Der Heil, "Curieuses Gespräche Im Reiche derer Todten Zwischen zweyen hochberühmten Männern," Lüneburg, 1731 [HAB] by Paul K, 2009. Used under CC BY 2.0.

reduce the scope for entering fraudulent transactions or falsifying information. The use of cryptographically linked blocks would ensure that no one could alter or delete records without detection.

Value-added auditing. A blockchain ledger would allow government auditors to verify a large portion of the most important data behind the financial accounts of individual departments automatically. The cost and time necessary to conduct a financial audit would decline considerably. With blockchain-enabled digitization, auditors could deploy more automation, analytics, and machine-learning capabilities such as automatically alerting relevant parties about unusual transactions on a near real-time basis. Supporting documentation—contracts, purchase orders, and invoices—could be encrypted and securely stored or linked to a blockchain.

These improvements would free auditors to spend time where they could add more value, such as analyzing complex dealings, recommending improvements in public spending process, and ensuring adequate internal controls and processes for departments to measure and report on their performance.

Introducing a shared blockchain ledger would introduce substantive changes to the receiver general's mandate and workflow.

Adapation of the receiver general mandate and workflow

Introducing a shared blockchain ledger would introduce substantive changes to the receiver general's mandate and workflow. Automating the labor-intensive reconciliation process will free the receiver general to focus more on upgrading the efficacy, timeliness, and transparency of government accounting and reporting functions. Consider the following:

Network governance. As governor of the blockchain network, the receiver general would be responsible for managing participants and their various roles in initiating and validating transactions. The

receiver general would also be responsible for any updates to the consensus protocol for verifying transactions.

Blockchain training. Transitioning to blockchain solutions will require education and training for financial executives and departmental leaders. The receiver general could partner with technology leaders in the federal government to educate executives on how blockchain works and how it will transform financial management and accounting.

The receiver general could build external applications that would interface with the blockchain ledger to make information accessible without sacrificing privacy or national security.

Data integrity. The success of a blockchain ledger depends on the quality of the data going in. By spending less on manual reconciliations, the receiver general could be more involved in doing quality control of the data management practices at the departmental level.

Data transparency and open government. On a public blockchain, any member of the public could view each record; any person could verify the authenticity of a transaction. This granularity would be overkill for releasing meaningful information about government revenues and spending to Canadians and compromise the privacy of the individuals and entities that transact with the government. In some instances, it could pose a threat to national security.

However, the receiver general could build external applications that would interface with the blockchain ledger to make information accessible without sacrificing privacy or national security. For example, the receiver general could create smart contracts with rules and algorithms that allowed data in the blockchain ledger to be automatically shared with third parties, once predefined conditions were met. Researchers, journalists, citizens, industry associations, and other interested parties could use such applications.

Challenges and risk management

What follows are some of the key risks that the receiver general must consider in evaluating the potential for using blockchain to create a single digital ledger for the public accounts of Canada.

Blockchain is an emerging technology, and therefore carries some risks for early adopters. On one hand, the flexibility of the blockchain ecosystem offers organizations customized implementation to meet their needs. However, this diversity can impede the development of standards and best practices, creating a burden for training the workforce and building, operating, securing, maintaining, and defending the technology for users in government. What follows are some of the key risks that the receiver general must consider in evaluating the potential for using blockchain to create a single digital ledger for the public accounts of Canada.

Blockchain implementation skills. Blockchain solutions are currently built in modern programming languages. For example, Bitcoin uses C++, Ethereum uses JavaScript and Solidity for smart contracts, and Hyperledger, the Go language and Java. Programmers at established software vendors can shift to blockchain development with minimal requirements, whereas government IT employees may require training in blockchain and underlying programming

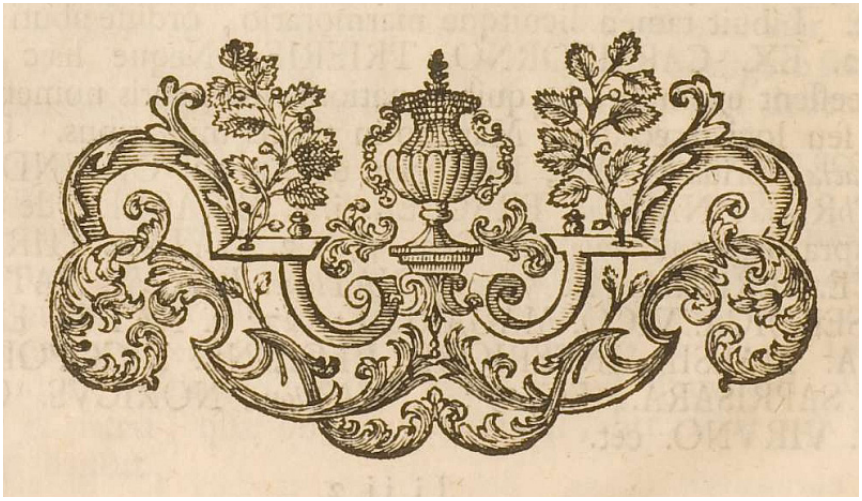
languages. Sourcing the right talent to manage a government-wide blockchain implementation will be challenging, with the technology industry's current shortage of skilled workers and the government's hiring challenges.

Sourcing the right talent to manage a government-wide blockchain implementation will be challenging, with the technology industry's current shortage of skilled workers and the government's hiring challenges.

Interoperability with blockchain. Blockchain is not a "plug-and-play" technology. On the contrary, blockchain solutions need to replace or tightly integrate or interoperate with existing systems. Most federal departments have aging infrastructure or legacy IT systems, which may impede blockchain adoption. With 102 federal departments, each with its own unique financial management system, the transition to a blockchain-enabled ledger will not be smooth. We need to investigate the blockchain compatibility of these systems as part of our feasibility study.

Modernizing policies and procedures. To adopt blockchain across the Government of Canada, each federal department must consider its existing policies, procedures, and financial management practices with an intent to update incompatible elements. Outdated legacy policies will severely cripple IT operations in transitioning to a distributed model. In particular, legacy data exchange procedures will hamper a blockchain platform's operation and restrict its interaction with other systems, internally and externally across government. A blockchain system would likely not succeed long term if the participating federal departments could not evolve with it. Blockchain is still a very young technology and will require flexibility and adaptability for early adopters.

Computational power. Running a government-wide blockchain ledger that records all the transactions of the Government of Canada would require a significant amount of computational power. To achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem and provide a proof of work. The amount of computational power—and electricity consumption—required in the proof-of-work method increases with the scale of the network.



Kunkelius, Johannes, "Johannis Kunkelii, Elect. Sax. Cubicularii intimi & Chymici Utiles Observationes sive Animadversiones De Salibus sixis," Rotterdam, 1678 [HAB] by Paul K, 2009. Used under CC BY 2.0.

In the receiver general use case, limiting participation to federal departments should rule out the presence of malicious users.

Security. The security of a blockchain network generally grows with the number of members supporting consensus, as more sharing and agreeing to data means that more nodes would need to collude or be simultaneously tampered with (i.e., hacked) in any attempt to attack, corrupt, manipulate, or "fool" the system and its individual databases. While miners can theoretically collude to incorporate false transactions into the blockchain, the probability of success diminishes with an increasing number of nodes required to verify each transaction.

Nevertheless, the presence of giant mining pools and the other massive bitcoin-mining conglomerates concentrated in countries with low electricity prices is a growing concern within the community, given the risk that such conglomerates could establish the critical mass required to monopolize control over a blockchain effectively.

In the absence of numbers, private blockchains achieve security by giving their operators control over who can read the ledger of verified transactions, who can submit transactions, and who can verify them. In other words, security is based on limiting participation to trusted actors. In the receiver general use case, limiting participation to federal departments should rule out the presence of malicious users.

Adopting blockchain has challenges, but they are not insurmountable. Any new technology always carries risk, but the public sector has a history of successfully, if slowly and cautiously, navigating those risks. The growing adoption of cloud computing is among the most recent examples. Given that the receiver general is pre-planning its IT modernization, it has an opportunity to include a blockchain solution in its roadmaps now and to launch small-scale proofs of concepts and pilot projects in cooperation with willing early adopters. Meanwhile, it can leverage lessons learned and proven best practices from early adopters in other jurisdictions.

Implementation costs

It is too early to offer an accurate estimate of the costs and benefits of designing, building, and implementing a blockchain-enabled ledger for the receiver general.

Feedback from blockchain vendors suggests that it is too early to offer an accurate estimate of the costs and benefits of designing, building, and implementing a blockchain-enabled ledger for the receiver general. Vendors raised these considerations.

Heterogeneity of financial management systems in the federal government. Each of the 102 departments in the federal government has a unique financial management system. Therefore, we need a more detailed technical assessment of the extent to which existing systems could interoperate with blockchain and whether we would need to upgrade, modify, or replace DFMS wholesale to integrate a blockchain-enabled ledger into the compiling of the public accounts of Canada.

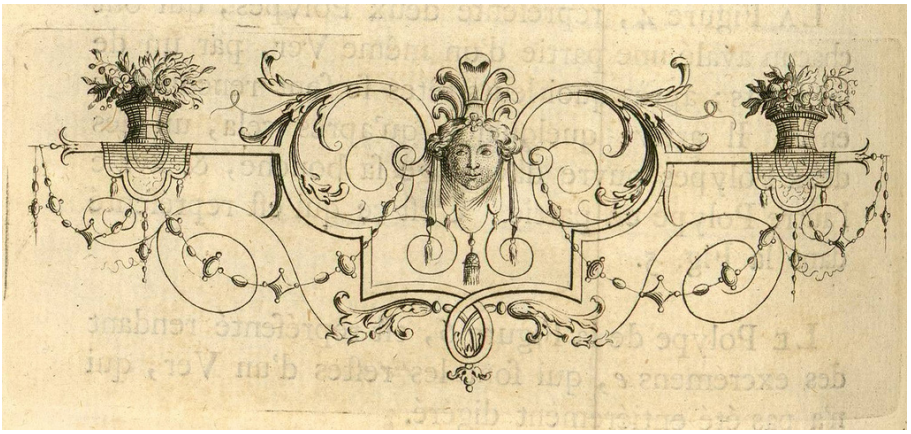
Differing departmental capacities to adjust to blockchain-enabled solutions. We need a similar analysis of capacity building, training, and process redesign needed to support the implementation of blockchain technology. In the launch of the Phoenix pay system,

we learned that the ongoing capacity-building and support costs of implementation can easily exceed the cost of the initial technical build and system implementation.

Blockchain technologies are still immature and constantly evolving.

Lack of comparable references cases. There are no other comparable implementations of blockchain technology in government at this scale. The land and corporate stock registries are significantly less complex than a wholeof-government adoption of a distributed ledger for the public accounts of Canada. Estonia's implementation of blockchain-enabled systems is far-reaching, but Estonia is working with a much smaller bureaucracy and far fewer legacy systems.

Rapidly evolving blockchain ecosystem. Blockchain technologies are still immature and constantly evolving. Interoperability between blockchain and the leading enterprise resource planning and financial management solutions is also advancing; whether and how these advances will roll out to existing users in government is unclear. Thus, the costs of design and implementation will depend on the state of evolution of the component technologies. Given these factors, along with the Government of Canada's experience with the Phoenix pay system, the receiver general should adopt a cautious and incremental approach to blockchain technology.



Trembley, Abraham, "Mémoires, pour servir à l'histoire d'un genre de polypes d'eau douce, à bras en forme de cornes," Paris, 1744 [SICD] by Paul K, 2009. Used under CC BY 2.0.

Blockchain is disrupting the centuries-old standard of double-entry bookkeeping and giving rise to a new paradigm—"triple-entry accounting".

Triple-entry accounting

According to some blockchain enthusiasts, blockchain is disrupting the centuries-old standard of double-entry bookkeeping and giving rise to a new paradigm—"triple-entry accounting"—that will rock the world of chief financial officers, controllers, corporate auditors, and certified or chartered public accountants. It is hyperbole based on misunderstandings of both double and triple entries.

In the double entry method, every financial transaction has equal and opposite effect in at least two different accounts, in the form of debits and credits. It is used to complete this equation:

Assets = Liabilities + Equity

In other words, double-entry bookkeeping allows organizations to maintain records of their assets and liabilities that reflect what they own and owe, and what they have earned and spent over any given period of time.

The cryptographically sealed record of transactions—effectively a shared receipt—was the equivalent of a "third entry" that could extend double-entry systems.

In 1982, Yuji Ijiri, a professor of accounting and economics at the Graduate School of Industrial Administration at Carnegie-Mellon University, added a third component—momentum—after the global standard debit and credit.[17] While he used the phrase, "triple-entry accounting," he did not coin it—Russian scholars did, around 1900—nor did he view his system as paradigm-shifting; he considered double-entry accounting highly extensible.[18]

In 2005, Ian Grigg argued that the cryptographically sealed record of transactions—effectively a shared receipt—was the equivalent of a "third entry" that could extend double-entry systems:

> *The digitally signed receipt, with the entire authorization for a transaction, represents a dramatic challenge to double-entry bookkeeping at least at the conceptual level. The cryptographic invention of the digital signature gives powerful evidentiary force to the receipt, and in practice reduces the accounting problem to one of the receipt's presence or its absence. This problem is solved by sharing the records—each of the agents has a good copy. …*
>
> *This leads to the pairs of double entries connected by the central list of receipts; three entries for each transaction. … We term this* triple-entry bookkeeping*. Although the digitally signed receipt dominates in information terms, in processing terms it falls short. Double-entry bookkeeping fills in the processing gap, and thus the two will work better together than apart. In this sense, our term of triple-entry bookkeeping suggests an advance in accounting, rather than a revolution.*[19]

Our term of triple-entry bookkeeping suggests an advance in accounting, rather than a revolution.

Ben Taylor, the CEO of SoftLedger, a cloud accounting software company, argued that Grigg's use of the phrase is confusing to accounting professionals and misleading to technologists: the presence of digitally-signed receipt is not a fundamental departure from double-entry accounting. He pointed out a common misconception, that "the writing of each piece of information to the blockchain is actually a third entry. It's not."[20]

Numerous blockchain commentators have used "double-entry accounting" to refer to the recording of a single transaction between two parties in the separate accounting records of each party—such as a buyer and a seller recording the sale and the purchase of an asset in their respective books.[21] In this misrepresentation of double-entry accounting, the act of recording a transaction on the blockchain "creates an interlocking system of enduring accounting records" between the two parties, "rather than these entries occurring

separately in independent sets of books."[22] Hence, the flawed notion of the third entry.

This misrepresentation is unfortunate, but it should not diminish the value of blockchain in accounting applications. The ability to write transactions to a blockchain in real time and between multiple parties is powerful. A ledger that shows the entire sequence and relationship among transactions provides not simply a credible audit trail but real-time status—the network state—of all transactions relevant to the parties.

The ability to write transactions to a blockchain in real time and between multiple parties is powerful.

Lambeck, Peter, "Petri Lambecii Hamburgensis, Prodromus Historiæ Literariæ," Frankfurt, 1710 [HAB] by Paul K, 2008. Used under CC BY 2.0.

Algorithmic techniques have extended well beyond their origins in cryptocurrencies to become tools to record, enable, and secure huge numbers and varieties of transactions.

Conclusions and recommendations

In sector after sector, algorithmic techniques have extended well beyond their origins in cryptocurrencies to become tools to record, enable, and secure huge numbers and varieties of transactions, incorporating rules, smart contracts, and digital signatures among many emerging technologies. Jurisdictions ranging from Estonia to the United States are using blockchain to power innovations in business registration, identity management, e-voting, healthcare, and international trade. Based on our research, we recommend the following:

Technical staff will require training in blockchain and underlying programming languages. A blockchain system will likely not succeed long-term unless participating federal departments evolve with it.

Examine the potential for significant process efficiencies. For the Government of Canada, trial balances, journal entries, sub-ledger extracts, account reconciliations, and supporting spreadsheet files likely exist in various electronic and manual formats. With the proposed blockchain-enabled solution, it could consolidate multiple independent and isolated departmental ledgers into a single shared ledger that would retain a complete, indelible, and authoritative history of all transactions by the government. Entering and verifying transactions directly on the blockchain could eliminate time-intensive offline or batch reconciliation processes between the RG-GL and the departmental financial management systems.

Begin to reimagine the role and responsibilities of government auditors. The receiver general and government auditors would gain near real-time visibility into individual transactions, as opposed to aggregated summaries. By giving auditors real-time access to unalterable audit evidence (e.g., agreements, purchase orders, and invoices), we could improve the pace of financial reporting and auditing. Auditors could spend more time probing complex transactions, recommending how to improve the efficacy and efficiency of public spending, and ensuring that departments have adequate internal controls and processes for measuring and reporting on their performance.

Begin to reimagine the role of the receiver general. Automating the labor-intensive reconciliation process, in particular, will free the receiver general to focus more on upgrading the efficacy, timeliness, and transparency of government accounting and reporting functions. New roles for the receiver general would include managing participants and their various roles in initiating and validating transactions on the ledger as well as building external applications that would boost the transparency of the government's reporting process.

Understand the trade-offs between private ledgers and public ones. With greater security and access control, a permissioned blockchain solution would allow access to identical copies of a ledger to a limited number of preselected trusted participants, namely each federal department and the receiver general. The benefits of a private or permissioned blockchain include faster transaction verification and network communication and the abilities to fix errors, reverse transactions, restrict access, and reduce the likelihood of outsider attacks. Using a permissioned network, the receiver general could choose to assign differing roles to different departments.

Include a blockchain-enabled ledger in forward-looking IT plans. Blockchain is still an emerging technology and carries some risks for early adopters. Technical staff will require training in blockchain and underlying programming languages. Most federal departments have aging infrastructure and/or legacy IT systems in critical functions, which may impede blockchain adoption. A blockchain system will likely not succeed long term unless the participating federal departments evolve with it. The receiver general has an opportunity to include a blockchain solution in its roadmap

now and to leverage lessons and proven practices of early adopters elsewhere.

Proceed with an incremental approach. In light of the implementation challenges, and the evolving state of blockchain technologies, the receiver general should adopt a cautious and incremental approach to blockchain technology. A proposed first step is an in-depth feasibility study of cost and implementation-related parameters discussed. As a second step, pending the outcome of the feasibility study, the receiver general should work with two or three early adopter departments to design and test a POC and run a multi-year pilot to test assumptions and conclusion of the feasibility study.

Questions to ask in developing proof of concept

- *How much does the current system of accounting cost to administer, for a department and for the government as a whole?*
- *How would a blockchain solution affect the mandate and function of those responsible for government accounts?*
- *Will the system align with existing laws and regulations?*
- *Will changes to legal or regulatory frameworks facilitate adoption or effectiveness?*
- *Could the solution leverage existing blockchain-based accounting efforts in either the public or private sectors?*
- *Are there financial or fiduciary risks associated with the solution? If so, could those risks be mitigated?*
- *How would a blockchain ledger change the user experience for government departments and/or affect other stakeholders such as government auditors and the public?*
- *What will such a system cost each department and the government as a whole?*

Do we go ahead, invest in this emerging technology, and embrace the required changes in technology, processes, and organizational design, or do we focus on improving the existing system and optimizing its processes?

Ultimately, the core question facing the receiver general is: do we go ahead, invest in this emerging technology, and embrace the required changes in technology, processes, and organizational design, or do we focus on improving the existing system and optimizing its processes?

Questions to ask in an after-action review

- *How much did it cost to build a blockchain POC?*
- *How much did it cost run a multi-year pilot process, including costs to support the implementation of the blockchain technology, such as investments in process redesign, capacity building, and ongoing technical support?*

- *Were administrative efficiencies realized or demonstrated over the course of the pilot?*
- *Based on these costs and benefits, what are the estimated costs and benefits of scaling the solution across the federal government?*
- *What is the cost-benefit analyses of status quo versus a blockchain-based system?*
- *If departments jointly participate in building and administering a shared blockchain ledger, how will the government account for pro-rata share of costs for each department?*
- *Given the estimated benefits, over what time horizon should the government expect to see a payback on its investment?*

Collaborate with stakeholders. The receiver general should work closely with involved departmental financial managers to understand sunk costs, operational costs (i.e., departmental overhead), and costs borne by the receiver general. These will be important data when comparing costs and benefits of the status quo with blockchain-based processes. The receiver general and departmental financial managers should coordinate the tracking and analysis of efficiencies and benefits arising from a blockchain-enabled pilot. Given the learning curve and organizational adjustments in play, participants may not realize efficiencies and benefits until the second year of the pilot, once they better understand its effects on organizational design and financial management processes.

The receiver general should work closely with involved departmental financial managers to understand sunk costs, operational costs, and costs borne by the receiver general.

Endter, Susanna Maria, "Der aus dem Parnasso ehmals entlauffenen," Nürnberg, 1691 [HAB] by Paul K, 2008. Used under CC BY 2.0.

About the author

Anthony D. Williams is co-founder and president of the DEEP Centre and an internationally recognized authority on the digital revolution, innovation and creativity in business and society. He is co-author (with Don Tapscott) of the groundbreaking bestseller, *Wikinomics: How Mass Collaboration Changes Everything*, and its follow-up, *Macrowikinomics: New Solutions for a Connected Planet*.

Among other current appointments, Anthony is an expert advisor to the Markle Foundation's *Initiative for America's Economic Future*, a senior fellow with the Lisbon Council in Brussels and the Institute on Governance in Ottawa, and chief advisor to Brazil's Free Education Project, a national strategy to equip two million young Brazilians with the skills required for a 21st Century workforce.

Anthony was recently executive editor for the Global Solutions Network at the Martin Prosperity Institute, a committee member of the National Research Council's Committee on Science for the EPA's Future, a visiting fellow with the Munk School of Global Affairs at the University of Toronto and Program Chair for the 18th World Congress on Information Technology in Montreal. His work on technology and innovation has been featured in publications such as the *Huffington Post*, *Harvard Business Review*, and *The Globe and Mail*.

Notes

1. Organization for Economic Co-operation and Development, "Government at a Glance 2017: Estonia," Organization for Economic Co-operation and Development, 2017. www.oecd.org/gov/gov-at-a-glance-2017-estonia.pdf, accessed 20 March 2018.
2. @e_Residents, Twitter post, 23 Jan. 2018, 4:08 am. twitter.com/e_Residents/status/955728839791038465, accessed 20 March 2018.
3. Funderbeam, "Start-up Investment Report: Estonia," Dec. 2017, with data from 2 Oct. 2016. www.ifuturo.org/sites/default/files/docs/startup_investment_report_estonia.pdf, accessed 20 March 2018.
4. Nathan Heller, "Estonia, the Digital Republic," *The New Yorker*, 18 Dec. 2017. www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic, accessed 20 March 2018.
5. US General Services Administration, "FY 2019 Congressional Justification," 12 Feb. 2018. www.gsa.gov/cdnstatic/GSA%20FY%202019%20CJ.pdf, accessed 3 April 2018.
6. Jose Arrieta, Remarks delivered at the ACT IAC Blockchain Forum, 31 Jan. 2018. www.actiac.org/2018-blockchain-forum-0, accessed 3 April 2018.
7. David Thornton, "GSA experimenting with blockchain to cut contracting time," Federal New Radio, 16 Nov. 2017. federalnewsradio.com/it-modernization-2017/2017/11/gsa-experimenting-with-blockchain-to-cut-contracting-time, accessed 3 April 2018.
8. Jose Arrieta, remarks during Panel 1, "Blockchain and the Importance of Modernization," ACT IAC Blockchain Forum, Mayflower Hotel, Washington DC, 3 April 2018. www.actiac.org/2018-blockchain-forum-0, accessed 3 April 2018.
9. David Thornton, "GSA experimenting with blockchain to cut contracting time," Federal New Radio, 16 Nov. 2017. federalnewsradio.com/it-modernization-2017/2017/11/gsa-experimenting-with-blockchain-to-cut-contracting-time, accessed 3 April 2018.
10. "Corporate Headquarters," Division of Small Business, State of Delaware, n.d. dedo.delaware.gov/Industries/Corporate-Headquarters, accessed 6 April 2018.
11. Jeffrey W. Bullock, "Delaware Division of Corporations 2016 Annual Report," Delaware Division of Corporations, 2016. corp.delaware.gov/2016AnnualReport.pdf, accessed 6 April 2018.
12. John Williams, "Stock ledgers revolutionized with Delaware corporate blockchain legislation," *Delaware Business Times*, 28 June 2017. www.delawarebusinesstimes.com/stock-ledgers-revolutionized-delaware-corporate-blockchain-legislation, accessed 6 April 2018.
13. Sara Merken, "Delaware blockchain move drawing in companies, law firms," *The Bureau of National Affairs*, 11 Aug. 2017. www.bna.com/delaware-blockchain-move-n73014463104 accessed 6 April 2018.
14. Caroline Heider and April Connelly, "Why land registration matters for development," World Bank Group, 28 June 2016. ieg.worldbankgroup.org/blog/why-land-administration-matters-development, accessed 9 April 2018.
15. "The Land Registry in the Blockchain," Kairos Future, March 2017. chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf, accessed 9 April 2018.
16. Tom Turula, "Sweden is trialing a blockchain-powered land registry—which could save taxpayers $100 million," *Business Insider Nordic*, 4 April 2017. nordic.businessinsider.com/sweden-is-pioneering-a-blockchain-run-land-registry---which-could-save-taxpayers-$100-million-2017-4, accessed 9 April 2018.
17. Yuji Ijiri, "Triple-entry bookkeeping and income momentum," American Accounting Association, Sarasota, FL, 1982.
18. Richard Mattessich, *Two Hundred Years of Accounting Research: An International Survey of Personalities, Ideas, and Publications* (from the Beginning of the Nineteenth Century to the Beginning of the Twenty-First Century) (London, U.K.: Routledge, 2008): 201, 239-240, 247, 336.
19. Ian Grigg, "Triple Entry Accounting," Working Paper, 25 Dec. 2005. iang.org/papers/triple_entry.html, accessed 12 June 2018.
20. Ben Taylor, "Triple-Entry Accounting and Blockchain: A Common Misconception," *Forbes*, Forbes Media, 28 Nov. 2017. www.forbes.com/sites/forbesfinancecouncil/2017/11/28/triple-entry-accounting-and-blockchain-a-common-misconception/#15f854f0190f, accessed 12 June 2018.
21. See, for example, Daniel Jeffries, "Why Everyone Missed the Most Important Invention of the last 500 Years," *Hackernoon*, 22 June 2017. hackernoon.com/why-everyone-missed-the-most-important-invention-in-the-last-500-years-c90b0151c169, accessed 12 June 2018.
22. Blockchain ABC, "Triple Entry Accounting," n.d. blockchainabc.blogspot.com/p/blog-page.html, accessed 12 June 2018. The post claims that Ian Grigg invented the term; Grigg did not. See Mattessich, *Two Hundred Years of Accounting Research*.

blockchainresearchinstitute.org