Developing winning blockchain applications in the public sector
Blockchain basics for government
About the authors

**WENDY HENRY** leads Deloitte Consulting LLP’s US Government and Public Services Blockchain practice, working with clients to distill emerging technologies into simple business value discussions. She is a hands-on technologist with 30 years of large-scale, complex system integration experience across a wide variety of technologies, including blockchain, cloud, digital innovation, and location-based technologies.

**BRUCE CHEW** is a managing director in Strategy and Analytics with Deloitte Consulting LLP where his work focuses on strategy development and implementation and the building of organizational capabilities. He is also the federal research leader for the Deloitte Center for Government Insights.

**ANDREA LORA** is a senior consultant in Deloitte Consulting LLP’s US Government and Public Services Blockchain practice. She works with federal clients to design and build business-focused technology solutions, and has a passion for delivering innovative blockchain solutions and thought leadership.

**HOGENE CHAE** is a senior consultant in Deloitte Consulting LLP’s Government and Public Services practice, with a focus on customer transformation by designing and implementing capabilities and architectures to bring customer strategies to life.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what’s behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

## Contents

- Introduction: Working with a foundational technology | 2
- Three considerations for adopting blockchain | 3
- A promising test case: Intragovernmental transactions reconciliation and reporting | 5
- Characteristics of a strong blockchain application | 7
- Ongoing considerations | 16
- Conclusion: The challenges and rewards of early adoption | 17
- Endnotes | 18
MOST CONVERSATIONS ABOUT blockchain spur more questions than answers. That’s hardly surprising; the technology is relatively new, difficult to explain in a few words, and surrounded by a buzz that’s generating excitement about its possibilities as well as accusations of hype.

But this should likely be expected. Blockchain falls into the category of “foundational technologies”—as with the internet and personal mobile devices before it, it could transform not just what we can do, but how we do it, in fundamental ways. As noted in *Will blockchain transform the public sector?*, the first paper in our blockchain basics for government series, a decision to employ blockchain is “not just a technology question—it is a decision that can transform business models and processes and reshape the set of stakeholders and their roles.”

While its use in the financial sector gets most of the press, dozens of applications for blockchain are being explored by governments at all levels and around the globe. Our research has shown that technology is only one factor in successful blockchain applications—and not the most important one.

Thinking of blockchain only as software, a tool to solve a specific problem, limits our ability to understand its challenges and its potential. To make full use of blockchain—and to make it work for your organization—we should address a deeper set of questions, with answers extending across multiple domains.

**FIGURE 1**

What is blockchain?

A peer-to-peer digital ledger system with cryptographic identity and security for recording business transactions, information, and events that is...

- Near real time
- Trustless environment
- Distributed ledger
- Irreversible
- Censorship resistant

Source: Deloitte analysis.
Three considerations for adopting blockchain

We recommend beginning with a small-scale pilot program to allow time for research and investigation. A pilot also provides a stepping stone toward larger-scale transformation. We recommend thinking big and starting small. Implement your pilot program at an edge of your business and adapt, alter, and expand it as your abilities and understanding evolve.

Of course, before beginning to develop a specific blockchain application, it’s important to first evaluate the business problem being addressed. That means evaluating each potential use in terms of three main factors: desirability, feasibility, and viability.

- **Desirability:** The challenge or potential opportunity would be desirable for your agency if it aligns with and furthers your goals or operations. But to be successful, blockchain applications should provide value across the ecosystem. In identifying problems to solve, government and public service stakeholders should target existing issues that keep them from meeting mission requirements, reducing stakeholder pain, using taxpayer dollars effectively, and/or improving citizens’ experience.

- **Feasibility:** The challenge or opportunity is considered feasible if there are no insurmountable technical or organizational obstacles to its success. Starting small can give an organization time to discover such obstacles and see how the solution functions with the organization and its stakeholders. A pilot, moreover, can be more nimble and face less ingrained resistance to change. It can inform later adaptations to existing organizational processes without demanding fundamental change all at once. Successes at the edge then can be rolled out more broadly, applying lessons learned at earlier stages.

- **Viability:** After you have decided there is a business case and determined it is feasible to move forward, it is important to evaluate whether the use case is blockchain-centric. The use case is typically considered viable when blockchain offers greater advantages and value than other solutions. Problems for which blockchain is particularly well suited tend to have at least three of four main characteristics (see table 1); if this threshold isn’t met, you may want to seek alternative solutions. If a blockchain use meets this threshold, its viability can be further enhanced if one or both of two “value magnifiers” apply.
### TABLE 1

A potential blockchain application should have at least three of four core characteristics and will benefit from value magnifier criteria

<table>
<thead>
<tr>
<th>Core characteristics</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared data</strong></td>
<td>Need for a structured repository of information through which multiple independent parties may share and record data</td>
</tr>
<tr>
<td><strong>Multiple writers</strong></td>
<td>More than one entity required to generate transactions</td>
</tr>
<tr>
<td><strong>Low trust</strong></td>
<td>A degree of mistrust between entities in the ecosystem (between government entities, “mistrust” is usually described as having competing objectives)</td>
</tr>
<tr>
<td><strong>Immutability</strong></td>
<td>Need for transaction data to be permanently recorded, serving as a single, undisputed source of truth to enable auditability and enforce accountability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value magnifiers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Opportunity for disintermediation</strong></td>
<td>Trusted intermediary or central gatekeeper can be eliminated from the transaction validation process</td>
</tr>
<tr>
<td><strong>Transaction interaction</strong></td>
<td>Different entities can create interactive or dependent transactions</td>
</tr>
</tbody>
</table>

Source: Adapted from Mark White, Jason Killmeyer, and Bruce Chew, *Will blockchain transform the public sector?*, Deloitte University Press, September 11, 2017.
A promising test case
Intragovernmental transactions reconciliation and reporting

The reconciliation and reporting of intragovernmental transactions (IGTs) seem to provide a good test case to illustrate how to evaluate the use of blockchain. This discussion of IGT as a representative use case reflects conversations with many agencies on the potential impact of blockchain in this activity, highlights some of the top questions and concerns expressed in these conversations, and begins to document the case for blockchain as an enabler of government financial management.

Many other blockchain applications are being explored, including various payment situations beyond IGT, voting, land registration, identity management, supply chain traceability, health care, and taxation. We chose IGT as an illustration, however, because it’s a government function involving all agencies; while IGT recording and reporting is relatively straightforward in theory, it has proven difficult to execute effectively in practice. As governments look to increase their use of shared services, shared cost and service models between entities are likely to become more common.

In this case, blockchain may eliminate current weaknesses in transaction reconciliation and reduce compliance issues. A blockchain application could give all stakeholders a common platform for a variety of transaction-related activities, better visibility into transaction histories, and automated interagency agreement terms to support compliance.

Evaluating the IGT case

As stated above, it is important to first evaluate the business problem or the opportunity for alignment to business needs and strategy, identify any technical or organizational issues that may impact the ability to implement the solution, and finally, determine whether blockchain is the best technology to deliver value in the solution.

Desirability: IGTs are a significant, shared business problem affecting nearly all agencies. A solution providing trading partners with near-real-time settlement and an accurate record of transactions would be desirable for all involved. From a business perspective, it could help minimize errors and increase managerial confidence in transaction reporting. From the user’s perspective, it could minimize the time needed to complete administrative tasks and allow employees to reallocate their time to more mission-critical tasks.

Feasibility: IGT is by definition a business transaction between two heterogeneous business partners (agencies). Organizationally, culture as well as policy may vary between the agencies. Complex questions concern the integration points between trading partners and systems, changes to current processes, and governance of the network. Data security and infrastructure are important to government leaders and could be key considerations when designing user interfaces. These are issues that exist independent of the technology chosen and should be kept in mind when deciding to move forward in developing any solution.

Viability: IGT has the four main characteristics listed in table 1, making a viable case for blockchain. IGT involves shared data access by multiple writers, in a low-trust process that requires immutability to address current problems. IGT also has added the potential for disintermediation via automated reconciliation and real-time transparency. In addition, there is the possibility of codifying terms and
IGT RECONCILIATION AND REPORTING

IGTs result from business activities conducted between two government entities. To properly present the balances in the *Financial report of the United States government*, IGTs must be eliminated during the preparation process. If not, they can result in misstated balances. For buy/sell IGTs, when two federal agencies enter into a reimbursable agreement, each will have a reciprocating "purchase" (accounts payable) and "sale" (accounts receivable) that should net to zero; otherwise, the buy/sell IGT category will show a difference.\(^4\)

According to the US Government Accountability Office's (GAO's) financial audit of fiscal years 2017 and 2016, the federal government continues to be unable to adequately account for and reconcile intragovernmental activity and balances between federal entities. Federal entities are responsible for properly accounting for and reporting their intragovernmental activity and balances in their entity financial statements. When preparing the consolidated financial statements, intragovernmental activity and balances between federal entities should be in agreement and must be subtracted out, or eliminated, from the financial statements. If the two federal entities engaged in an IGT do not both record the same transaction in the same year and for the same amount, the IGT will not be in agreement, resulting in errors (that is, differences or unmatched amounts) in the consolidated financial statements.\(^5\)

The inability to adequately reconcile IGTs among federal entities can lead to:

- Hundreds of billions of dollars in unreconciled activity (as per the GAO's financial audit of fiscal years 2017 and 2016)
- The inability to reliably report a significant portion of the federal government's assets, liabilities, costs, and other information
- The inability to reliably measure the full cost as well as financial and nonfinancial performance of certain programs and activities
- A lack of reliable financial information for the federal operations
- Differing execution of financial management policy
- Errors and low trust in reporting

conditions of the interagency agreement (IAA) into a "smart" contract on the blockchain, an example of *transaction interaction*.

Based on our conversations with federal agencies, IGT appears to represent a viable and relatively straightforward case for the use of blockchain, and one that seems worth exploring for the issues it raises. Even the simplest blockchain implementation, however, should consider not only present needs but also future possibilities. And that typically requires detailed analysis of both the technology and broader characteristics that will determine ultimate success.
Characteristics of a strong blockchain application

Organizations starting to explore blockchain are often focused on the technology. However, it is equally important to understand the unique ecosystem that is a blockchain and the considerations in successfully forming or joining one of those ecosystems. In the last few years, Deloitte’s global team of blockchain professionals has consulted on proofs of concept and pilots across 23 industries, encompassing a wide spectrum of projects for both government and commercial organizations in 20 nations around the world. Drawing on this experience, we have developed guidelines for approaching blockchain readiness from a holistic perspective, incorporating both common technology considerations and the broader but equally important choices that should be addressed to create a successful application (figure 2).

In developing and evaluating a proposed blockchain application, consider each of the six areas in figure 2, and where and how addressing gaps could strengthen outcomes. Each area is discussed below and illustrated using IGT as an example. Key questions to be considered for each are summarized in table 2 following the discussion of all six areas.

![Figure 2: Six factors that should be considered to create a successful blockchain application](image)

Source: Adapted from Eric Piscini et al., Taking blockchain live: The 20 questions that must be answered to move beyond proofs of concept, Deloitte, 2017.
The consortium: Who should be involved?

Before wrestling with questions of technology, resources, and staffing, a more fundamental question may be **who should be involved?** We call the participants in a blockchain ecosystem a *consortium*—the agencies, companies, regulators, and other organizations that will participate in processes and outcomes, guided by an agreed-upon set of standards. Put another way, it’s simply a group of partners. The exact mix of partners and their roles will be unique to each consortium.

Defining the consortium’s membership is far from trivial. Blockchain practically **demands** collaboration, to set standards, develop infrastructure, and execute transactions. When considering our notional IGT system, we found that government leaders quickly sensed the value of building an inclusive consortium, but seemed to struggle to define who specifically should participate and what everyone’s roles should be. Consider also that members’ roles may evolve as a blockchain application matures. For example, as the IGT consortium develops an application in a controlled environment, internal auditors initially may serve as advisors but eventually become users as the solution scales to the greater ecosystem.

Agreement on members and their roles is a key step in creating a successful consortium. Beyond direct participants, others may become involved from an oversight or compliance perspective and may participate as users of the system but not members of the consortium. It’s important to include all the participants necessary for success, in a large enough group to eventually achieve a viable scale. To ensure its survival over time, a consortium should be adaptable and scalable, without unnecessary membership limits. Members, therefore, should design the network to allow for flexibility in both the number of participants and transaction volumes. Rules for **changing** rules also should be established.

Another important question concerns **the common goals of the consortium.** If members can’t agree on clear, common goals and reasons for operation, the consortium could be set up for failure. If a member brings key resources but doesn’t receive enough benefit to compensate for its contributions, the goals should be adjusted or an additional payment or benefit agreement worked out.

In discussions concerning IGT applications, the primary goals identified include increased transparency throughout the agreement life cycle, the integrity of the agreement and transaction data, and near-real-time reconciliation. Members can collaborate to create shared data standards, designate responsibilities, and refine processes. IGT cases have also highlighted other effects, including disintermediation, which could be of major economic benefit in the future.

Why does all this matter? In nearly every conversation with government leaders, the same basic questions tend to arise: **who owns it and who pays for it?** While the first question may seem simple—no one entity owns it—it contributes to the complexity of the second question. A truly shared ecosystem with no central owner represents an unprecedented and complex shift in cost and ownership models for government. An important first task of any governmental consortium thus would be to define alternative models for cost and operations based on factors such as the group’s shared goals, roles, and expected usage. We explore this in more detail in the following section.

Operations: How does it all fit together?

Choices made in defining a blockchain solution typically affect each member of the consortium—their day-to-day operations and the way in which they work together. Addressing the following key concerns up front can help to eliminate unanticipated challenges and ensure the solution’s success.

Clearly outlining **who is responsible for managing and maintaining the platform** is likely to be key to a successful interagency operation. Any decision to update or alter a blockchain
network could have significant downstream impacts, particularly as the number of users increases and the platform matures. As with any effort involving multiple stakeholders, diplomacy and patience are important when making decisions about a shared blockchain solution.

Given the 24/7 nature of operations and maintenance, a trusted third-party vendor could be the best choice for some or all platform support. Vendor roles and responsibilities should be clearly defined, covering procedures and activities in areas including operations, production control, diagnostics and problem handling, maintenance, data administration and distributed ledger monitoring, system security plans, and configuration management. Consortium members could manage any outside vendors via an executive oversight committee that defines roles and responsibilities and evaluates the quality of vendor support.

The intragovernmental consortium may select federal financial regulatory agencies to hold primary responsibility for managing and updating the platform, after members agree to a process for updates. If carefully managed, the system can be maintained with minimal impact on external systems and stakeholders.

Another important factor to consortium operations is how the consortium will scale to include more members and how existing agreements and contracts will be affected.

Members will need an agreement to modify the consortium, associated contracts, and other elements of its operations. In the spirit of inclusion and scalability, we generally recommend designing the solution with considerable flexibility in mind.

Consortium members should share the overarching goal of a frictionless network of transaction data. If new members share this vision, it’s less a question of if the consortium can include more members, but rather how. Each participant’s role in the consortium can help indicate the impacts to operations, maintenance, and progress toward the overall goal in times of change.

Scalability is important to ensure a consortium isn’t bound by a limit on the number of members.

The consortium should design the network to allow for flexibility and growth, both in membership and transaction volume. In general, blockchain derives its power from numbers; greater value is realized as the network expands. The ubiquity of intragovernmental transfers is part of the reason that our IGT use case appears attractive. The easier it is to scale, the better.

**Business impacts: How will people and processes across the ecosystem be affected?**

A blockchain solution will affect many day-to-day aspects of the organization, and indeed can have an impact on the entire business model. As explained in *Will blockchain transform the public sector?*, some specific characteristics of business problems are more likely to lend themselves to a blockchain-integrated solution than others. Important operational decisions must be made about the platform and how its stakeholders will interact. It’s important to understand that a blockchain protocol is a process accompanied and even driven by change.

It is also important to understand the implications to all partner agencies’ day-to-day operations, as well as the assumptions and understandings of each partner prior to adoption. As noted earlier, blockchain can transform business models and processes. Failure to understand, anticipate, and plan for these changes not only risks missing out on performance improvement opportunities, but can also jeopardize implementation success.

In the IGT case, for each trading partner, these implications include internal reconciliation within existing systems, budget and fiscal schedules, risk decisions, and, most importantly, the alteration of other, potentially core business processes needed to implement and achieve blockchain’s benefits.

Since buyer and seller transactions would be maintained in a reliable, secure, and easily accessible distributed ledger, these IGT trading partners...
would be allowed to quickly identify root causes for IGT reconciling differences, allowing them to make the necessary corrections and more quickly meet reporting requirements. This, in turn, could help agencies reduce financial reporting risk over revenue and expenses, as well as minimize the time spent on dispute resolution for all parties involved. A long-term business impact could be the government’s ability to better utilize financial and nonfinancial performance data to inform the buy/sell agreements as they’re being structured.

To fully understand the business impacts, we should also consider the impact on the people and teams who will be affected by changes. The need for blockchain expertise and skills is discussed below; here the focus is on the many actors and activities that may be affected by the changes triggered by moving to a blockchain solution. Agency staff members will need at least some training and technical support to help them understand, adapt to, and/or use the new technology. In the end, readiness for blockchain is likely to depend more on the willingness to accept such changes than on potential technological constraints.

As you design a solution inclusive of blockchain, each stakeholder should identify and evaluate the touchpoints and interactions—of systems, people, and assets—on their existing business processes. Blockchain facilitates sharing a transaction layer through application programming interfaces (APIs), and therefore understanding which ones can be shared and the impact on your current business processes can help identify efficiency gains or overall changes to processes.

Talent: Do we have the right people?

Today, there don’t seem to be enough blockchain architects, software developers, and project managers with the expertise needed to handle projects from conception through implementation, in the public or the private sectors. While the talent pool is expected to increase as the technology becomes more ubiquitous, for now, talent poaching and project slowdowns are frequent problems. Before embarking on blockchain projects, agencies should take a clear-eyed look at the talent and resources required.

The first consideration is whether you have the talent needed to implement the blockchain application successfully. The current shortage of blockchain experience in government makes internal—external partnerships an attractive option. Subject matter experts from the operating side can provide valuable input that’s needed as much as blockchain experts who have experience with similar projects, such as intercompany payments. The operating experts can provide information about the intricacies of government regulations and procedures, as well as the security standards that the blockchain application must follow.

After the successful implementation of the blockchain application, you should ask if the agencies involved have the talent and training needed to sustain the system. When the application goes live, government IT staff must have the training needed to maintain it. This will require ongoing blockchain training, certifications (as they become available), and incentives to retain staff. Poorly maintained systems could lead to failure. In the IGT use case, the sustained availability of blockchain-specific skills may be a particularly difficult stumbling block at present, but there is always the possibility of outsourcing.

If you choose to outsource operations and maintenance, you should consider the ability and stability of third-party contractors. Clear service-level agreements can be crucial to ensure customer satisfaction. Clearly stated roles and responsibilities can help mitigate any potential conflicts.

Developing winning blockchain applications in the public sector
Compliance: Are we compliant with the current and future regulatory environment?

Consortium participants should establish their operating model according to existing regulations, while also preparing to adapt to future rules and regulations that may arise around blockchain technology. If two agencies have conflicting regulations for IT components that are important to blockchain technology, such as cloud computing, databases, or open-source software, it’s likely that they’ll need to spend a significant amount of effort to define integration points and identify potential risks well before implementation. In government, a pragmatic approach is recommended for resolving these issues before creating a pilot.

Integration is a common theme—integration among transactions, processes, IT infrastructure, and staff. In our discussions with federal leaders, a common concern is data security—that integration points aren’t creating vulnerabilities for closely held data. Thus, defining user access, key management, and the overarching data model are three important steps toward initial system design. Data stored on the blockchain itself is inherently cryptographically secure; the goal is to keep it from getting into the wrong hands.

Although government finance and IT regulations are not yet tailored to blockchain-specific applications, any solution would need to comply with existing standards and regulations, including the Federal Risk and Authorization Management Program (FedRAMP) standards. The FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization for, and continuous monitoring of cloud products and services. FedRAMP allows agencies to rapidly adapt from old, insecure legacy IT to secure and cost-effective cloud-based IT. As cloud services are key to blockchain’s infrastructure, FedRAMP standards can determine constraints or government-specific considerations for the technology stack.

Our IGT use case would have to also conform to the Economy Act. The Economy Act authorizes agencies to enter into agreements to obtain supplies or services from another agency. Through these inter-agency agreements, the servicing agency performs acquisition activities on the requesting agency’s behalf, such as awarding a contract, task order, or delivery order. In a blockchain-enabled IGT environment, compliance with the Economy Act and other interagency regulations could be woven into the system itself, streamlining regulatory reporting. This pattern of governmentwide requirements (for example, FedRAMP) and solution-specific rules and regulations (for instance, the Economy Act) will be common in government blockchain solutions.

Technology: High-level and tactical decisions for implementation

A blockchain application, however complex, is a piece of software and not a stand-alone solution. Any technical choices you make take place within the context of a broader operating environment, whether existing or new. A software protocol will define the rules and semantics used to communicate and exchange messages among computers. Today’s available blockchain protocols typically vary in terms of maturity, suitability, and technical requirements. But with many vendors and protocol options available, how do you make the right choices?

The key upfront factors affecting implementation are generally rooted in the relevant transaction life cycle, which typically, as in our IGT example, involves a diverse network of participants with varying roles, multiple IT environments, and several categories of transaction activities that must abide by unique rules.

INITIAL TECHNOLOGY FACTORS AFFECTING IMPLEMENTATION

Performance, scalability, and interoperability

When selecting a blockchain protocol, agencies should consider the need for both interoperability and scalability, to adjust to inevitable technological
changes over time. In the case of a government blockchain ecosystem, we urge leaders to imagine a landscape of shared, common blockchains, rather than disconnected, agency-operated chains, which would largely defeat the technology’s purpose. Defining the scope and scale of the solution as early as possible could be a key success factor in building blockchain solutions.

Begin by considering an acceptable performance standard for transaction processing, which may require a particular blockchain protocol and, more importantly, a specific consensus mechanism for partners. The consensus mechanism is intended to provide a fair, functional, reliable, and secure assurance that all the transactions occurring on the network are genuine. The consensus mechanism is tightly coupled with the overall performance of the protocol. Some of the most common consensus algorithms, such as those for cryptocurrency networks, are highly secure but have high energy requirements and longer transaction times—that is, confirmation may take 10 to 60 minutes. For high levels of transactions, the efficiency and energy cost of the consensus mechanism may be important determinants of scalability.

In fiscal year 2017, the Treasury’s Bureau of the Fiscal Service reported 1.2 million transactions among agencies managed through an interagency agreement, which averages to nearly one transaction every second. For IGT, given this high volume and that the project would only have agency participants known to each other, a permissioned protocol supporting a lightweight consensus mechanism could drive better performance through streamlined transaction validation, which could be the most efficient approach. The relationship between transaction volume and consensus is a key topic in government use cases, and in general, it may be most efficient to run much of business-focused applications on a permissioned network with a lightweight consensus mechanism.

The following tactical decisions depend largely on these initial decisions.

**Interaction with existing technology**

Members can use blockchain as a lightweight data integration layer, collecting information from legacy systems and external data sources via private or open APIs. Generally, it’s recommended to never store personal identification information or any other sensitive data on the blockchain; instead, consider storing a hash of encrypted data on the chain and the encrypted data either in a co-located, off-chain database or an existing source system. Sending large amounts of data to the blockchain can slow network performance, so a best practice is to use external databases to store data that doesn’t have to be captured by the blockchain.

A hash is a unique fingerprint of data that cannot be used to reconstruct the original data values. Using the hash allows parties to verify that the source data hasn’t been changed without exposing any part of the actual data on the blockchain. A blockchain solution also often requires integration with trusted external data sources, known as “oracles,” to draw information from existing systems securely and efficiently. This model would require working with each agency participant’s IT personnel to fully understand the source system’s and/or off-chain database’s architecture and design. The blockchain won’t replace these systems, but would serve as an immutable record of the data agencies need to record, execute, manage, and audit inter-agency transactions effectively.

For an IGT consortium, any legacy system that formally accepts the delivery of goods or services associated with IAAs can function as a primary oracle, feeding the blockchain time-stamped, encrypted information on senders, recipients, and goods/services delivered.

**Architectural choices at specific levels of the technology stack**

Consider using the following questions to guide discussions and identify the right solution for your needs at each layer of the technology platform or “technology stack” (figure 3). In our experience, the
blockchain protocol and application layers spark
the most conversations during initial, high-level
design discussions.

**Application layer**

Choices here are shaped largely by specific busi-
ness demands. Will it be necessary to create a native
mobile app, or can a web interface be made mobile-

---

**FIGURE 3**

**Asking the right questions can help identify the right blockchain solution at specific layers of the technology stack**

<table>
<thead>
<tr>
<th>Application layer</th>
<th>Services layer</th>
<th>User interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Middleware &amp; workflow management</td>
<td>Oracles</td>
</tr>
<tr>
<td></td>
<td>Module 1, Module 2, ... Module n</td>
<td>1, 2, ... n</td>
</tr>
<tr>
<td>Network and protocol</td>
<td>Blockchain abstraction layer</td>
<td></td>
</tr>
<tr>
<td>Infrastructure layer</td>
<td>Blockchain node</td>
<td>Legacy infrastructure</td>
</tr>
</tbody>
</table>

**Application layer**
- Should application interfaces use a native mobile app or a web-based app?
- Which device/OSs must be considered?

**Services layer**
- Which customizations are needed to support the project?
- What services options are available for stability and security?
- Which external data sources ("oracles") will feed into the blockchain?

**Network and protocol**
- Which protocol(s) should be used?
- Should you use closed or open source?
- How should interaction with the chosen API and user interface function?
- Which consensus mechanisms can be considered?

**Legacy infrastructure**
- What are the computing and consensus requirements?
- Which cloud provider ("backend-as-a-service") should be used?
- Which protocols does each provider support?

Source: Deloitte analysis.
friendly? A wide range of device types or operating systems, or plans to incorporate new ones in the future, might require cross-platform development tools. In general, developing a blockchain-based mobile or Web application is very similar to building a traditional software application. Traditional human-centered design, user experience, and Web/mobile application development practices can be key to building an intuitive solution that users find valuable. It isn’t a trivial detail for our IGT use case, however, and seamless integration into each user’s daily tasks is critical.

**Blockchain protocol layer**

Blockchain protocols often support specific business areas. For example, R3 Corda was designed primarily for financial services applications. Ethereum and Hyperledger, two open-source protocols, seem to have a wider array of uses; their ability to support customized business rules logic on top of the blockchain has made them two of the most widely adopted protocols for permissioned business applications.

For the IGT ecosystem, protocol options are limited to those that support a permissioned network and include lightweight consensus mechanisms, such as proof of authority (PoA) or Paxos consensus mechanisms—mechanisms that allow for known block signers (ensuring that only consortium members can create blocks), predictable block creation intervals (based on standard interactions between consortium members), and minimal transaction latency (for near-real-time data sharing). For our purposes, other, more energy-intensive and expensive consensus mechanisms such as proof of work (associated with “no-trust” ecosystems such as bitcoin) are not required due to the level of trust among participants.

Following the initial development of a blockchain application, we also frequently discuss the interoperability of multiple blockchain solutions and the ability to reuse one technology

---

**TABLE 2**

When assessing readiness, there are key questions to consider across six primary areas

<table>
<thead>
<tr>
<th>Consortium</th>
<th>Operation</th>
<th>Business impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Who should be involved?</td>
<td>• Who is responsible for managing and maintaining the platform?</td>
<td>• What are the implications to your day-to-day operations?</td>
</tr>
<tr>
<td>• What are the common goals of the consortium?</td>
<td>• How will the consortium scale?</td>
<td>• What are the partners’ assumptions and expectations about operational implications?</td>
</tr>
<tr>
<td>• Who owns it and who pays for it?</td>
<td>• How will existing agreements and contracts will be affected by changes?</td>
<td>• What is the impact to the people and teams who will be affected by the changes?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Talent</th>
<th>Compliance</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Do you have the talent needed to implement the blockchain application successfully?</td>
<td>• Does the operating model comply with existing regulations?</td>
<td>• What are the high-level needs for performance, scalability, and interoperability?</td>
</tr>
<tr>
<td>• Do the agencies involved have the talent and training needed to sustain the system?</td>
<td>• Does the system comply with existing regulations and how will it adapt to future regulations?</td>
<td>• How will you address the tactical considerations at each level of the technology stack?</td>
</tr>
<tr>
<td>• What is the ability and stability of third-party contractors?</td>
<td>• What are the new and existing data security considerations?</td>
<td>• Are blockchain solutions interoperable and can I reuse one technology stack?</td>
</tr>
</tbody>
</table>

Source: Deloitte analysis.
stack across multiple applications. While one may be tempted to reuse existing blockchain technology, tailoring the technology stack for each specific purpose typically provides the most value over time. That said, many situations could employ similar infrastructures and solution architecture components. If you hope to expand your use of blockchain over time and can already identify multiple, similar uses, we suggest starting with those rather than with other, more complex options. Our vision for the future of blockchain in government is focused on interoperability between networks and business partners.
Ongoing considerations

Lack of a federated identity

“Digital identity” is often defined as a mechanism for allowing individuals to securely interact within a network. In relation to blockchain, we’ve seen the value of an “asset-agnostic” approach, giving equal weight to the digital identity of humans and digital or physical objects.

One of the first challenges facing newly formed consortia is how to represent asset identities digitally. In government, each agency tends to interact with citizens in its own way, and each generally has different identity markers, many still paper-based. The lack of a unified, federated identity—a combination of attributes forming a coherent, shared, and widely accepted identity—hinders these agencies from seamlessly entering a blockchain consortium. To realize the full benefits of blockchain, they should understand and address the risks of federated digital identities (which we believe to be minimal), and explore approaches to unification.

Lack of reliable cost projections and analysis

Government agencies are subject to stringent cost controls, budget restrictions, and public accountability, and the benefits of any blockchain solution should be made clear and explicit before they can invest limited resources. To employ blockchain in government, agencies should make a case for quantifiable efficiency increases, reduced delays, and cost savings. Third-party companies and government should work together to show clear and measurable added value.
Conclusion
The challenges and rewards of early adoption

Blockchain is a foundational technology, which means it should be thought of in more than purely technology terms. As we have illustrated with the IGT example, while technology considerations will be important to successful blockchain applications in government, so will key questions concerning the members of the consortium, operations, business impacts, talent, technology, and compliance.

Working with a foundational technology in its early days can bring many challenges, but can offer far greater rewards. Blockchain offers government organizations an opportunity for true collaboration and transformation. Small, wisely chosen implementations could give agencies a chance to define solid blockchain implementations, address common issues, and deepen connections with other members of their consortia. Early adopters could see the benefits sooner than most, while potentially establishing themselves as leaders in areas that should only grow in importance over time. The factors outlined in this paper are intended to help leaders identify and implement winning blockchain applications in government. And those winning blockchain applications have the potential to reduce costs, speed outcomes, and lower barriers across the public sector.
Endnotes


2. Ibid.


Contacts

**Wendy Henry**  
Government and Public Services  
Blockchain leader, US  
Specialist leader  
Deloitte Consulting LLP  
+1 202 213 1327  
wehenry@deloitte.com

**Kevin Armstrong**  
Government & Public Services  
Blockchain leader, Global  
Partner  
Deloitte Consulting LLP  
+1 250 686 4848  
karmstrong@deloitte.ca