



The Joint Financial Management  
Improvement Program

# Harnessing Blockchain in the Federal Government

Key Considerations for  
Financial Management &  
Information Systems

---

## Table of Contents

Foreword .....	1
Executive Summary .....	3
Exploring IT Considerations for Blockchain .....	3
Exploring Blockchain Considerations for Federal Financial Management, Human Capital, and Oversight .....	6
Introduction .....	7
Background .....	9
Understanding Blockchain Technology .....	9
Decentralized Nature of Blockchain.....	9
Consensus Mechanism.....	11
Smart Contracts.....	15
Digital Ledger .....	15
Determining Whether Blockchain Technology May Be Useful to an Agency .....	16
Federal Grants Management and Its Challenges .....	17
How JFMIP Arrived at the Federal Research Grants Use Case.....	21
The Blockchain Grants Financial Management Prototype.....	24
Blockchain Prototype Architecture.....	24
Design, Development, and Deployment of the Prototype .....	24
Outcomes of the Prototype.....	28
Knowledge Gained .....	29
IT Considerations .....	29
Financial Management, Human Capital, and Oversight Considerations ...	30
Foundational Knowledge Base .....	30
IT Considerations for Agencies in Using Blockchain .....	32
Infrastructure Layer .....	32
Network and Protocol Layer.....	33
Services Layer .....	33
User Interface Layer .....	36
Available Prototype User Actions and Potential Future Improvements ...	36
Managed Service Factors .....	38
Cybersecurity Factors .....	39
Authority-to-Operate Considerations.....	45
Multi-Agency ATO Considerations .....	47

Operational Considerations.....	48
Business Processes .....	48
Testing .....	49
User Experience .....	49
Infrastructure .....	50
Security.....	50
Industry Best Practices .....	50
Interoperability .....	51
Data Standardization .....	51
Shared Service Factors .....	52
Potential Implications of Blockchain Use for Federal Financial Management, Human Capital, and Oversight .....	54
Federal Financial Management .....	54
Governance.....	55
Human Capital.....	57
Oversight.....	59
Audit Planning Factors.....	61
Audit Evidence and Resource Factors .....	65
Blockchain’s Effect on Audit Resources.....	72
GAO’s Read-Only Node on the Grants Financial Management Prototype .....	74
Appendix I: Methodology.....	76
Appendix II: Technical Details of Blockchain Prototype.....	84
Appendix III: Additional Information on Related Laws, Regulations, and OMB Guidance .....	88
Appendix IV: Abbreviations .....	94
Appendix V: Glossary .....	95
Appendix VI: Contacts and Acknowledgments .....	98

---

## Foreword

**Blockchain** has entrenched itself into the media over the past several years. With part fascination and part apprehension, the world has seen a stream of headlines about its various uses, including cryptocurrencies, non-fungible tokens, and smart contracts. The core concept of a blockchain is grounded in the idea of decentralization and independent checks by participants wherein multiple 'peers' or 'nodes' in the network validate each transaction, ensuring greater transparency and data integrity. Use of cryptocurrency is not required for every use case and was not part of this initiative.

Blockchain technology is still in an early stage of evolution, and clarity is needed on its use within the federal government. Using blockchain in financial management offers potential opportunities for efficiencies, transparency, workforce flexibility, and data integrity. Understanding government-wide blockchain considerations in the areas of information technology, federal financial management, human capital, and oversight is critical to potential implementations.

In August 2021, the Joint Financial Management Improvement Program (JFMIP)—a cooperative venture between the Department of the Treasury (Treasury), the Government Accountability Office (GAO), the Office of Management and Budget (OMB), and the Office of Personnel Management (OPM)—began an initiative to expand a blockchain prototype from a single-organization network at Treasury to a two-organization network involving Treasury and GAO. Moving to a multi-agency approach would enable us to better understand government-wide considerations for this technology.

The JFMIP chose to test the prototype using the area of financial management of federal research grants. The grants financial management area can often be burdensome and frequently does not provide timely information to stakeholders. Accordingly, using it in a blockchain prototype could reveal potential improvements.

This report examines blockchain's challenges and opportunities and highlights key considerations for implementing a blockchain. Such considerations address the areas of information technology, federal financial management, human capital, and oversight.

Agency management, including Chief Financial Officers and Chief Information Officers, program managers and staff; entities receiving federal funding; and

federal auditors may find the blockchain considerations in this report to be useful. The JFMIP envisions this document as a learning tool for the federal financial management community in preparing for a future when blockchain is in use.

The JFMIP wants to thank the diverse group of experts across government and industry who contributed to this report. Their expertise was invaluable in developing this report.



Gene Dodaro  
Comptroller General  
U.S. Government Accountability Office



Deidre Harrison  
Deputy Controller  
Office of Federal Financial Management  
Office of Management and Budget



Dave Lebryk  
Fiscal Assistant Secretary  
U.S. Department of the Treasury



Katie Malague  
Chief Management Officer  
Office of Personnel Management



---

## Executive Summary

The JFMIP is a cooperative venture between Treasury, GAO, OMB, and OPM with the mission of promoting the continuous improvement of federal financial management.<sup>1</sup>

This report documents the JFMIP's efforts to develop a foundational knowledge base to inform potential future blockchain implementation efforts. Using Treasury's Bureau of the Fiscal Service (Fiscal Service) blockchain prototype for the federal grants financial management process, this report provides information technology (IT) considerations for a potential multi-agency blockchain, including cybersecurity, authority-to-operate, and operational factors. The report also explores potential federal financial management, human capital, and oversight efficiencies and challenges.

Based on the experience of this initiative and our learning from engaging with the prototype, the JFMIP has three central themes to take away from this report: (1) more work is likely needed to prepare the federal government for interagency blockchains, (2) those agencies beginning to consider the process of implementing blockchain solutions should carefully compare the potential costs and challenges to the benefits of the technology and proceed accordingly, and (3) JFMIP and other federal entities are contributing to a growing body of knowledge on blockchain, which can give other agencies a head start in their decision-making process.

---

## Exploring IT Considerations for Blockchain

The JFMIP's work on the blockchain prototype has shown that blockchain technology has the potential to bring greater automation and transparency to federal grants financial management processes. However, IT challenges including governance and data standardization remain. This report details how we used a blockchain prototype to automatically track federal grant funding as it flowed from agencies to grantees and sub-grantees, with financial transparency for all users. By creating a digital asset, or "token," to represent an awarded grant on the blockchain, we showed that value can be easily transferred between the grantee and sub-grantee. We also demonstrated that all actions performed on the grant are recorded in a secure digital ledger that

---

<sup>1</sup>The Budget Accounting and Procedures Act of 1950 gave statutory authorization to the JFMIP agencies to conduct a continuous program for the improvement of accounting and financial reporting in government. See 31 U.S.C. § 3511(d).

cannot be altered or deleted. The blockchain's transparency allows involved parties to view aspects of a grant's life cycle appropriate for the level of their access privileges.

### **Digital Assets and the Grants Financial Management Blockchain Prototype**

- **The use of blockchain in the grants financial management process involves tracking “tokenized” grants when the agency awards the tokens to a non-federal entity.**
- **The grants financial management blockchain prototype is designed to track all financial transactions for the grants.**
- **In this report, the term digital assets refers to tokens that have been awarded to grant recipients, but may be defined differently for other blockchain use cases.**

**Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01**

The JFMIP team found in the prototype that blockchain technology could effectively maintain data integrity and confidentiality through cryptography. This would help ensure that data remain tamper-resistant, secure, and confidential, providing federal agencies with an added layer of security and control over their data. While data integrity and confidentiality are promising for the prototype, a lack of government-wide data standardization would make it difficult to implement a scalable solution.<sup>2</sup> In addition, the JFMIP team found that hosting the blockchain in the cloud provides several benefits, including reliable access for federal agencies, grantees, and sub-grantees, the ability to use managed service blockchains, and cybersecurity protections built into the cloud service we used.

Establishing a blockchain for federal use, however, would be a complex task requiring meticulous planning, execution, and coordination among all parties

---

<sup>2</sup>Scalability refers to the ability to expand the network, such as in the case of the JFMIP's initiative to expand the prototype from one agency to another. Scalability also refers to the ability to add more users to the blockchain.

involved. Many blockchains, like the grants financial management blockchain prototype, would also rely on "smart contracts." These contracts are software code stored on a blockchain that contains a set of conditions, so that transactions automatically trigger when the conditions are met. Such contracts are highly inflexible and require precise programming to avoid errors that could result in improper transfers.

Furthermore, a coordinated effort from all participating agencies would be required to achieve a multi-agency authority-to-operate (ATO).<sup>3</sup> A convening agency would take the lead in setting up and managing the blockchain network, establishing access controls, and coordinating with the consortium of agencies and other participants on the blockchain. The convening agency would also be responsible for ensuring that all necessary security controls are implemented and that all participating agencies have access to the information and resources they require to achieve their own ATO.<sup>4</sup>

Cybersecurity has been designated as a government-wide high-risk area by GAO for over 25 years. It remains an area requiring urgent actions to protect the systems and data essential to the federal government and key critical infrastructures such as health care, energy, and banking and finance.<sup>5</sup> Accordingly, ongoing cybersecurity challenges will need to be considered as a key element of implementing an interagency blockchain.

While blockchain technology could assist with the financial management of grants use case, it should be stressed that the purpose of the prototype was not to stand up a grants solution at this juncture but rather to inform future blockchain implementation efforts for any potential use case. To consider taking this prototype to a pilot, an analysis of alternatives and further evaluation would be necessary to determine the appropriate solution that addresses challenges and considerations.

---

<sup>3</sup>ATO is the formal authorization for an IT system within federal agencies, granted by the designated authorizing official, such as the Chief Information Security Officer (CISO). This involves assessing security controls, evaluating risks, and ensuring secure and approved operations.

<sup>4</sup>In this report, a "convening agency" is the agency taking the lead in setting up and managing the blockchain network, establishing access controls, and coordinating with other consortium members for activities such as obtaining an ATO.

<sup>5</sup>GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 2023).



---

## Exploring Blockchain Considerations for Federal Financial Management, Human Capital, and Oversight

For federal financial management, implementing blockchain at federal agencies has the potential to increase transparency, reduce financial disputes between parties, and reduce the complexity of reconciliations. For example, grantees submit various financial reports to the federal government, which are compared to the relevant financial records. Differences can occur due to the timing of when entities post transactions in their separate systems. A blockchain-based financial management system could provide one integrated and validated data source that could be used by all stakeholders. This could make this process more efficient and alleviate timing differences.

However, blockchain would not prevent misstatements or users' failures to enter valid transactions, nor would it likely contain all the information needed to record properly all valid transactions or events. Before implementing blockchain, federal agencies must determine if a blockchain is the appropriate solution for the problem being solved. They also must agree on who the participants will be; how the blockchain will be constructed, governed, and operated; and what the common set of requirements will be.

With respect to blockchain's potential impact on the federal workforce, the tenets of OPM's Future of the Workforce vision are built to be robust, independent of individual technologies.<sup>6</sup> Consequently, there are no broad concerns for human capital presented from the use of blockchain technology. The suite of financial management requirements already includes many technologies and reporting methods. The addition of another type of technology is not predicted to cause major shifts in job series or classifications.

Finally, implementing blockchain at federal agencies could also involve both benefits and challenges for oversight. Consequently, federal auditors may want to consider the effect of a particular blockchain's design and implementation when planning audits. Blockchain could streamline the audit process and improve the integrity of data. However, blockchain does not guarantee reliable data and fraud-free or error-free financial reporting and cannot replace professional judgment.

---

<sup>6</sup>See OPM, The Future of the Workforce, accessed Aug. 27, 2023, <https://www.opm.gov/policy-data-oversight/future-of-the-workforce>.

---

## Introduction

The efficient management of federal grants is a top government priority, but it is complex and time-consuming due in part to reporting requirements for both grant recipients and grant-making agencies. Federal grant spending has been on a steady rise in recent years. In 2022, the federal government distributed \$1.2 trillion in grants to state and local governments, which represented 4.8 percent of gross domestic product (GDP). Since the year 2000, federal grants to state and local governments have annually averaged 3.6 percent of GDP.

Current grants financial management processes have led to several challenges for the federal government and grant recipients.<sup>7</sup> For example, agencies and recipients utilize various drawdown and reporting systems to perform grants financial management processes resulting in inconsistent processes and redundancies. The current environment does not provide timely visibility into the sub-grantees receiving federal grants, which makes tracking federal grant funding a complex and time-consuming effort. Furthermore, with every grant award, there are significant administrative, compliance, and reporting requirements for both grant recipients and grant-making agencies.

Various organizations both within and outside the federal government have discussed blockchain technology as a potential option to address these challenges. For example, the MITRE Corporation issued a report in 2019 that assessed the potential to improve grants management by using blockchain technology.<sup>8</sup> That study found improvements in grant management can be enabled using blockchain technology, but actions related to policy changes, improved data analytics, and the protection of sensitive information will be needed to achieve the identified benefits.

In 2019, Fiscal Service built a prototype to further explore the viability of blockchain as a solution to current grants financial management process challenges. However, establishing a blockchain use case for federal financial management creates several considerations for agencies, especially if it is built

---

<sup>7</sup>To research and identify problem areas in the federal grants financial management process blockchain could address, Fiscal Service organized a number of informational meetings, symposiums, and presentations with grant stakeholders at various organizations and agencies. Fiscal Service intended to capture recurring issues identified across all areas of federal grants financial management; and to then work on addressing them with the grants management blockchain prototype.

<sup>8</sup>The MITRE Corporation, *Report - Assessing the Potential to Improve Grants Management Using Blockchain Technology*, June 2019. The MITRE Corporation is a not-for-profit research and development company that focuses on challenges in the civil and defense domains.

as a multi-agency blockchain. To explore these blockchain considerations, in August 2021, leadership from the four JFMIP agencies convened and decided to expand the architecture of Treasury's blockchain prototype across agency boundaries to GAO.

To explore IT considerations for agencies using blockchain, the process of expansion was documented and studied by subject-matter experts at Treasury, GAO, and OPM. This included documenting programming issues, process bottlenecks, and challenges. These challenges, as well as attempts at their resolution, served as a foundational source of knowledge for many of the topics in this report. The JFMIP also interviewed experts and reviewed publications on blockchain to understand better the results of the prototype's expansion.

Additionally, to explore potential implications of blockchain use in the areas of federal financial management, human capital, and oversight, the JFMIP interviewed blockchain experts at a variety of public accounting firms, inspector general offices, and agencies. This allowed us to understand better the possibilities blockchain may provide federal financial managers and auditors, as well as challenges to blockchain implementation both in a grants use case as well as other use cases throughout government. The JFMIP also reviewed academic journals and other publications that explore blockchain's potential impact on financial management and oversight.

This report is a summary of the knowledge acquired through the building and expanding of Treasury's blockchain prototype, as well as our interviews with experts, and research into blockchain's implications for federal financial management, human capital, and oversight. See appendix I for a full discussion of our methodology. However, the considerations provided in this report are for illustrative purposes only and are not exhaustive of all considerations, or indicative of an optimal framework to approach assessing blockchain's use at any particular agency or office. Accordingly, the following limitations apply to this report.

- This report is not prescriptive.
- This report is not exhaustive when it comes to technology options.
- This report should not be interpreted as policy or recommendations.
- The initiative did not involve or affect any actual grant transactions.

---

## Background

Understanding blockchain’s considerations for federal agencies requires an explanation of key concepts of decentralization, consensus mechanisms, and digital ledgers. A blockchain is a decentralized digital ledger designed to enhance the security and permanence of transactions. To research this technology further, the JFMIP sought out a complex area of federal financial management to understand the potential impact of a blockchain in addressing financial management challenges. The JFMIP identified federal grants management as a suitable area for exploration, given blockchain’s potential usefulness to this process and our access to a grants management blockchain prototype already built at Fiscal Service. The JFMIP sought to better understand blockchain through the testing of this prototype and gather insights into how blockchain could be used in federal grants management.

---

## Understanding Blockchain Technology

A blockchain is a secure way of conducting and recording transfers of digital assets without the need for a central authority. The technology is “distributed” because multiple participants (individuals, businesses, etc.) share and synchronize copies of a digital ledger. New transactions are added in a manner that is cryptographically secured, permanent, and visible to all participants in near real time.<sup>9</sup>

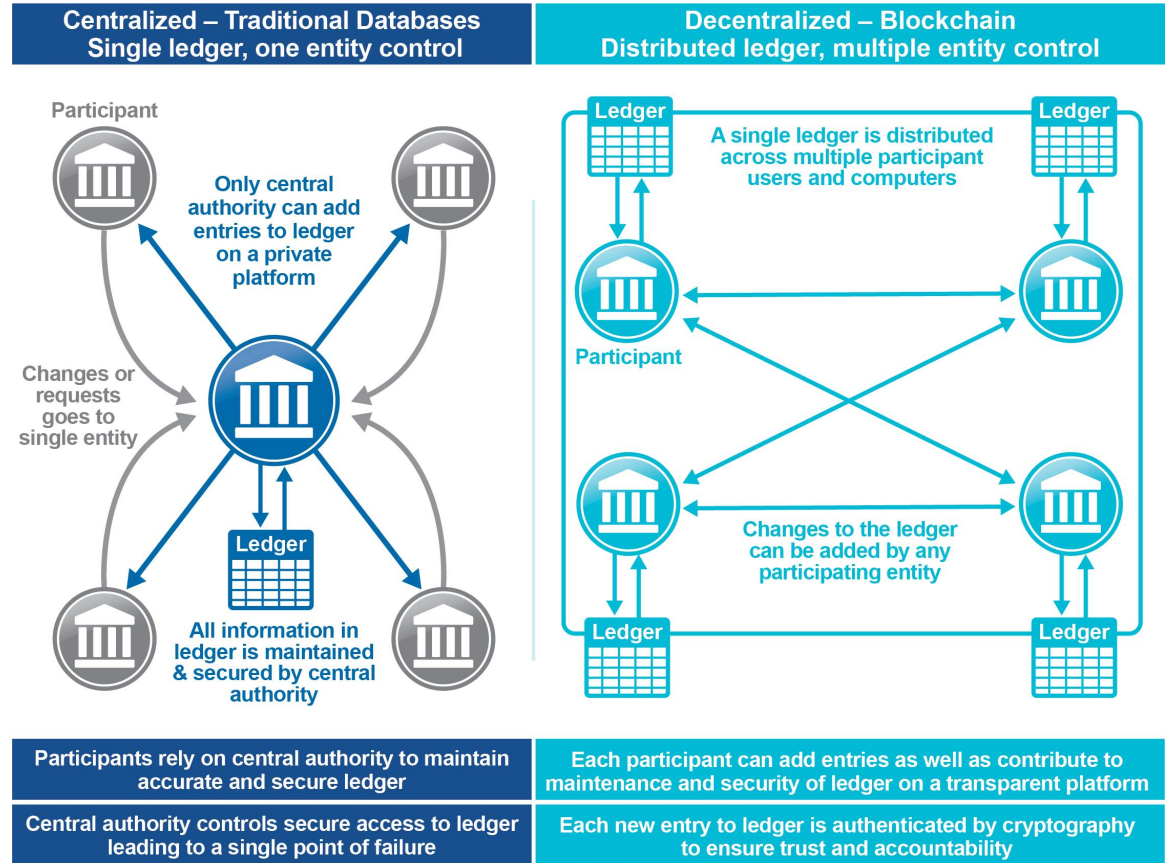
### Decentralized Nature of Blockchain

Decentralization is the defining feature of a blockchain. Users can create or view records without the need for an intermediary or central authority. Blockchain technology offers mechanisms that aim to reduce the risk of fraudulent or malicious activities on the ledger. The ledger is duplicated across all participants, ensuring everyone has access to identical information. Once a transaction is recorded, it cannot be deleted. Blockchains can also limit access to known participants. These safeguards collectively ensure that the technology provides a more secure, tamper-resistant method of recording and storing data. The differences between decentralized and centralized approaches are shown in Figure 1.

---

<sup>9</sup>Cryptography is the practice of using codes and special methods to secure and protect information so only the intended people can understand it.

**Figure 1: Blockchain’s Decentralization**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

Blockchain can be viewed in a similar fashion to those official letters used for important communications years ago that were sealed with wax and an emblem. If anyone tried to open the letter, the seal would break, leaving behind clear evidence of tampering. Similarly, with blockchain, once data are added, any attempt to change it becomes evident to all participants due to the cryptographic links between blocks.<sup>10</sup>

Unlike traditional transaction models, which require participants to store their own records or use a third-party intermediary, everyone on the blockchain network always has access to the records. This eliminates the need for users to store information on their local systems or a centralized database. The risk of fraud going undetected is reduced since any tampering

<sup>10</sup>Cryptography is essentially the protection of information using mathematical functions, collectively referred to as encryption. Central to cryptography’s effectiveness are “keys,” which are a series of characters that can be either public or private. Keys can lock (encrypt) or unlock (decrypt) the protected information.



attempts would need to occur across a network of computers held by different parties, making it a highly impractical endeavor for malicious activities.

Blockchain duplicates data on asset ownership and transactions among multiple computers and users, known as nodes, minimizing the likelihood of network compromise, or tampering.<sup>11</sup> Even if a malicious hacker compromises a node, the remaining nodes on the blockchain will automatically identify the transactions from the compromised node as invalid.

## Consensus Mechanism

Blockchain uses a consensus mechanism to ensure that each transaction is genuine and correct.<sup>12</sup> This means that before a transaction can be considered valid, it must be approved by a standardized method, in which many computers on the blockchain network agree on its authenticity.<sup>13</sup> The process can be executed through various methods, such as Proof of Work, Proof of Stake, and Proof of Authority, each adhering to specific rules.

- **Proof of Work** requires large amounts of computing power and energy to generate a new transaction on the blockchain (also known as “mining”). This large amount of computing power makes it more difficult and costly for bad actors to individually update the blockchain.
- **Proof of Stake** enables the verification of transactions by only allowing nodes to add new transactions in proportion to how much they have previously invested or “staked” into the blockchain. This makes it difficult for bad actors to generate new transactions without significant investment beforehand.

---

<sup>11</sup>A blockchain node is a computer or device connected to a blockchain network. It stores and shares a copy of the entire blockchain with other nodes in the network, helping to maintain the integrity and security of the data. Nodes can participate in verifying transactions and adding them to the blockchain and can also perform other tasks such as hosting smart contracts.

<sup>12</sup>Consensus mechanism is a way for a blockchain to verify that a transaction is valid by having many computers on the network agree that the transaction is genuine and authentic before it is considered valid.

<sup>13</sup>A standardized method consists of a predefined set of rules and procedures that have been agreed upon by network participants. These rules ensure that transactions are processed consistently and predictably, with all network participants adhering to the same guidelines.

- **Proof of Authority** limits blockchain network access to only a group of trusted nodes, thereby ensuring that only authorized entities can add or validate transactions. This limitation maintains the ledger's integrity and provides added security.

The network's agreement on which method to use can be built in a variety of ways, but the goal is to prevent bad actors from cheating and to ensure that changes are verified by other users. This is analogous to a book club where members must agree on a book before it is read.

Blockchains are divided into two categories: permissionless and permissioned. The permission setting controls who can access, read, and write to the blockchain.

- **Permissionless** blockchains allow anyone to contribute data. This means that every transaction is visible and accessible to every network participant. However, this means that any sensitive data entered are completely exposed, which can be a privacy and security concern.
- **Permissioned** blockchains are privately operated, and only authorized users are allowed to access the network. In a privately operated network, participation in the blockchain is governed by a set of rules established by a committed group or “consortium,”<sup>14</sup> and the public cannot access it.<sup>15</sup>

Traditional databases support four general operations on a record – create, read, update, and delete – while blockchain only has read and create operations on a record, making it virtually impossible to remove or change a data record.<sup>16</sup> This comparison is illustrated in Table 1.

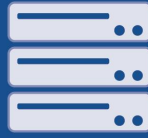

---

<sup>14</sup>A committed group or consortium on a permissioned blockchain refers to the approved users who establish the rules and manage participation in the privately operated network.

<sup>15</sup>Classified information requires specialized security measures and protocols beyond the restrictions of permissioned blockchains.

<sup>16</sup>A traditional database is a centralized system that stores financial data in a structured format. Access to this data is controlled by a central authority and updates are processed by the same authority.

**Table 1: Comparison between Databases and Blockchain**

	 <b>Centralized Database Systems</b>	 <b>Blockchain Networks</b>
<b>Structure</b>	Centralized ownership; administrator controls access and integrity of data	Decentralized ownership; no single point of failure
<b>Transactions</b>	Four major actions- create, read, update, and delete	Two major actions- create and read
<b>Data integrity</b>	Encrypted data and robust access controls	Encrypted data using cryptography and consensus mechanisms to protect data

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

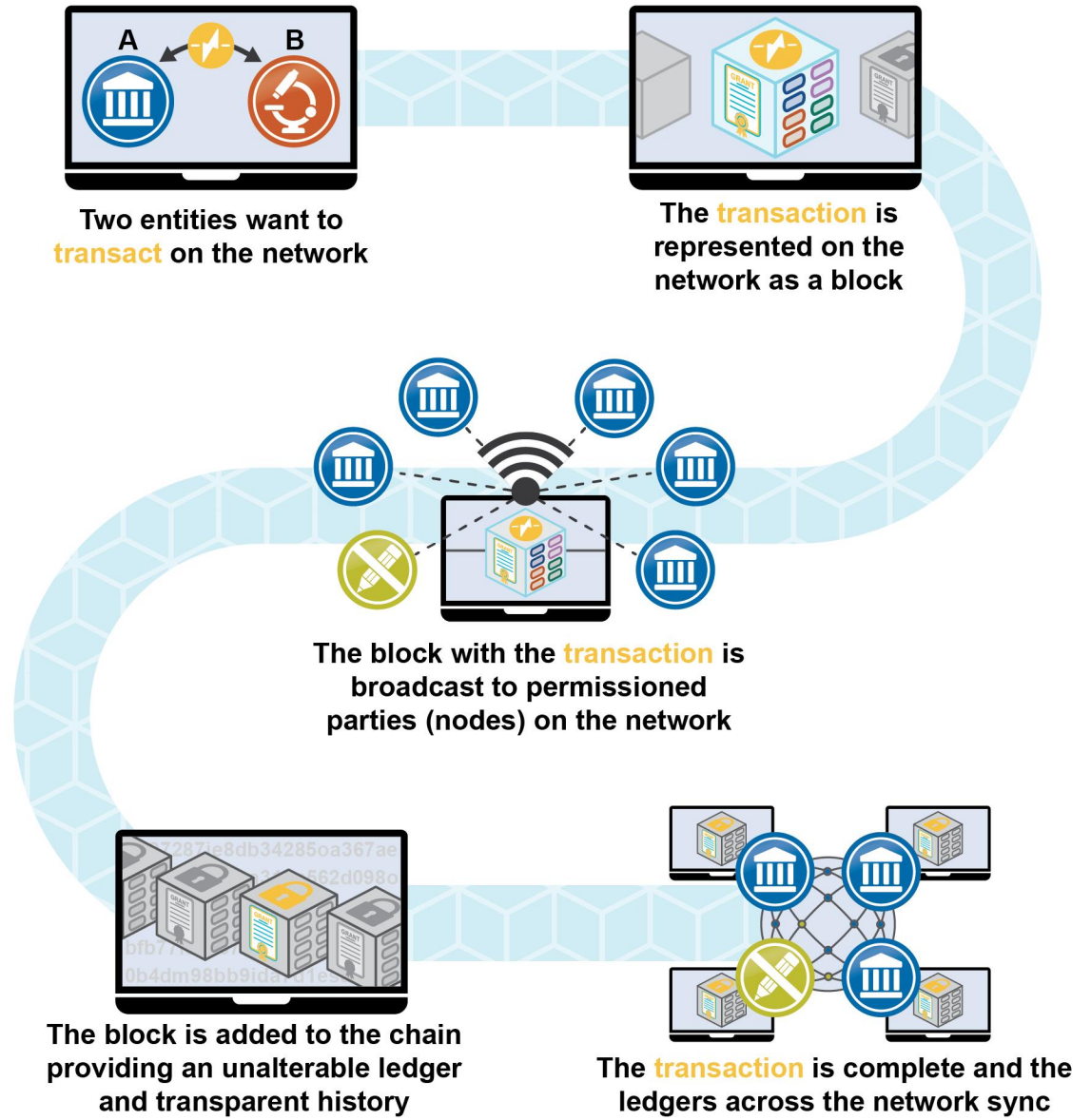
To create its tamper-resistant ledger, blockchain technology groups transactions into *blocks*.<sup>17</sup> It then calculates a number, known as a *hash digest*,<sup>18</sup> based on data from those transactions and from data in the previous block. This operation effectively *chains* the blocks together.<sup>19</sup> If any of the existing data in the blockchain is changed, the hash digests of that block will no longer match, and the system blockchain will reject the change. This ensures that all synchronized versions of the ledger are consistent and the blockchain will notify all users about the rejected change. This results in secure and unalterable records because the hash digest provides integrity checks against other blocks to prevent the records from being changed. The process is illustrated below.

<sup>17</sup>A block is a collection of data in a blockchain that includes transactions and a unique identifier called a hash. It serves as a building block for the blockchain, adding new data as each block is created and linked to the previous ones.

<sup>18</sup>A hash digest is like a digital fingerprint that uniquely identifies a block of data on a blockchain. It makes it hard for someone to tamper with the data because any change would alter the fingerprint and be easy to spot.

<sup>19</sup>Chains are used to connect blocks of data, providing a secure and tamper-resistant record of transactions, similar to a pearl necklace that cannot be altered without breaking the string.

Figure 2: Process Illustrating How Blocks Are Created and Linked



 : Agency
  : Grantee
  : Read-only

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

## Smart Contracts

Smart contracts are not contracts in the legal sense of the term.<sup>20</sup> Rather, they are tools to extend the functionality of a blockchain beyond recording transactions. They operate by executing basic logic "if...then..." phrases encoded into the blockchain code. When predetermined conditions are met and validated, a network of computers executes the actions. These actions could include tracking grant transactions among the authorized parties. When the transaction is completed, the blockchain is updated. This means that the transaction cannot be modified, and the results are only visible to parties who have been granted permission.

Smart contracts are used to automatically transfer digital assets on the blockchain if certain conditions are met. They can also be used to apply internal controls or business rules, such as checking the user's access permissions or verifying the availability of funds. Smart contracts consist of code and data that can automatically run on the blockchain using cryptographically signed transactions.<sup>21</sup> Multiple nodes execute the code, and if all nodes derive the same answer, a node records the result to the blockchain.

## Digital Ledger

A ledger is used to track financial transactions, including settlement (asset transfer) and reconciliation (accuracy verification). Errors can occur when an entity unintentionally records the same transaction twice in its financial records, resulting in an overstatement or understatement of accounts. This can result in misleading information on the entities' financial statements.

Blockchain addresses the issue of duplicate transactions with the use of digital signatures where each transaction is unique and verified by multiple nodes on the network. Also, duplicate transactions can be identified by the smart contract logic and handled according to the business requirements contained in the logic.

---

<sup>20</sup>U.S. jurisdictions vary on the recognition of smart contracts as legally binding contracts and the enforcement of smart contract terms.

<sup>21</sup>Cryptographically signed refers to a method of using mathematical algorithms to verify the authenticity of a transaction or contract on the blockchain.



---

## Determining Whether Blockchain Technology May Be Useful to an Agency

Blockchain may be useful for some agencies' current financial management processes. However, its utility may be limited or even problematic for other processes. Financial management processes involving many distributed participants or transactional workflow such as management of a supply chain might find substantial utility in blockchain technology. On the other hand, processes with relatively few participants, who all trust each other, might find the use of a blockchain to be unnecessarily complex. Agencies considering blockchain technology likely need to perform an analysis of both their organizational capacity, and the specific requirements of the impacted financial management processes, to better understand blockchain's utility in each case.

GAO published a technology assessment in March 2022 that provides an overview of the potential benefits and challenges of blockchain in federal agencies.<sup>22</sup> The report provides a flowchart with questions that can be answered by federal agencies in determining whether a blockchain may be useful.<sup>23</sup> Some of the questions GAO listed for agencies to consider include:

- Does the agency need a distributed, historical data store?
- Will more than one organization contribute data?
- Is the agency able to share all data among all users of the blockchain for all time?

GAO found that blockchain can be effective in some cases, but also potentially limiting or even detrimental in other cases where traditional spreadsheets and databases may be more useful.<sup>24</sup> The report also offers other important considerations in weighing the benefits and challenges of blockchain for a

---

<sup>22</sup>GAO, *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges*. GAO-22-104625 (Washington, D.C.: Mar. 23, 2022).

<sup>23</sup>In GAO's report GAO-22-104625, "Figure 2: Flowchart for determining whether blockchain may be useful," provides a flowchart to determine whether a given blockchain use case would be useful to an agency.

<sup>24</sup>GAO-22-104625. GAO found potential challenges and limitations in a number of blockchain-based use cases. For example, GAO found that using blockchain to address perceived and actual threats to computerized voting may not address all current challenges and could introduce new vulnerabilities. These vulnerabilities include additional points of attack via the many nodes on a blockchain and potentially compromising voter anonymity by linking votes to a voter's identity through the blockchain's time stamps.

given application. For additional information on blockchain technology, please see the other articles listed in appendix I.

---

## Federal Grants Management and Its Challenges

For additional context, federal grants have grown considerably in value and complexity, which makes grants management an increasingly important function for federal financial managers. There were over 900 grant programs offered by 26 federal agencies amounting to approximately \$700 billion in grants and cooperative agreements in fiscal year 2018. This accounted for almost 17 percent of the federal government's total spending and 3.3 percent of fiscal year 2018 GDP. The amount of grants had grown to approximately \$1.2 trillion in fiscal year 2022. Emergency funding and related efforts to address the COVID-19 pandemic, as well as recent legislation such as the Infrastructure Investment and Jobs Act,<sup>25</sup> caused a massive increase in federal grants to meet a diverse set of urgent needs. These needs included COVID-19 testing, housing assistance, and road and bridge repairs—in addition to the normally issued federal grants.

In addition to these urgent needs, federal grants can also serve the nation's fiscal health. In September 2023, GAO reported that unemployment insurance fraud was likely between \$100 billion to \$135 billion during the COVID-19 pandemic.<sup>26</sup> As of July 2023, the Department of Labor has issued \$1.4 billion in grants to states for initiatives including fraud prevention, detection, investigation, and recovery.

The increase in grant programs and funding has contributed to complexity in the federal grants management processes. This has resulted in an increased burden and cost of grants management for agencies and grantees.

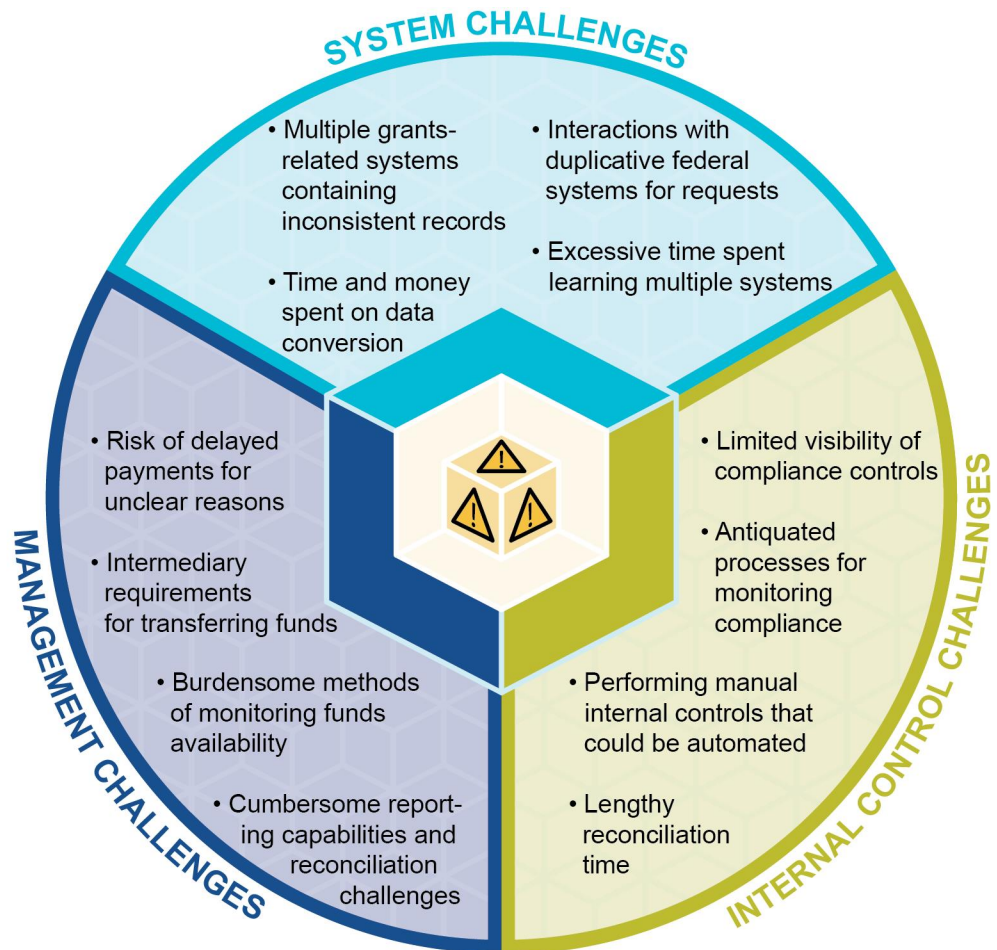
The federal government's current grants financial management process faces several challenges. Figure 3 illustrates these challenges.

---

<sup>25</sup>Pub. L. No. 117-58, 135 Stat. 429 (2021).

<sup>26</sup>GAO, *Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely Between \$100 Billion and \$135 Billion*, GAO-23-106696 (Washington, D.C.: Sept. 2023).

**Figure 3: Current Financial Management Challenges with the Federal Research Grants Process**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

Key stakeholders identified in the proposed blockchain use case face challenges, as highlighted in Figure 3. To identify these challenges, the Office of Financial Innovation and Transformation (FIT) within Fiscal Service engaged a broad group of grant stakeholders, including Treasury internal officials, federal agencies that provide grants, grant recipients and sub-recipients, and subject matter experts. This engagement consisted of dozens of discussions and workshops with these organizations.

Figure 4 illustrates the current state of the federal research grants financial management process. Currently, when a grantee is ready to request funds to carry out the work of the grant, the grantee goes to one of several grant systems to submit their request. Once the request is approved, the automated

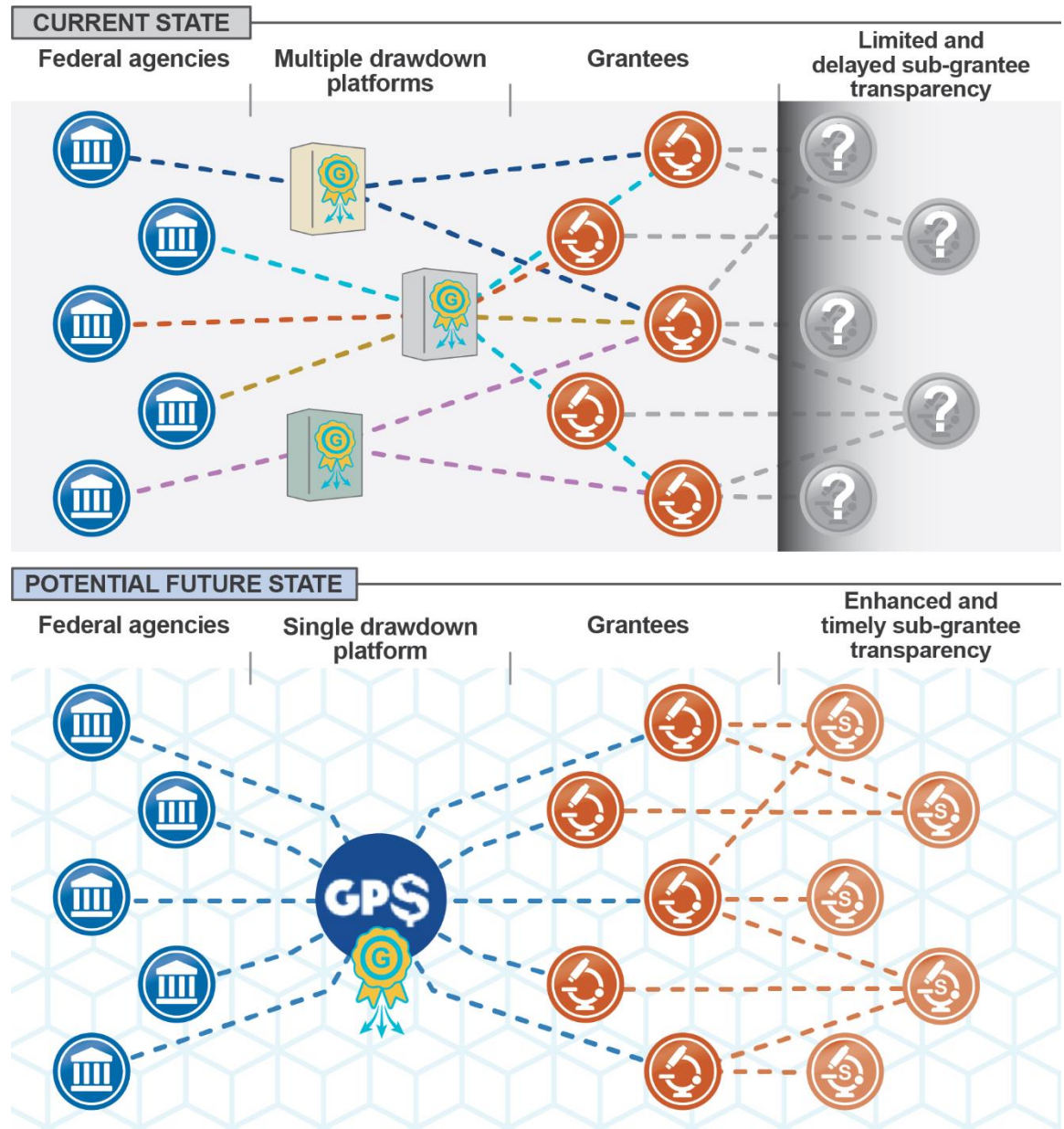
clearing house network moves the money from the Treasury, or the federal government's bank account, to the grantee's bank account.<sup>27</sup> Federal systems generally do not include information on the subsequent sub-grantees or the related transaction history. Tracking federal grant funding can therefore be a complex and time-consuming effort. Furthermore, with every grant award, there are significant administrative and reporting requirements for both grant recipients and the grant-making agencies. For example, a 2018 survey of university academic researchers revealed that researchers spend 44 percent of their time performing compliance tasks for their grants, including meeting their financial management requirements.<sup>28</sup>

---

<sup>27</sup>The automated clearing house, or ACH, network is the primary system used for electronic funds transfer by many entities, both governmental and non-governmental.

<sup>28</sup>IBM, Center for the Business of Government, *Reducing Administrative Burden in Federal Research Grants to Universities* (2020).

**Figure 4: Federal Research Grants Financial Management Process - Current State and Potential Future State**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

The lower section of Figure 4 shows a potential future state of the financial management process with a single drawdown platform based on a blockchain system. This model provides transparency into the financial process down to the sub-grantee level, standardizes the drawdown process, eliminates or significantly reduces reconciliations, and streamlines reporting. Having all the information on the blockchain allows for more consistent and



streamlined processes. The use of blockchain technology and tokens provides authorized users with one integrated and validated data source that could be used by all parties. This allows sub-grantee data to be available at the time of the transaction, compared to the current process that requires separate monthly reporting.

### **A Single Drawdown Platform: Would a Grants Financial Management Blockchain Be Truly Decentralized?**

A key proposed benefit of the grants financial management blockchain prototype is that it allows for a single drawdown platform to be used by all granting agencies and grant recipients. This is a potential improvement upon the current state of grants management, which is comprised of multiple drawdown platforms. However, this change would centralize grants management drawdowns, which would appear to contradict the decentralization offered by blockchain technology.

Despite appearances, a single drawdown platform would not in any way offset or diminish the decentralization of the underlying technology, which is blockchain. Blockchain, as shown in Figure 1, decentralizes ledgers. Although there would be one drawdown platform, the underlying ledger capturing transactions on the platform would be decentralized or distributed across multiple participant users.

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

---

## How JFMIP Arrived at the Federal Research Grants Use Case

In 2017, Fiscal Service performed a strategic evaluation that identified potential initiatives that, if adopted, could make federal financial management processes more transparent and efficient. Fiscal Service understood that blockchain was beginning to play a larger role in financial services in the private sector. While blockchain was synonymous with Bitcoin and other cryptocurrencies, Fiscal Service conducted research and outreach sessions to demonstrate and understand how blockchain could be leveraged for use cases outside of cryptocurrency.

Following that research and outreach, Fiscal Service conducted several blockchain proofs of concept. These proofs of concept provided Fiscal Service with a better understanding of when blockchain might add value and

when it is unlikely to add value. Additionally, this work allowed Fiscal Service to better understand some of the related technical and regulatory challenges, among others.

In 2019, the National Science Foundation (NSF), a federal agency that awards about \$8.8 billion annually in grant funding to carry out various research projects, reached out to Fiscal Service to partner on addressing the administrative burden grantees face when receiving federal grant funding. Fiscal Service developed a working blockchain prototype for assessing how this technology may improve transparency and reduce the reporting burden for grant recipients.<sup>29</sup> A secondary objective of the prototype was to provide for greater accuracy and timely reporting from grant recipients to federal agencies and the Federal Funding Accountability and Transparency Act Subaward Reporting System, as well as from federal agencies to USASpending.gov.<sup>30</sup>

Focusing on understanding the problems and user experience from the beginning, the project sought input from NSF, the Department of Housing and Urban Development, the Department of Commerce, and NSF grantees and sub-grantees (both of which include universities) at each step. Fiscal Service's team then produced the grants financial management blockchain prototype. The approach was to start with a narrow focus, gather feedback, revise the prototype, and continue, while expanding the field of stakeholders. The prototype was operating as a single-organization network within a non-production environment managed by Fiscal Service. This prototype was a minimally viable product for testing how blockchain could work, which means it was built with just enough features to allow for basic testing and analysis. Minimally viable product testing is common in the early stages of a product's development cycle.

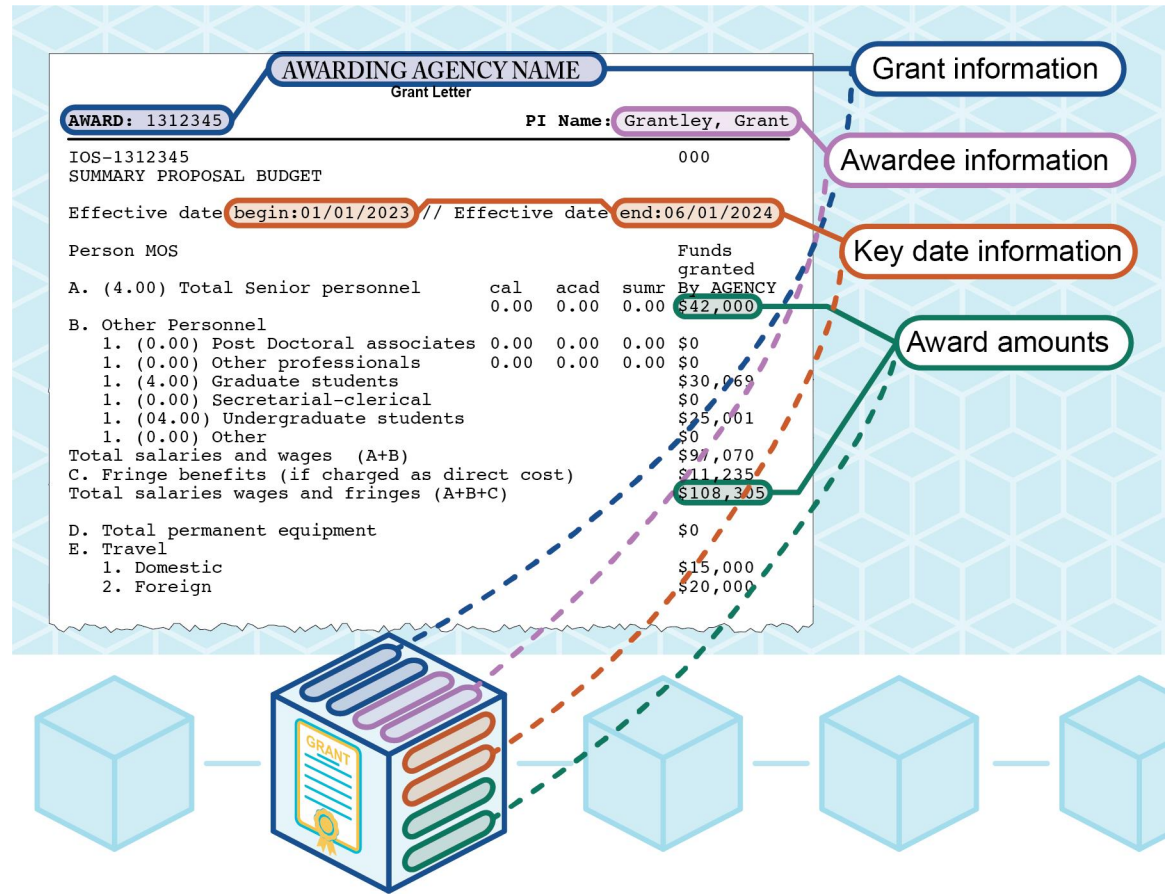
Fiscal Service developed the prototype to make the blockchain's interface resemble an online form to users. An awarding agency can "tokenize" grant information in the application (i.e., create a digital representation of the grant award). See Figure 5 for tokenization.

---

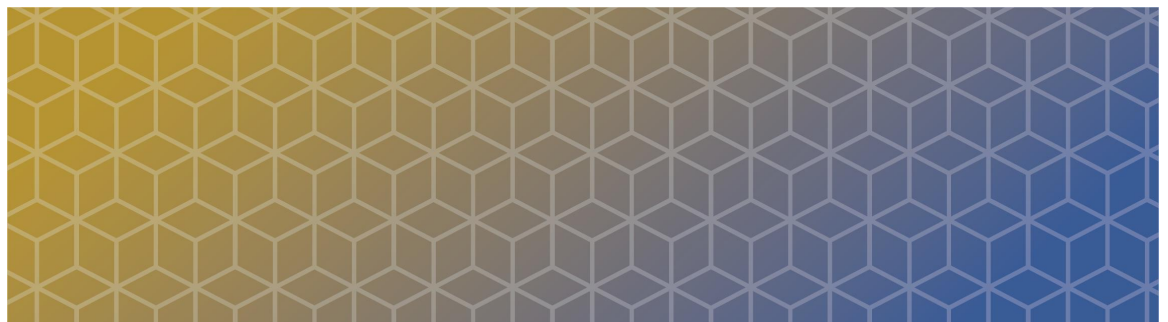
<sup>29</sup>For more information on Fiscal Service's blockchain prototype, see appendix II.

<sup>30</sup>For more information on the Federal Funding Accountability and Transparency Act Subaward Reporting System and USASpending.gov, see appendix III.

Figure 5: Tokenizing a Grant



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01



---

## The Blockchain Grants Financial Management Prototype

In August 2021, leadership from all four JFMIP agencies, motivated by a shared vision to address scalability issues and foster seamless interagency cooperation, took a pivotal step. They opted to broaden Treasury's blockchain prototype across agency boundaries to GAO and use it as a mechanism and test case for greater federal efficiency. The architecture, design, development, and deployment of the prototype are outlined in this section.

---

### Blockchain Prototype Architecture

The architecture of this blockchain is structured into four distinct layers. In the context of blockchain architecture, a layer refers to a building block or level that plays a specific role in making the blockchain function smoothly. Each layer has its own function and works in conjunction with the others to ensure the blockchain operates seamlessly. These layers are:

1. **Infrastructure Layer:** Acting as the foundation of the blockchain, this includes physical components such as nodes, storage, and network infrastructure. It can be hosted either on the cloud or on users' own servers.
2. **Network and Protocol Layer:** This layer defines the character of the blockchain, determining attributes such as whether it is public or private, and the consensus mechanism applied.
3. **Services Layer:** This includes elements such as smart contracts, digital wallets, tokens, and interfaces to off-chain databases.
4. **User Interface Layer:** A web-based interface that allows users to interact with the blockchain, enabling actions like grant generation and other transactions.

---

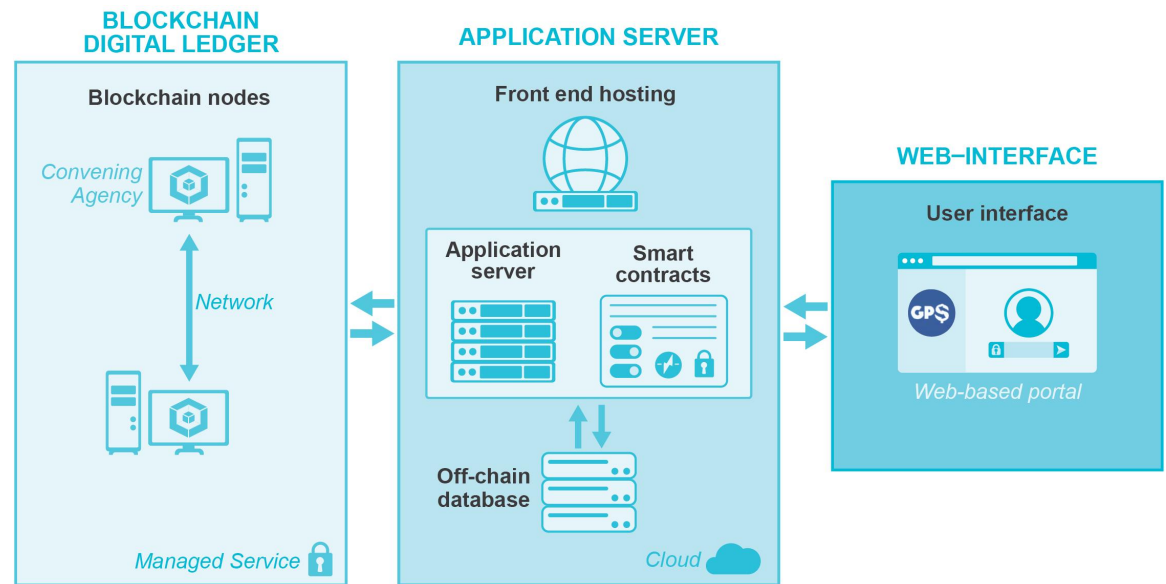
### Design, Development, and Deployment of the Prototype

This section describes at a high level the construction of the grants financial management prototype. It is important to note that during the exploration of new technology, agencies have limited resources available and make some design and technology decisions based on these constraints. This was the case with this prototype. Further assessment and final decisions would need to be made when a prototype is considered for deployment to users. This section highlights those constraints where applicable, and includes other technical

trade-off decisions made at various stages of the construction process that can inform other federal agencies undertaking similar initiatives.

The blockchain prototype construction follows a three-part approach as shown in Figure 6.

**Figure 6: Blockchain Prototype Deployment**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

The grant financial management prototype was developed in three stages:

1. **Blockchain Digital Ledger Node:** GAO, in collaboration with Fiscal Service, set up the blockchain digital ledger node to securely record and store all transactions. A managed service subscription account (i.e., an account with a third-party service provider) was created, and the appropriate account type was selected. A consortium, or group of approved users of the prototype, was established, connecting Fiscal Service and GAO to the managed services blockchain. Two main options for the blockchain’s protocol, or basic set of rules, and provider were considered: Ethereum and Hyperledger Fabric.
  - *Ethereum:* A well-known blockchain platform for its inclusion of smart contract functionality, Ethereum uses an open-source framework. This means that its creator and copyright-holder allows Ethereum users the right to study, use, and change the platform, which encourages community-driven innovation and improvements. This results in users of Ethereum benefitting from



consistent troubleshooting and support not just from the creators, but also from the community of users. Ethereum is widely used and has a robust and active community offering support to users. Similarly, Ethereum utilizes the Solidity programming language (further discussed in appendix II, part 2), which is widely used by software developers.<sup>31</sup> While Ethereum was found suitable for our specific needs, in some scenarios it can encounter scalability challenges.

- *Hyperledger Fabric*: Another open-source platform for blockchain is Hyperledger Fabric. It is developed and supported by an approved group of experts spread throughout the globe, ensuring a wealth of diverse blockchain knowledge. Compared with Ethereum, Hyperledger Fabric may require agencies to undertake additional planning and to possess a deeper understanding of enterprise-oriented functionality, such as network setup, identity management, and permission controls.

---

<sup>31</sup>Solidity is a special programming language used for creating smart contracts on the blockchain. It is unique because it enables developers to write rules and conditions directly into the contracts, ensuring that transactions are secure, reliable, and trustworthy. It has mechanisms to catch errors early in the development process to ensure greater program reliability.

## Choosing Your Path: Managed Services vs. On-Premises Hosting

### Managed Services: The Outsourced Solution

- Lower operational burden and faster startup
- Increased capacity for growth, or “scalability,” and on-demand sizing
- Potential for costs increasing over time due to dependence on a vendor

### On-Premises: The Self-Hosted Solution

- Complete control
- Tailored customization
- Higher initial cost
- Need for in-house expertise
- Limited scalability
- In-house costs for security and maintenance

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

Fiscal Service and GAO incorporated Ethereum into the prototype. To ensure the integrity of the grants financial management process, we employed the Proof of Authority consensus method. This method enabled a designated group of nodes to authenticate transactions. Subsequently, we proceeded to establish a connection between the blockchain and the application server.

2. **Application Server:** This server serves as a central point for smart contracts, off-chain databases, and the front end website in the grants financial management system. We chose a reliable cloud server with a widely used operating system to ensure strong security and smooth software deployment. Then, we set up this server with a front end website, an off-chain database, and a connection to the blockchain digital ledger node.
3. **Web Interface:** This interface serves as a user-centric website tailored for grants management. Adhering to standard industry practices, a cloud-based web hosting server was chosen, equipped with pre-set screens and essential software components. Furthermore, a unique URL was established for the site, which was then linked to the application server using conventional methods.

In the intricate landscape of grants management, various user roles necessitate distinct levels of involvement and technical proficiency:

**Convening Agency (i.e., Treasury’s Fiscal Service):**

- Assumes the paramount responsibility for the comprehensive setup of the blockchain environment.
- Manages all technical facets to guarantee the system’s integrity and functionality.
- Supervises the full spectrum, including the web interface, to ensure seamless operations.

**Consortium Participants:**

- Typically engage with the grants management process by utilizing the cloud-based server and digital ledger node components.
- Interact through these components, with moderate demand for setup and blockchain expertise.

**Grantees and Recipients:**

- Primarily interact with the user-friendly web interface.
- Execute grant-related activities with ease through simplified interactions.
- Encounter a user-centric experience that reduces the need for major blockchain knowledge.

---

## Outcomes of the Prototype

The prototype had several beneficial outcomes, including

- expanding the blockchain knowledge base of Treasury and GAO officials;
- identifying and assessing IT considerations for a potential multi-agency blockchain;

- evaluating financial management, human capital, and oversight considerations; and
- creating an expanded foundational knowledge base that can be used by other federal agencies, state and local governments, and the private sector.

## Knowledge Gained

Participating in the JFMIP blockchain project provided Treasury and GAO with in-depth practical knowledge in establishing a multi-agency blockchain. Through participation in the project, Treasury and GAO officials gained:

- technical knowhow for building blockchain from the ground up in the cloud using a managed service platform;
- insights into the various capabilities and limitations of blockchain;
- knowledge of blockchain security controls such as encryption, public and private key architecture, smart contracts, on-chain and off-chain data linkage and consensus methods; and
- understanding of the intricacies involved in a multi-agency blockchain, such as information sharing agreements and a shared ATO framework.

The expertise acquired on this project can potentially be applied to many areas where blockchains are planned, such as in health care, energy, power, and supply chain.

## IT Considerations

This report provides information technology (IT) considerations for a potential multi-agency blockchain, including cybersecurity, authority-to-operate, and operational factors. The blockchain prototype has shown that this technology has the potential to bring greater automation and transparency to key processes. While IT challenges such as governance, data standardization, and scalability exist, the prototype has demonstrated that it can automatically and transparently track grant funding. Further, we showed that grant actions could be recorded in a secure ledger that cannot be altered or deleted.

The team also determined that data integrity and confidentiality can be achieved through cryptography that would help ensure that data remain tamper-resistant and secure. Nevertheless, thoroughly addressing ever-increasing cybersecurity threats and challenges will need to be an essential element of any interagency blockchain.

## Financial Management, Human Capital, and Oversight Considerations

The report also identifies federal financial management, human capital, and oversight efficiencies and challenges. Regarding financial management, blockchain has the potential to increase transparency and reduce the complexity of reconciliations. In addition, it can provide a single integrated and validated source of data that can be used by all stakeholders. However, before committing to blockchain, agencies and other entities considering this technology will need to reach agreement on how a blockchain would be constructed, governed, and operated among other things.

The team has no broad concerns regarding human capital and the use of blockchain. Use of this technology should not cause major shifts in job series or classifications but may require minor changes in the evaluation of candidates.

Regarding oversight, blockchain could streamline the audit process and improve data integrity. However, auditors would still need to consider the blockchain's design and implementation as part of any audit.

## Foundational Knowledge Base

This report documents the JFMIP's efforts to develop a foundational knowledge base to inform potential future blockchain implementation. The JFMIP envisions the report as a learning tool in preparing for a future when blockchain is in use. Specifically, this educational document will help agencies who are interested in exploring multi-agency blockchain use cases. It also provides a basis for discussion among key parties within agencies, including the financial management, Chief Information Officer, and Chief Data Officer communities.

The JFMIP would like to note that the scope of this initiative did not include several areas related to federal grants management and blockchain. This initiative did not



- develop a working prototype with real or production environment data,
- create application programming interface connections to integrate with any live or production systems (e.g., grant drawdown system or payments application),
- execute a real transfer of money (e.g., cash deposits, wire transfers),
- look at end-to-end grants management, or
- involve anything related to cryptocurrencies.



---

## IT Considerations for Agencies in Using Blockchain

---

The grants financial management prototype architecture offers insights for other agencies interested in implementing their own blockchain network. There are various factors to consider while using blockchain technology to ensure that the system is efficient, secure, and practical.

In this section, we look at the factors that agency leaders could consider while developing interagency permissioned blockchains. We focus on the deployment, operational, infrastructure, and cybersecurity implications of a blockchain system. In addition, we investigate the challenges that blockchains may pose to the components of information security within organizations, such as confidentiality, integrity, and availability. Furthermore, we look at the ATO considerations for a multi-agency blockchain.

### Infrastructure Layer

The blockchain prototype's infrastructure layer is hosted in the cloud. This approach has advantages and disadvantages, with the following factors to consider when planning this approach.

- Cloud hosting provides the ability to easily scale up or down based on usage patterns, resulting in overall cost savings by allowing federal agencies to pay only for the resources they consume on a flexible, pay per use basis.
- Cloud hosting can provide reliable access for federal agencies, grantees, or sub-grantees.
- Cloud hosting often has robust security features such as encryption, firewalls, and intrusion detection systems that protect against unauthorized access or data breaches.
- Cloud hosting expenses can be unpredictable and difficult to manage because they depend on usage and demand.

- Cloud hosting could mean reliance on a single cloud provider, through vendor lock-in, limiting flexibility and perhaps increasing long-term expenses.<sup>32</sup>

## Network and Protocol Layer

Several choices were made in the blockchain prototype at the network and protocol layer. The grants financial management prototype uses a private blockchain that operates on dedicated cloud servers with access controls and firewalls that restrict access to authorized users. This differs from public blockchains, like Bitcoin, that have open access. The prototype is a permissioned blockchain—access to the network is confined to a small group of participants that have been authorized access to and participation in the network. The system can limit users who can access the network at any given time for several reasons, including:

- **Performance:** Agencies may limit the number of concurrent users to ensure network performance and reliability during peak usage.
- **Security:** It is crucial for agencies to be able to respond to threats and malicious activity effectively. To this end, agencies can act and restrict user access if necessary.
- **Capacity Management:** Agencies can prevent interruptions by engineering their network infrastructure based on anticipated volume of transactions and users. Regular evaluation and adaptation of this infrastructure are essential to maintain smooth and consistent operations.
- **Authorization:** The prototype uses a proof of authority consensus mechanism that strictly controls who can create transactions, thereby providing additional security in financial use cases.

## Services Layer

The blockchain prototype's services layer makes use of smart contracts, tokens, wallets, and connectivity to an off-chain database.

---

<sup>32</sup>Vendor-lock-in refers to being dependent on a specific company's products or services, making it difficult to switch to alternatives.

## Smart Contracts

The smart contracts are written in the Solidity programming language, which is widely used in blockchain applications and provides structure and security for these applications.

Smart contracts are intentionally designed to be inflexible, which is necessary to guarantee the security and dependability of the blockchain's business logic. Smart contracts are intended to be executed automatically, without the need for human intervention, and must be programmed to handle all possible scenarios and exceptions. This requires a rigorous coding and testing approach, as well as a thorough understanding of the underlying algorithms and data structures.

When deciding whether to use smart contracts, agencies should

- consider the rigorous programming requirements of smart contracts when building blockchain services, requiring developers with expertise in Solidity, cryptography, distributed systems, and cloud computing.
- understand the business logic and use case thoroughly. Agencies may need to invest resources and time to gain a complete understanding of the operational aspects of the application they are designing.
- identify all possible scenarios and exceptions that smart contract logic should be able to handle. This step may require significant planning and research, with the need to allocate resources accordingly.
- have clear documentation of the smart contract logic. This is essential for transparency and auditability, especially when working in a consortium type arrangement where multiple parties need to have a shared understanding of the smart contract's function and operation.
- have a comprehensive software development life cycle including a testing strategy that includes functional, performance, and security testing.
- have a clear governance framework for the smart contract's maintenance and updates.
- have contingency plans in the event of unforeseen circumstances or changes in the business logic.

- have effective change management policies and procedures in place for ongoing approvals and updates.

## Tokens

Tokens in the grants financial management blockchain prototype represent a grant and its associated information such as amounts for salaries, direct and indirect expenses, and travel. Throughout the grant's duration, tokens are exchanged between the granting agency and the grantees and sub-grantees.

Tokens of various types are used in blockchains; the grants financial management prototype uses ERC 1155 tokens.<sup>33</sup> These tokens have various advantages, including the ability to combine multiple transactions into one, making the process faster and more efficient. They also require less storage space and offer enhanced security to prevent cyber intrusions. Agencies can consider these factors in deciding on the type of token to utilize. (See appendix II, part 3 for more details.)

## Wallets

In the blockchain prototype, grant recipients use wallets to temporarily store assets. Typically, the recipient accountant reviews the supporting documentation for eligibility before the drawdown can be processed. While this information is being gathered and reviewed, the wallet can serve as a holding area. After reviewing this information, the recipient can choose to redeem or return the funds.

The blockchain prototype uses a software wallet that allows for flexibility and simple integration with the application's user interface. However, the storage of critical information, such as private keys, necessitates a careful examination of the wallet type. Hardware wallets may be used in situations where increased security is required.

## Off-Chain Database

The off-chain database acts as the critical link between the blockchain and the front end user interface. It is responsible for tracking events on the blockchain, such as grant creation, transfer, and redemption, as well as other important

---

<sup>33</sup>An ERC 1155 token is a digital representation of a grant. It allows for multiple transactions, thus allowing efficient processing of multiple grant payments to multiple recipients. It also allows PDF files to be associated with a transaction, thus allowing for grants and related collateral to be in one place.



information such as users and their permissions. This database is only accessible to the convening authority, which in this case is Fiscal Service.

The off-chain database does not change or invalidate any information on the blockchain. Instead, it is used to manage the blockchain network and ensure its smooth operation. By keeping this database separate from the blockchain, the convening authority gains an additional layer of security and control, ensuring that it can manage and oversee the blockchain network in a secure and effective manner.

## User Interface Layer

The top layer, or “front end,” of the blockchain prototype has the user interface. It is the location of customer interaction, business logic, and user interface design. Key design factors include the following:

- **Ease-of-use:** be user friendly with clear and concise prompts that are easy to understand and navigate.
- **Consistency:** be consistent throughout the application to provide seamless experience.
- **Navigation:** be intuitive and easy to understand.
- **Pop-ups:** be used to convey responses or acknowledgements to some actionable events or confirmations.
- **Accessibility:** follow the Web Content Accessibility Guidelines by the World Wide Web Consortium.<sup>34</sup>

## Available Prototype User Actions and Potential Future Improvements

The actions possible on the blockchain prototype are documented in appendix II, part 4. They fall into several categories:

- **Grants management:** The blockchain prototype allows users to create, update, and view grants based on *AwardID*, organization, and other criteria. It offers customization of thresholds and options to simplify

---

<sup>34</sup>Web Content Accessibility Guidelines ensure web content is accessible to individuals with disabilities, promoting inclusivity and equal access.

processes for grantees and sub-grantees, enhancing efficiency and reducing reporting burdens.

- **Grant requests:** Within the blockchain prototype, grantee users can perform grant-related actions, including creating, reviewing, validating, approving, or rejecting funding requests. Sub-grantees also have the capability to carry out similar actions when applicable.
- **Report generation:** The prototype enables the generation of various reports that can be stored as CSV files, facilitating further analysis and data utilization.

The blockchain prototype was a minimally viable product and followed many of the design factors mentioned above. It was noted that future iterations may continue to improve on the user interface with the following considerations:

- **Improve pop-up details:** Users need clearer instructions and more information in pop-ups, especially for error messages. This helps users correct errors and reduces incorrect entries.
- **Allow viewing of grant descriptions on all subsequent web pages:** This would make it easier for users to understand the purpose of a grant and help them make informed decisions.
- **Maintain grant and sub-grant grouping:** This would help users keep track of the grants and sub-grants in one affinity group and reduce confusion or delay in navigating to a better organized list.
- **Implement additional notifications:** Users would benefit from notifications about session expiration and invalid data entry. This would provide additional information to help users avoid making mistakes.

The blockchain prototype consists of two main components: a user-centric front end, focusing on actions and data interaction, and a back end, responsible for transaction processing and blockchain operations.

## Front End vs. Back End: Unveiling Blockchain Interactions

### The Front end Journey: User Actions

- **User Interactions:** Users engage with the blockchain through a user-friendly interface. Actions such as initiating grant transactions, viewing account balances, or approving grants are done here.
- **Data Validation:** Initial checks on user-provided data are performed, including edit and format validations.
- **Request Generation:** Once validated, user actions generate a corresponding request to the back end blockchain node.
- **Notification & Confirmation:** The front end receives updates about transaction status from the back end, informing users about success or failure using pop-ups or alerts.
- **Data Presentation:** The front end presents data obtained from the back end, such as account balances or transaction histories, in a readable and understandable format.

### The Back end Voyage: Blockchain at Work

- **Transaction Reception:** The back end receives the transaction requests from the front end.
- **Authentication & Signature Verification:** Transactions are authenticated and digital signatures are verified, confirming the sender's identity and intent.
- **Transaction Validation:** Rigorous checks occur to ensure transactions abide by the blockchain network rules and consensus mechanism.
- **Block Creation:** Valid transactions are bundled into a block. Each new block is linked to the preceding block, forming a chain using “hashing” techniques.
- **Smart Contract Execution:** The contract’s “logic” is executed on the back end.
- **Transaction Logging:** Details of every transaction are logged and stored immutably on the blockchain, providing a clear and tamper-resistant audit trail.

**Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01**

## Managed Service Factors

The blockchain prototype used a managed-service blockchain. This choice has potential benefits and some areas to consider. The following are some considerations that federal agencies may consider if they choose this approach.

- A managed-service blockchain may be ideal for prototypes and pilots because it reduces the complexity and learning curve of deploying a blockchain. It typically runs in the cloud and provides additional tools to accelerate deployments. There may also be expertise available for consultation from the supplier. Managed-service blockchains in the cloud may also help provide (1) redundancy of information, which can help protect against any failures causing disruption, and (2) scalability, which offers increased capacity to grow the blockchain and user base in the future.
- In the long run, it may lead to reliance on a supplier, a condition known as "vendor lock-in." In addition, customization may be costly, and new features may be delayed because they will be delivered in accordance with the vendor roadmap. The agency also may have limited options for dealing with unsatisfactory vendor performance.
- Using a specific managed service necessitates advance planning on the part of participating agencies. GAO used the same managed service as Fiscal Service, avoiding any potential interoperability issues. If a different managed service is used, or if the agency plans to build its own blockchain, interoperability may need to be carefully considered.

## Cybersecurity Factors

The cybersecurity triad of confidentiality, integrity, and availability plays a crucial role in the implementation of blockchain technology (see figure 7 along with National Institute of Standards and Technology's (NIST) Special Publications 800-53 and 800-37).<sup>35</sup>

Confidentiality factors involve protecting sensitive information through encryption, strong passwords, regular data backups, software updates, and multi-factor authentication. The use of a permissioned blockchain and secure cloud environment further enhances confidentiality.

Integrity factors ensure the accuracy and trustworthiness of data through immutability, cryptographic algorithms, hashing, and digital signatures. Public

---

<sup>35</sup>National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53 Rev. 5 (Gaithersburg, MD: Dec. 2020) and *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37 Rev. 2 (Gaithersburg, MD: Dec. 2018).

key infrastructure,<sup>36</sup> secure key storage,<sup>37</sup> and key rotation procedures contribute to data integrity.<sup>38</sup>

Availability factors focus on redundancy, regular testing, and disaster recovery planning to ensure the continuous availability of the blockchain network. Redundancy and scalability can be achieved through cloud-based hosting and managed services. Regular testing and maintenance are crucial for cybersecurity, network performance, and addressing potential spikes in usage.

Federal agencies can consider these factors to provide a foundation for secure and reliable operations, and should work together to resolve discrepancies when policies, procedures, or processes do not align with each other. As identified in GAO's 2023 High-Risk List, additional actions are needed to ensure the cybersecurity of the nation. As of February 2023, 52 of 133 priority recommendations to key departments and agencies had not been fully implemented. These recommendations relate to addressing weaknesses with agencies' cybersecurity programs.

### Confidentiality Considerations

As federal agencies are exploring the use of blockchain technologies, it is paramount to prioritize confidentiality. This involves enforcing authorized restrictions on information access and disclosure to safeguard personal privacy and proprietary information. Strategies to preserve confidentiality within a blockchain framework include:

- *Encryption of Sensitive Data:* Blockchain technologies generally utilize private or public keys to restrict access and secure data. It is imperative to encrypt sensitive data, a process that scrambles data to render it unreadable without the correct decryption key.

---

<sup>36</sup>Public Key Infrastructure is a system that uses pairs of cryptographic keys: a public key, which is openly shared and used to encrypt data, and a private key, which is kept secret and used for decryption and digital signatures. When someone wants to send encrypted data or verify the authenticity of a digital signature in a blockchain transaction, they use the recipient's public key. The recipient then uses their private key to decrypt the data or validate the signature. This process ensures secure communication and data integrity in blockchain transactions. One can think of the public key as a bank account number which is known to others for depositing funds and the private key as a PIN known only to you for accessing your bank account.

<sup>37</sup>Secure key storage refers to various methods of protecting cryptographic keys and preventing unauthorized parties from gaining access to the keys and resulting information. Storage protects the key while keeping it readily available for use.

<sup>38</sup>Key rotation refers to preemptively changing or replacing a key with a new key, and making corresponding updates to the places in which the key is used.



- *Password and Passcode Security*: The implementation of strong and complex passwords and passcodes is essential to avert unauthorized system and data access.
- *Regular, Secured Data Back-ups*: Ensuring regular back-ups of data will help in preventing data loss during unforeseen circumstances or disasters. Data backups should be secure (e.g., encryption, secure storage).
- *Up-to-date Software and Security Features*: Maintaining the most recent versions of software and security features can offer protection against the exploitation of known vulnerabilities.
- *Multi-factor Authentication*: Incorporating multi-factor authentication, which necessitates users to authenticate their identity through multiple methods, adds an extra layer of security. In the blockchain context, agencies might also utilize established permissions, roles, and cloud IP address access controls to enhance security.
- *Employee Education*: Agencies should consider implementing training programs and creating user manuals to educate employees on security best practices.

The blockchain prototype utilizes an off-chain database for storing various types of data. Access to this database is regulated by the convening agency, Fiscal Service, offering a substantial degree of protection. There is, however, room to enhance security further through additional safeguards.

### Integrity Considerations

As federal agencies consider the implementation of blockchain technology, it is vital to focus on the integrity aspect, which pertains to safeguarding information from unauthorized modification or destruction, and thus ensuring the non-repudiation and authenticity.<sup>39</sup> In the realm of blockchain technology, the Public Key Infrastructure helps ensure data integrity and encompasses architecture, organization, techniques, practices, and procedures that underpin the operation of a certificate-based public key cryptographic system. Strategies to uphold integrity in a blockchain network include:

---

<sup>39</sup>Non-repudiation in blockchain refers to the ability to prove the authenticity and integrity of transactions. It ensures that once a transaction is recorded on the blockchain, it cannot be denied or disputed by the sender, providing strong evidence of its origin and accuracy.

- *Public and Private Keys:* Transactions in a blockchain are conducted employing a pair of keys: a public key and a private key. The entity holding the private key utilizes a digital signature, akin to a password, maintaining the data's authenticity and security in transactions. This signature is mathematically tethered to a public signature, thereby securing the data within the blockchain and allowing immediate detection of any unauthorized alterations, enhancing the trustworthiness of the stored information. However, whoever has a private key can initiate transactions on the blockchain; thus, a bad actor possessing a key could threaten the blockchain as a whole. Additionally, losing private keys means losing the ability to access data and verify the blockchain's information for participants on the blockchain.
- *Secure Key Storage and Management:* Federal agencies should facilitate secure key storage to avert unauthorized access, tampering, and theft. In doing so, they may need to consider hardware security modules for storage. Procedures for timely key rotation and revocation, alongside a mechanism to promptly nullify lost or stolen keys, are essential.
- *Digital Signatures and Cryptographic Techniques:* The blockchain employs cryptographic techniques to assure data non-repudiation and authenticity. Every transaction bears a timestamp, a unique address, and a transaction hash that verifies the data, ensuring its security within the blockchain.
- *Smart Contracts:* The blockchain prototype leverages smart contracts to uphold the necessary logic and agreement process, utilizing attributes like timestamps and transaction hash information to identify and verify the data.
- *Data Entry:* Entrusted to the granting agency in the blockchain prototype, it is critical that the grant information be accurately entered at the initial stage. Ensuring accurate information can be reinforced with timestamps and transaction hash information to attest to the data's accuracy once registered in the blockchain. Ensuring accurate data are entered into the blockchain by granting officers requires appropriately designed, consistently implemented, and effectively operating controls over the entire data entry process. These controls could include closed loop verifications and other checks.

The blockchain prototype illustrates the potential for federal agencies to leverage digital signatures and other mechanisms to ensure non-repudiation, offering a framework that promotes data integrity throughout its lifecycle.

### Availability Considerations

As federal agencies consider the adoption of blockchain technology, it is important to consider availability. Blockchain technology inherently provides a high level of availability because it operates in a distributed manner and in the cloud. The decentralization and cloud redundancy help ensure that no single point of failure would disrupt availability. Nonetheless, the following factors should be considered to help ensure that the blockchain network is available for use.

- *Redundancy*: It is important to have redundancy in place to ensure that if one node or server goes down, there are backups in place to take over its functions. This can include implementing backup mechanisms and ensuring that multiple nodes are available to serve the blockchain network. A cloud-based blockchain has the potential to easily address redundancy requirements.
- *Regular testing*: Regular testing and maintenance of the blockchain network are crucial to ensure that it is available for use. This includes testing for scalability, load balancing, and network congestion. It is critical to have the resources and infrastructure in place to deal with potential spikes in usage and demand.
- *Disaster recovery*: Having a disaster recovery plan in place is essential to quickly recover from any potential disruptions or outages. This includes maintaining and testing contingency plans to continue operations.

The blockchain prototype is a minimum viable product, with front end and back end servers running on single-computer platforms. However, because the blockchain is being hosted in the cloud, these servers can be increased to include redundancy and scalability, allowing for greater performance and reliability.

### Continuous Improvement and Evaluation

Continuous improvement and evaluation are important to federal agencies considering blockchain because it helps to ensure that the blockchain system remains secure and effective over the long term. By implementing continuous

improvement and evaluation controls, federal agencies can proactively identify and address vulnerabilities and other security flaws in the blockchain system, thus reducing the risk of cyberattacks and other security breaches.

- *Configuration management:* Creating and maintaining secure configurations for the blockchain system, which includes the underlying infrastructure, network devices, and applications. Creating a configuration management plan, implementing security baselines, and monitoring configuration changes are all part of this.
- *Patch management:* Identifying, assessing, and mitigating software updates such as software vulnerabilities in the blockchain system. This includes performing regular vulnerability scans and patch management to identify and address any potential security flaws.
- *Incident management:* Having a well-defined incident management process in place, including incident response protocols, incident reporting, and incident recovery. This control requires incident response teams that are trained and equipped to manage incidents.
- *Disaster recovery process:* Having a plan in place for recovering from disruptions or failures between all stakeholders.

### Open-Source Component Considerations

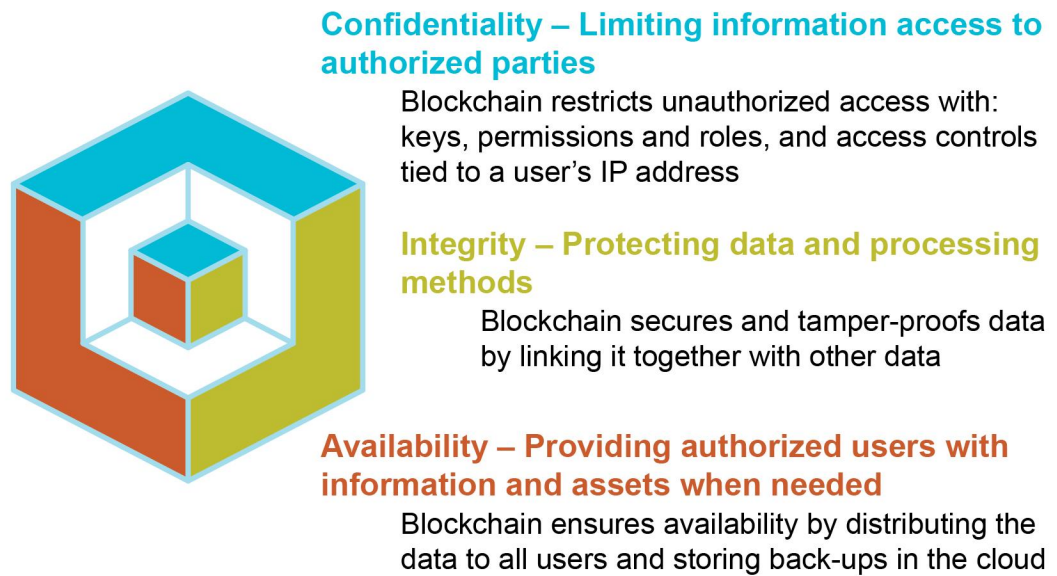
A federal agency that uses a managed service must be aware of any open-source components used by the managed service provider and must create a complete cyber supply chain risk management program to mitigate any supply chain vulnerabilities. This includes assessing the security of third-party suppliers and partners, putting in place security controls, monitoring the supply chain, and reviewing and upgrading vendor contracts on a regular basis to ensure they satisfy security standards.

Federal agencies may consider the following factors to deal with open-source components:

- Performing due diligence on third-party vendors and partners.
- Analyzing the security procedures and controls of vendors and partners.
- Monitoring the supply chain to detect potential threats such as known vulnerabilities in open-source components.

- Regularly reviewing and updating vendor contracts and evaluating if they are meeting necessary security standards and obligations.
- Having an incident response strategy in place to help mitigate and contain potential security breaches.

**Figure 7: Cybersecurity Factors**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

---

## Authority-to-Operate Considerations

ATO is the official management decision by a senior government official known as the authorizing official, such as the Chief Information Security Officer, to authorize operation of an information system on behalf of a federal agency. The authorizing official also explicitly accepts the risk to organizational operations, organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.



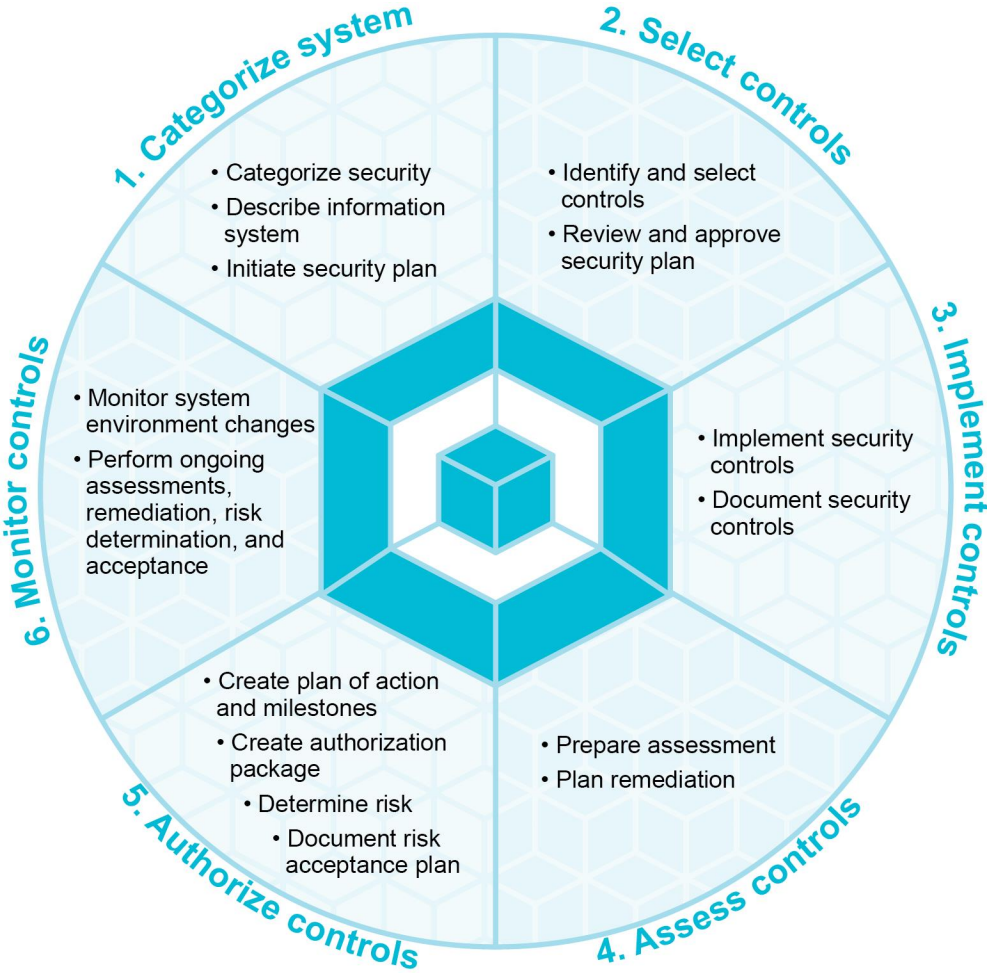
The Federal Information Security Modernization Act (FISMA) of 2014 establishes the requirements surrounding this activity.<sup>40</sup>

NIST's Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, encompasses security, authorization, and administration for government information systems. The risk management framework defines a cycle for safeguarding and monitoring ATO processes. It offers a six-step approach for developing secure data processes in new information systems, providing valuable practices for federal agencies. The six steps are summarized below in Figure 8.

---

<sup>40</sup>The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 120 Stat. 3073, largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946-2961. As used in this report, FISMA refers to both FISMA 2014 and to those provisions of FISMA 2002 that were incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

**Figure 8: Authority-to-Operate System Protection and Monitoring Cycle**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

### Multi-Agency ATO Considerations

When obtaining an ATO for a cloud-based blockchain network, a multi-agency entity or initiative must consider specific factors. The convening agency can secure an ATO based on a risk management framework and then share its authorization packages with other agencies.<sup>41</sup> This allows them to acquire an authority to use without having to execute a full ATO. To supplement the

<sup>41</sup>According to a framework established by the Federal Risk and Authorization Management Program (FedRAMP) to assist agencies with meeting the FedRAMP requirements for cloud services, agencies can leverage existing security authorization packages (e.g., ATO) other agencies established with cloud service providers. OMB also permits leveraged authorizations when an agency chooses to accept some or all of the information in an existing authorization package generated by another agency. An agency might do this based on the need to use the same cloud-based information system used by another agency.

ATO, memorandums of understanding and information sharing agreements can be used to outline security requirements, rules of engagement, and network participant responsibilities. To share ATO documentation with other government agencies, a repository can be established.

For the grants financial management blockchain, Fiscal Service and GAO used an information sharing agreement to establish a common framework for sharing data and technology. Given the complexity of planning and coordinating a blockchain ATO across agency lines, agencies may need to consider these ongoing challenges across government when exploring potential blockchain implementations.

---

## Operational Considerations

As federal agencies continue to explore and implement blockchain technology, there are a variety of operational considerations that should be considered. These considerations will vary depending on the specific use case and agency and would require careful planning and implementation to ensure a successful blockchain deployment. The operational considerations include guidance on business processes, testing, user experience, infrastructure, security, industry best practices, interoperability, data standardization, and cybersecurity, some of which were previously examined in previous sections of this report but are relevant here. For key sources of guidance identified by the JFMIP, please also see the articles listed in appendix I.

### Business Processes

- Define the business processes to be automated by the blockchain.
- Map out the flow of data and information between all parties involved in the business processes.
- Define the data elements that will be recorded on the blockchain.
- Define the smart contract programs that will govern the interactions between parties.
- Establish governance and decision-making processes for the blockchain.
- Develop procedures for system administration and maintenance.

- Define roles and responsibilities for all parties involved in the blockchain network.

## Testing

- Perform thorough testing of the blockchain and smart contracts, including data entry, date validation, and functional testing with error conditions.
- Test blockchain integrity using cryptographic hashes to ensure data immutability and security.
- Anticipate and test for different usage scenarios, such as high traffic and peak usage, to ensure system scalability and performance.
- Identify and address potential failure scenarios through comprehensive testing to enhance the robustness and reliability of the blockchain implementation.
- Consider implementing a sandbox environment for interoperability and ongoing testing purposes.<sup>42</sup>

## User Experience

- Develop a user-friendly interface for interacting with blockchain.
- Ensure that the blockchain is accessible and user-friendly for all users.
- Provide clear feedback for user actions and alert them in advance for any session timeouts.
- Develop user manuals and training materials to educate users on how to use the blockchain.
- Provide technical support and assistance to users.

---

<sup>42</sup>A sandbox is a controlled testing environment that enables safe experimentation, validation, and development of the blockchain system. It allows for testing alternative scenarios, interoperability with other systems, and ongoing evaluations without impacting the live environment.

## Infrastructure

- Ensure the blockchain infrastructure is scalable and can handle increased usage and demand.
- Implement redundancy to ensure that if one node or server goes down, there are backups in place to take over its functions.
- Establish a disaster recovery plan to quickly recover from potential disruptions or outages.
- Maintain a fallback posture to help recovery in case of a disaster or outage.
- Ensure that front end and back end servers are secure and protected.

## Security

The implementation of blockchain requires consideration of the following key principles.

- Use approved encryption standards to protect sensitive data and communications and keep software and security features up to date.
- Require the use of multi-factor authentication and implement secure key storage along with procedures for key rotation, revocation, and cancellation of lost or stolen keys.
- Use digital signatures, time stamps, and other methods to ensure non-repudiation.
- Implement data validation, data integrity controls, and confidentiality controls to safeguard cloud and blockchain data.
- Educate employees on security best practices.

## Industry Best Practices

Blockchain implementation best practices include categorizing information systems, selecting and installing security controls, analyzing their performance, authorizing the system, and ongoing security monitoring.

- Categorize the information system and identify the type of information the system processes and the potential impact to the organization if it is compromised or lost.
- Select security controls to manage risks based on system categorization.
- Implement security controls and provide supporting documentation such as system security plans, reports on the service organization's controls, and security assessment reports.
- Assess security controls to determine risk management effectiveness.
- Authorize the information system based on the security control assessment.
- Monitor security controls to ensure that security controls are working properly and that system changes do not compromise security.

## Interoperability

Interoperability is an important component of blockchain technology since it allows for smooth interaction and integration with current systems, interfaces, and networks.

- Consider the compatibility of the blockchain with existing systems, interfaces, and networks.
- Ensure the blockchain is designed to support interoperability with other systems, interfaces, and networks.
- Develop procedures for integrating with other systems, interfaces, and networks.
- Define data exchange formats and protocols.

## Data Standardization

Data standardization enables efficient data management and integration ensuring consistency across the various entities using blockchain.

- Naming Conventions: Consider adopting a uniform naming structure for consistent identification, e.g., grant name.



- **Data Formats:** Consider setting a common format for recording dates across all systems.
- **Grant Types:** Consider categorizing grants under consistent classifications.
- **Status Codes:** Consider consistent codes to depict the grant status.
- **Terminologies and Descriptions:** Consider adopting a standard vocabulary to avoid ambiguities.
- **Metadata Standards:** Consider setting metadata<sup>43</sup> tags and descriptions for efficient data retrieval.

---

## Shared Service Factors

Shared services are a way for government agencies to reduce costs while increasing efficiency. The adoption of cloud computing by multiple entities has enabled progress in this direction that was previously not possible in an on-premises deployment. Furthermore, with blockchain, government agencies can share data, securely transfer asset value, and meet reporting and oversight requirements while potentially reducing the cost of maintaining separate systems.

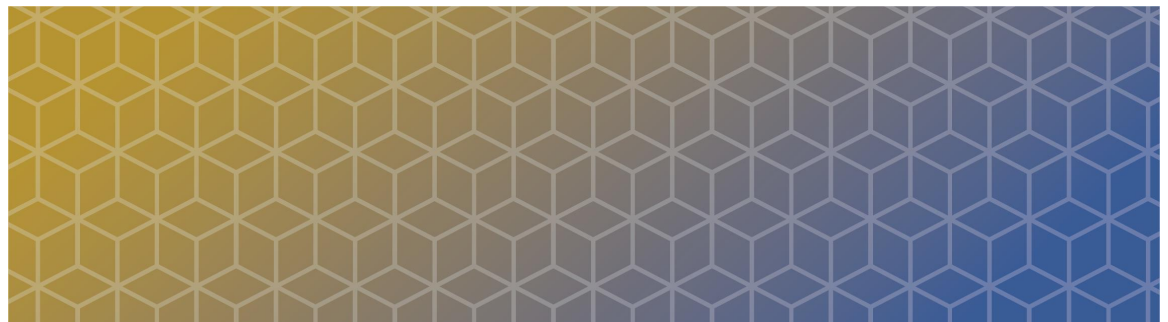
However, it should be noted that a shared services model requires careful planning and coordination because of the inherent challenges in meeting the requirements of multiple agencies. A successful implementation can offer the following benefits:

- It can enable government agencies to focus on mission and business outcomes. Each agency can make better decisions by analyzing end-to-end data to meet their business outcomes. In this regard, for grants, blockchain technology has the potential to provide a unified view of grant details across agencies, grantees, and sub-grantees to quickly identify problems and plan mitigations.

---

<sup>43</sup>Essentially “data about data,” metadata provides additional information and context about a data item, such as source, format, or the date it was created.

- Starting and developing their own systems for cross-agency services can be a costly proposition for government agencies. Agencies can avoid these high costs and improve efficiency by leveraging shared services. This approach also accelerates the implementation of innovative cross-agency projects, creating a win-win situation for all parties involved.
- It can assist government agencies in mitigating the risks of system failure. Agencies can ensure that they are using the most reliable and up-to-date technology by consolidating and standardizing systems, reducing the possibility of system downtime or other technical issues.



---

# Potential Implications of Blockchain Use for Federal Financial Management, Human Capital, and Oversight

---

## Federal Financial Management

Fiscal Service identified the following themes of both direct and overarching benefits observed across other blockchain implementations applicable to financial management and accounting functions:

- **Increased Transparency:** All transaction participants have access to data in real-time.
- **Reduced Financial Disputes Between Parties:** Blockchain provides a single, agreed upon view of the data.
- **Reduced Reconciliation:** Blockchain could streamline business processes by validating transactions in real-time and reducing the need for retroactive reconciliation. For example, in the case of the grants management prototype, blockchain could automate reconciliations with the data it captures. This is because these data could be synced with granting agencies' financial systems in real-time. Additionally, the blockchain could automatically populate the OMB Standard Forms commonly used with grants, including 270, 425, and 425A. This would be accomplished through the data tracked on the blockchain's grant tokens, thus potentially reducing the reporting burden for grantees.

Further, grantees could potentially see a reduction in the number of systems they must utilize to file reports. Instead of reconciling information from multiple systems, there would just be a blockchain serving as the only source of data. From the agency perspective, current payment systems can run only limited checks, such as fund availability. The tokens on the grants management blockchain prototype would have line-item detail, which could enable the automatic reconciliation, or check, of a grantee's expenses with the grant terms and conditions.

- **Reallocation of Workforce Resources:** The combination of increased transparency and reduced reconciliation provides flexibility for accounting staff to focus on more complex activities, such as analytics work, rather than conducting laborious accuracy and validation activities.

Blockchain technology could reshape how accounting is performed. It could play a critical role in equipping organizations to pivot from traditional accounting practices of moving data linearly between systems to an innovative practice of leveraging one integrated and validated data source where all applications can work in concert.

## Governance

Whenever a blockchain is considered for use in federal financial management, agency leadership will have to weigh many critical factors such as inter-agency collaboration and decision-authority for the blockchain, in addition to the IT considerations discussed previously. Standing up a multi-agency blockchain would be a complicated task, involving coordination across existing government-wide councils. For example, the Chief Information Officers Council would need to consider IT and cybersecurity risks including how the ATO process would work. The Chief Financial Officers Council would need to advise on financial management systems and reporting as well as general input on how a multi-agency blockchain could be funded, and the Chief Data Officers Council would need to weigh in on standardization and data sharing.

For the purposes of the grants financial management prototype, Fiscal Service developed a draft governance proposal for a convening agency to oversee operating a multi-agency blockchain. It includes items like roles and responsibilities for each party, funding-related considerations, and how input and decisions (e.g., additional use cases) would be made. This proposal was developed with a small set of stakeholders but would need further input from a government-wide perspective.

Fiscal Service identified and assessed models drawn from current governance examples across blockchain and other types of organizations. The following models were considered:

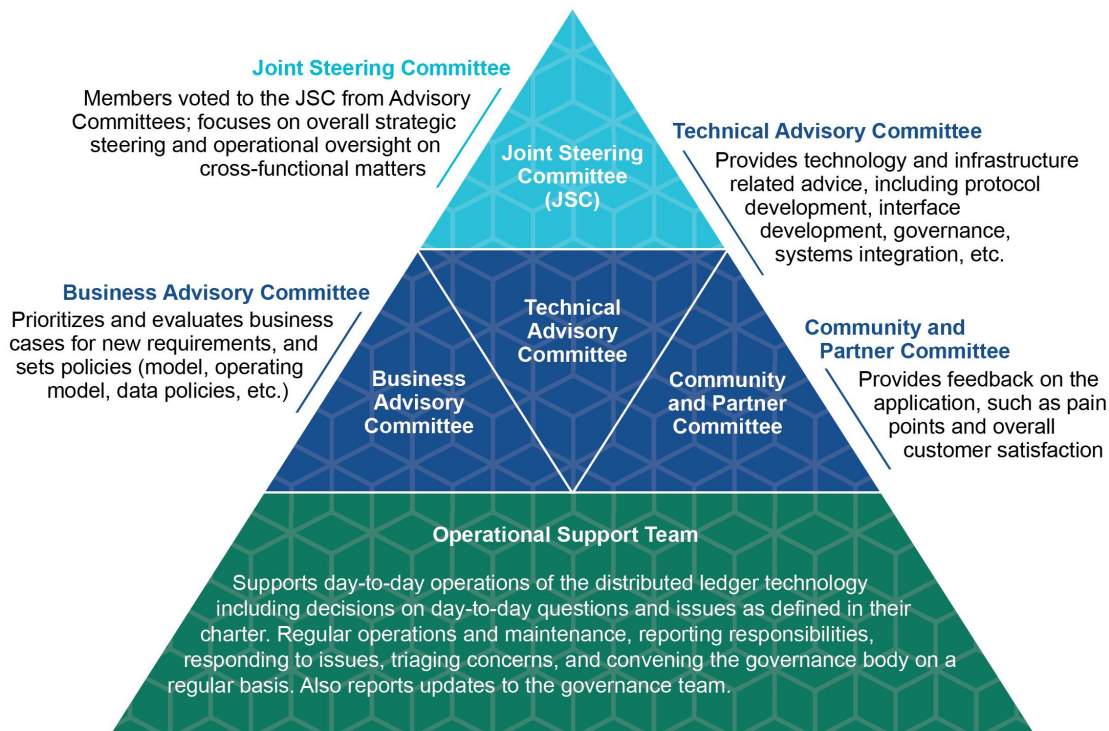
- **Standard Participation: *All members have the same rights*** sitting on a single board. Each is required to contribute the same number of agreed upon resources. This is also sometimes called federated participation. In thinking about the potential to have a government-wide implementation, there are significant differences in the agencies' size and number of programs for grants (and could apply to other

types of blockchains). This model would not allow for larger agencies to provide resources commensurate to their needs.

- **Targeted Participation: *Members individually decide*** where they want to engage based on their interest, business needs, and technical resources available. Given that this model allows for individual determination, there is the potential that there may be inadequate resources to govern and operate the consortium.
- **Rotational Participation:** In a rotational model, ***members take turns*** guiding and supporting the effort. Each member gets a turn to be the convening party. This model would require transfers of decision-making authority from one member to another. It poses risk that actions may get delayed due to transfer of these duties, potential funding issues, and changes in procedures and service lead times.
- **Layered/Mixed Participation:** A hierarchy is created through ***committees, covering business and technology*** where the business side makes strategic decisions, and the technical team develops and manages the technology/platform. As illustrated in Figure 9, committees vote on the executive board.

**Considering the complexities of working across and making decisions among multiple agencies, Fiscal Service recommended the layered/mixed approach shown in Figure 9 for the grants financial management prototype.** Fiscal Service believes that consortium members should represent business, functional, and technical perspectives and build a stable, long-lasting blockchain network for stakeholders. A layered governance model will create a clear, easy-to-understand structure for participants, and voting mechanisms will consistently align consortium efforts with a strategic vision validated by the members.

**Figure 9: Layered/Mixed Participation: Governance Framework for Blockchain**



Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

## Human Capital

OPM analyzed the impact of both this blockchain prototype and the emergence of blockchain technologies generally against the current and potential future human capital needs of the federal government. OPM determined that no major shifts are needed in job series or hiring based on the addition of another technology into the already complex field of financial management. However, minor revisions to the evaluation of candidates may be needed in the event of blockchain technology’s adoption by an agency.

OPM’s human capital business framework consists of five segments: Plan, Implement, Evaluate, Inform, and Improve. While this structure is already built to be resilient and independent of specific technologies, currently foreseen implications of blockchain technology to human capital is presented below.

- **Plan:** Aligning to the human capital initiatives and strategic goals may require either education or training of staff resources to better understand how and if a blockchain-based technology will offer benefit to the organization. Given the current set of government guidance around the adoption of a new technology, agencies’ decision makers



should already be equipped to assess the benefits blockchain offers without any additional or specific expertise on this technology.

- **Implement:** Although agencies may need to train current staff or hire additional staff with expertise in blockchain technology, federal hiring practices are unlikely to experience significant changes due to the adoption of a new technology or even a suite of technologies. Current challenges in attracting and retaining IT expertise are expected to continue if blockchain is widely adopted.
- **Evaluate:** Blockchain technology is unlikely to significantly affect the way business analytics are used to assess strategic or operational human capital measures.
- **Inform:** Any new technology adoption should be compared against prior states when in this stage of the human capital business process. This evaluation can also be used with iterative process development to improve future performance. A key question to ask during this process is: “what was spent in time and resources to cause what benefits?”
- **Improve:** Based on the data from the Inform stage, decisions can be evaluated to accept, alter, or reject any new implementation.

Continuing to iterate and improve human capital processes may allow agencies to better align with OPM’s Future of the Workforce vision.<sup>44</sup> Additionally, staff who would be evaluating an agency’s blockchain technology are likely classified under the Information Technology Management job series, general schedule 2210 job series, which has been operating as a very broad category for a significant period of time.<sup>45</sup> Should any changes in job series arise because of blockchain or any other new technology, it will most likely cause a change in job series descriptions as part of a larger set of alterations to the general schedule 2200 group.<sup>46</sup>

---

<sup>44</sup>See OPM, The Future of the Workforce, accessed Aug. 27, 2023, <https://www.opm.gov/policy-data-oversight/future-of-the-workforce>.

<sup>45</sup>The general schedule 2210 job series (GS-2210) seeks applicants with broad educational backgrounds such as in computer science, information science, mathematics and other fields, as well as experience in data processing functions and work process automation.

<sup>46</sup>The broader 2200 job series, which encompasses the 2210 job series, relates to Information Technology positions in the federal government.

Government auditing is essential in providing accountability to legislators, oversight bodies, and the public. For example, most executive branch agencies are required to undergo annual audits of their financial statements.<sup>47</sup> These audits must be performed in accordance with generally accepted government auditing standards (GAGAS) and may involve audit procedures of application controls such as those over blockchain-based financial management systems.<sup>48</sup> Application controls applied to business processes help ensure the completeness, accuracy, and validation of transactions and data.

Furthermore, auditors of certain large federal agencies must report annually on whether agency financial management systems comply substantially with federal financial management systems requirements, the U.S. Standard General Ledger, and federal accounting standards.<sup>49</sup> The systems should provide reliable, timely, and accurate financial information; support effective and efficient operations; and comply with laws and regulations.<sup>50</sup> In addition, OMB Circular No. A-136, *Financial Reporting Requirements*, provides guidance for executive branch entities that are required to submit audited financial statements.<sup>51</sup>

In addition to federal auditors, auditors in state and local governments and in private firms perform audits of federal grantees. States, local governments, and nonprofit entities expending federal financial assistance totaling \$750,000 or more in a fiscal year are required to obtain an annual “single audit” covering their financial statements, federal awards, related internal controls, and

---

<sup>47</sup>31 U.S.C. §§ 3515(a), 3521(e).

<sup>48</sup>GAO, *Government Auditing Standards: 2018 Revision Technical Update* April 2021, GAO-21-368G (Washington, D.C.: Apr. 2021). GAGAS is also required for all audits performed by agency Offices of Inspector General. 5 U.S.C. § 404(b)(1).

<sup>49</sup>31 U.S.C. § 3512 note. This requirement applies to the 24 federal departments and agencies listed in section 901(b) of title 31, U.S. Code. These entities are commonly referred to as “CFO Act agencies,” after the Chief Financial Officers Act of 1990, which enacted section 901.

<sup>50</sup>OMB, Appendix D to Circular No. A-123, *Compliance with the Federal Financial Management Improvement Act of 1996*, Memorandum No. M-13-23 (Dec. 2013).

<sup>51</sup>OMB, Circular No. A-136, *Financial Reporting Requirements*, (Washington, D.C.: May 19, 2023).

compliance with significant provisions of laws, regulations, contracts, and grant agreements.<sup>52</sup>

Generally speaking, federal auditors may provide oversight of blockchain technology as used in the federal grants process through annual financial statement audits and performance audits where the scope would involve systems employing blockchain.<sup>53</sup> Federal financial statement audits provide an opinion on whether the agency's financial statements are fairly presented in all material respects, which includes reporting on the agency's internal control over financial reporting and reporting on the agency's compliance with significant provisions of laws, regulations, contracts, and grant agreements.<sup>54</sup> Performance audits provide objective analysis, findings, and conclusions to assist management and oversight bodies on a wide variety of objectives, such as program effectiveness and internal control. Blockchain technology, like any other federal information system, could be relevant to auditors performing either of these types of audits.

GAGAS provides standards and guidance for auditors and audit organizations. In addition, auditors may use the Federal Information System Controls Audit Manual (FISCAM) or Cybersecurity Program Audit Guide (CPAG) methodologies. The FISCAM methodology is to be used in connection with federal financial statement audits and attestation engagements. FISCAM may also be used for performance audits when the engagement objectives include assessing the effectiveness of business process application controls, similar to an assessment performed for financial audits.<sup>55</sup> CPAG is to be used on performance audits of key components of agency cybersecurity programs.<sup>56</sup>

---

<sup>52</sup>31 U.S.C. §§ 7501-7506; 2 C.F.R. part 200, subpart F. In limited circumstances, some entities may elect a program-specific audit instead of the single audit.

<sup>53</sup>Federal auditors may also perform attestation engagements, in addition to financial and performance audits. Attestation engagements can cover a wide variety of services on a wide variety of issues in the federal government.

<sup>54</sup>Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives—operations, reporting, and compliance—of an entity will be achieved. Internal control over financial reporting is a subset of the entity's internal control and includes objectives for reliability of financial statements, safeguarding of assets, and compliance with provisions of applicable laws, regulations, contracts, and grant agreements.

<sup>55</sup>GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: Feb. 2009). An exposure draft update to the 2009 FISCAM has since been published by GAO. GAO, *Federal Information System Controls Audit Manual (FISCAM) 2023 Exposure Draft*, GAO-23-104975 (Washington, D.C.: July 2023).

<sup>56</sup>GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: Sept. 2023).

These methodologies outline the controls that auditors evaluate when assessing the CIA triad of confidentiality, integrity, and availability of information and information systems based on their objectives. A blockchain may create unique issues for auditors to consider in planning an audit, as well as potential efficiencies and challenges for auditors to consider in their evidence gathering and testing.

## Audit Planning Factors

Federal auditors would need to consider the effect of the blockchain technology's design and implementation when planning audits. While planning financial audits, auditors work to understand the entity's environment, review its internal control, and assess risks. Similarly, with performance audits, auditors assess risks during the planning phase and determine whether internal control is significant to the audit objectives. If significant, they obtain an understanding of those controls relevant to the audit objectives. For either type of audit, understanding information system controls is key when information systems are used extensively throughout the entity or program under audit, and the fundamental business processes related to the audit objectives rely on information systems.

Information system controls consist of those internal controls that depend on information systems processing and include general controls, application controls, and user controls.<sup>57</sup> Specifically related to blockchain, federal auditors may need to consider how these controls are designed in light of blockchain's decentralized nature and the resulting blurred system boundaries. Moreover, federal auditors may need to consider the challenges inherent in auditing blockchain-as-a-service. Finally, as with all information systems, auditors need to understand risks presented by interfaces between the blockchain and other information systems, including financial systems.

## Decentralization Nature of Blockchain

The distributed and decentralized nature of blockchains can blur the system boundaries of the audited entity and expand its environment, making it difficult to define the control environment. As a result, auditors may face challenges with identifying the information system boundary for a

---

<sup>57</sup>General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. Application controls, sometimes referred to as business controls, are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting. User controls are portions of controls that are performed by people interacting with IS controls.

blockchain, which is important for an auditor’s understanding and assessment of the entity’s control environment.<sup>58</sup>

Further, the autonomous nature of smart contracts operating on a blockchain could also blur the control and ownership of the blockchain. For example, federal auditors might have to determine if there is a need to evaluate both the design of a smart contract (i.e., the “if...then...” logic described previously) and the entity designing the smart contract. Because smart contracts are designed to operate continuously and without human involvement, some errors or other issues may go undetected for an indefinite amount of time unless the design flaw precipitating these errors is found. These potential issues with the smart contract’s design may be unintentional flaws, or fraud by the designing entity that could make the design issue difficult to detect. For these reasons, auditors may need to gain an understanding of both the design and designing entity of smart contracts as they assess risk areas for an audit.

Because entities on a blockchain must rely on information from other entities’ nodes, they could be exposed to the management policies of other parties on the blockchain. For example, the blockchain could extend agencies’ controls into other agencies or possibly non-federal entities, expanding the control environment. The general controls for the blockchain, such as security management and access controls, could potentially not be under the audited entity’s authority. However, these controls would be relevant to an audit involving the entity, and present unique challenges to the auditor.

Access controls may become a key area for blockchains.<sup>59</sup> The security of private keys—essentially the passcodes to the blockchain—could be critical for protecting the integrity of the blockchain’s data.<sup>60</sup> Failures related to private keys can happen instantaneously and irrevocably, making the information on the blockchain go from reliable to unreliable very quickly.

---

<sup>58</sup>GAO-14-704G. There are five components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring.

<sup>59</sup>Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure.

<sup>60</sup>Private keys, consisting of letters and numbers, are used in cryptography with the relevant algorithm to encrypt and decrypt data. The keys are to be shared only between the user who generates them and the user authorized to decrypt the data.

Consequently, private keys and associated controls could become a critical risk for blockchains serving as federal information systems.

Auditors may also consider how federal agency governance practices would be affected by the need for collaboration among participants on a blockchain. Blockchain technology introduces the need to rely on external parties because the control over the blockchain is diffused from one entity to several entities. Leaders from different entities would have to collaborate and agree on the process for changing the underlying code of a blockchain and related smart contracts, approving new users, and assigning authority. As a result, the use of blockchain technology may change the current approach to governance—and therefore auditors’ internal control assessment—by shifting the focus from a single agency to a collaborative environment.

### **Shared Service Blockchains**

In addition to potential challenges caused by blurred system boundaries and smart contracts, there may be further challenges for audits involving blockchain-as-a-service or a shared-service blockchain. Service organizations may engage blockchain specialists to issue reports that are specifically intended to meet the needs of entities that use such service organizations and their financial statement auditors. The user entity auditor may need to evaluate the internal controls at the service organization, such as through reading the relevant service auditor’s report and determining whether the report provides sufficient and appropriate audit evidence about the effectiveness of the service organization’s controls.

However, an agency’s use of a blockchain service may create unique challenges for the agency’s auditors as compared to an agency’s use of any other non-blockchain service. For example, the quality-of-service organization audit reports for blockchain might be insufficient for auditors to rely on them. These reports do not always include considerations unique to a blockchain, such as its decentralized environment.

Additionally, when reviewing service organization audit reports on blockchain for quality, auditors may need to think through the layering of various service organizations in order to determine whether the service organization audit report’s coverage is sufficient for their purposes. For example, the convening agency of a blockchain would likely need a service organization audit report for its controls. Depending on the participants of the blockchain, there may be a need for additional service organization audit



reports for the underlying cloud environment used by the blockchain, or for other provided services upon which the blockchain relies.

### Interfaces with the Blockchain

Interfaces with the blockchain also create risks that auditors may need to consider, such as lack of interoperability and the flow of inaccurate data into the blockchain. Auditors may have to evaluate risks arising from blockchain's integration with legacy systems. For example, while blockchain will likely need to work seamlessly with other systems of the entity to be an effective tool, most blockchain use cases today are standalone, with little evidence of successful interoperability. Reconciliations between the blockchain and other financial management systems would be necessary to demonstrate effective interfaces. Poor integration may lead to substandard outcomes, such as errors in financial information and a poor user experience.

Moreover, auditors may need to understand what financial management systems are synchronizing with the blockchain, since the interface transmission of data from these systems could be a key control point. Although blockchain secures data, that information is vulnerable to risks while outside the blockchain. Other systems may have invalid, inaccurate, or unauthorized information flowing into the blockchain, which the blockchain will not necessarily be able to detect. This issue could be further exacerbated because legacy systems are not always designed for sharing data on a broad scale across the entity or blockchain consortium. For example, different stakeholders may each have their own system for their individual needs, and not every stakeholder may use the same unit of measure. These silos could create problems for data sharing on a blockchain due to differences in data policies.

For highlights of the benefits, challenges, and actions auditors can perform regarding audit planning, see Table 2.

**Table 2: Considerations for Audit Planning**

BENEFIT	CHALLENGES	WHAT AUDITORS CAN DO
<p>Blockchain records are decentralized and verified by third parties. This may provide a predictable universe of transactions with which to plan audits.</p>	<p>Blockchain blurs system boundaries of audited entity.</p> <p>Smart contracts operating independently can blur the control and ownership of blockchain.</p> <p>Auditors' evaluation of an entity's internal control system and risk is affected.</p> <p>Auditors' reliance on service organization audit reports could be potentially affected.</p> <p>Blockchain exposes entities to the management policies of other parties on the blockchain, which is a risk that auditors must assess.</p>	<p>Assess the effectiveness of access controls to blockchain.</p> <p>Identify those in authority to oversee the blockchain to determine if authority is appropriate.</p> <p>Determine whether the service organization audit reports' coverage is sufficient for assurance on controls.</p>

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

## Audit Evidence and Resource Factors

As part of financial statement audits, the auditor gathers sufficient, appropriate audit evidence to report on the entity's financial statements, internal control, and, for certain agencies, whether the entity's financial management systems are in substantial compliance with applicable laws and regulations. In a similar way, auditors conducting performance audits determine the amount and type of evidence needed to obtain sufficient, appropriate evidence to address the audit objectives. Agency use of blockchains may affect how auditors conduct audits in several ways, including (1) gathering audit evidence, (2) executing audit procedures, and (3) using the resources required for the audit.

### Blockchain's Effect on Gathering Audit Evidence

The use of blockchain technology could streamline gathering audit evidence by (1) reducing the need to collect some data and (2) creating efficiencies in gathering data. However, blockchain may also present challenges to auditors in gathering evidence that may prevent efficiencies from being realized.

Auditors have traditionally faced the issue of the costs of gathering and preparing audit evidence from different sources. However, blockchain technology has the potential to reduce some of these costs because of its ability to store evidence from a variety of sources. For example, the use of tokenized grants in the grants financial management prototype could allow auditors to provide oversight over sub-grantee data that would be immediately available at the time of the transaction.

In addition, the number of external sources and documents needed for audit testing could be reduced because blockchain is designed to be an unalterable ledger of transactions and related details that both the audited agency and third-party participants agreed to via a consensus mechanism. This is especially relevant to auditors during the performance of audit procedures on the details of transactions. For example, the GAO and Council of the Inspectors General on Integrity and Efficiency *Financial Audit Manual* (FAM) discusses that tests of details, or procedures applied to individual items or transactions that the auditor selects for testing, include four types of tests.<sup>61</sup>

One type, external confirmation, includes auditors obtaining and evaluating direct responses from external parties verifying facts, such as the details of a transaction on an agency's ledger. External confirmations could theoretically become unnecessary in audits involving efficiently operating blockchains because all external parties to a transaction would be participants on the blockchain. This could mean that the third-party confirmation of a transaction that is typically provided by auditors obtaining external confirmations would be provided automatically on the blockchain. In practice, auditors could do this by obtaining the hash for a particular transaction using a read-only node, which may allow them to verify its occurrence.<sup>62</sup> However, if there is a risk of collusion among blockchain participants, the information on the blockchain could be insufficient for audit standards, and thus would require external confirmation.

---

<sup>61</sup>GAO and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual: Volume 1*, [GAO-22-105894](#) (June 2022, updated May 2023). The Financial Audit Manual (FAM) provides a methodology derived from professional auditing and attestation standards and OMB audit guidance. The four types of tests of details enumerated in the FAM are: external confirmation, observation, inspection, and recalculation.

<sup>62</sup>When a new block is added to the blockchain, it includes a number known as the hash digest, which the blockchain mathematically derives from the data in the previous block. The efficiencies hashes offer to auditors may be limited depending on several factors related to the blockchain's design, and whether or not all parties to transactions are participants on the blockchain. Further, some blockchains may save source documentation for transactions, and some would not. Source documentation is generally considered appropriate audit evidence.

Blockchains can assist in the seamless sharing of relevant and reliable information among participants. Such participants may include auditors with read-only nodes, as in the case of the grants financial management prototype. Auditors with read-only nodes have instant access to all transaction information stored on a blockchain. Because this information is immutable barring any collusion, auditors may have instant access to every transaction ever entered on the blockchain, which could streamline the process of gathering evidence for an audit. However, while blockchain has the potential to introduce efficiencies in evidence gathering, it also has limitations that could impact the extent of these efficiencies.

Blockchains will not provide all the audit evidence needed, nor guarantee error-free data for financial reporting. Documentary evidence may be necessary for the auditor to validate financial assertions relating to the existence, completeness, and accuracy of assets, liabilities, revenues, and costs.

Moreover, blockchains might not guarantee that a financial record, such as a general ledger account or trial balance, is complete because not all transactions may be recorded on a blockchain. Organizations currently employing blockchain technology tend to only record certain transactions related to accounts receivable and accounts payable onto the blockchain. In those instances, audit verification was still required because of the continued use of financial management systems by organizations for other relevant financial data.

Furthermore, blockchain cannot replace the extensive accounting knowledge required of auditors to determine whether ledger entries have been made correctly. Along with this limitation, auditors may need to consider if a blockchain validates ownership of transactions in the ledger and if its data legally qualifies as official financial records for an audited entity, as the data are not entirely under the entity's control. Consequently, data on a blockchain could require further analysis to become useful accounting information to auditors.

Lastly, data on a blockchain might need further processing for the purposes of periodic reporting. For example, blockchains, while reflecting all the transactions entered, do not always keep account balances current; thus, selecting transactions belonging to a specific period can be difficult. As a result, computing balances and validating transactions can require looking at the entire blockchain's history, which can expand the scope of the audit.



For highlights of the benefits, challenges, and actions auditors can perform regarding evidence gathering, see Table 3.

**Table 3: Considerations for Gathering Audit Evidence**

BENEFITS	CHALLENGES	WHAT AUDITORS CAN DO
<p>Blockchains can store evidence and supporting documentation within blocks, and can assist in the seamless sharing of information with auditors with read-only nodes. This may make evidence collection more efficient.</p> <p>Blockchain records can be verified immediately by auditors if they have read-only nodes on the blockchain, which could streamline evidence gathering.</p>	<p>Not all agency transactions are recorded on blockchains.</p> <p>Blockchains generally operate on a stand-alone basis and are not integrated with other agency systems.</p> <p>Other financial management systems with inaccurate data may interface with the blockchain, resulting in the need to test the entity's reconciliation of the blockchain to these systems.</p> <p>Blockchain data does not always provide evidence of ownership or asset existence and completeness.</p> <p>Erroneous and fraudulent transactions can still occur with accounting data secured on a blockchain.</p> <p>Blockchain cannot replace professional judgment.</p>	<p>Verify who owns the private key to validate ownership of transactions on the ledger.</p> <p>Be aware that audit procedures are still needed to detect erroneous and fraudulent transactions.</p> <p>Be aware that blockchain data could require further analysis to become useful accounting information.</p> <p>Understand that data contained in blockchains is not necessarily complete, accurate, valid, and relevant.</p>

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

### Blockchain’s Effect on Executing Audit Procedures

Audit procedures are the specific steps and tests that auditors perform to address the audit objectives. Blockchain and smart contracts might allow for the future automation of manual and repetitive audit procedures. Although not a benefit unique to blockchain, the use of blockchains can eliminate the need for recording and reconciling accounting data in multiple databases, saving time, and reducing the risk of human error. For example, when blockchains are used, the transactions are proactively reconciled by the participating nodes before being posted on the blockchain.<sup>63</sup> These proactive

<sup>63</sup>In permissioned blockchains, the nodes on the blockchain (network) are authorized by and thereby known on the blockchain. Therefore, specific nodes will be explicitly approved to verify and validate transactions.

reconciliations could reduce the need for subsequent reconciliations between the nodes.

Efficiencies in auditing accounting data could also occur, which is potentially a key benefit of blockchains. The integrity of the blockchain may reduce the time needed to reconcile agency records, assuming the necessary evidence and documentation is stored on the blocks. While this is possible, not all blockchains may store or provide sufficient evidence for all audits.

Depending on a variety of factors unique to each audited agency, auditors may need to plan procedures using data from feeder systems, external databases, or other sources. The auditor's required use of these other sources of information is inversely correlated to the efficiency a given blockchain provides to the audit.

Additionally, using smart contracts for audit testing could result in improved audit quality and financial reporting. Smart contracts could be leveraged as smart audit procedures. Attaching to smart contracts through programming code, these smart audit procedures are software programs designed to automatically execute audit procedures based on pre-defined conditions. Auditors can program smart audit procedures with "if-then" rules and load them onto the blockchain. These smart audit procedures allow auditors to gather potentially more reliable audit evidence, because of automation, which could also improve audit quality and financial reporting.

Smart audit procedures can automate manual and repetitive audit tasks that do not require auditor judgment, which allows auditors to focus resources on other areas that do require their judgment, such as higher risk areas. Auditors can also mitigate the risk of their own errors by using smart audit procedures. Additionally, auditors could play a role in monitoring how smart contracts are performing with these encoded smart auditing steps being executed alongside of the smart contracts.

Further, blockchain and smart audit procedures may present an opportunity to perform some tests on full populations of transactions for certain attributes, like external confirmations and observations as defined by the FAM, at a minimal cost.<sup>64</sup> While expanding beyond tests of samples to more expansive transaction testing is possible with audits involving traditional

---

<sup>64</sup>As discussed previously, external confirmations of transactions include obtaining and evaluating confirmation of a transaction's details from a third party. Observation includes an auditor observing a process or procedure being performed by an agency. Additional code written into smart contracts may serve as a proxy for the auditor in observing this smart contract process for all related transactions.



databases, blockchains may offer a more efficient path to testing more transactions. For example, programmers could design some audit procedures to be encoded in smart contracts. These encoded audit procedures could be the equivalent of constant auditor observation when smart contract transactions are executed.<sup>65</sup>

Additionally, as previously discussed with external confirmations, if all external parties to an agency's transactions participate on the blockchain, the consensus mechanism would provide external confirmation of all transactions. Further, wider sets of transaction data may be available on a blockchain than in traditional databases. This information on the blockchain has been pre-screened by blockchain participants and information is linked with related transaction details, which can ease audit tasks by reducing the need to match documentation from different sources.

However, auditors will have to consider whether the blockchain's potential for performing some tests of details for full populations is more efficient compared to traditional methods. The efficiency of increased transaction testing depends on the extent of information included on the blockchain as well as its participants. Consequently, auditors will likely have to use off-blockchain information to obtain sufficient evidence to support the amounts reported on the financial statements. As blockchain advances, it could allow for some testing performed on full populations; however, this ability would depend on the design, operation, and controls of the blockchain.

Blockchain's use can also improve audit quality by enhancing the reliability of audit evidence. This is a result of blockchain providing an unalterable record of transactions that is also decentralized. In addition, hosting accounting transactions on a permissioned blockchain could improve the reliability of the accounting data needed to prepare financial statements. Finally, the decentralization within a blockchain means that the evidence obtained from blockchain platforms often involves third parties in the transactions, which brings a higher degree of reliability than evidence provided just by the audit client.

Although transaction information on a blockchain is unalterable, this does not mean transaction information is free from error or fraud. Thus, determining the reliability of data is still paramount for auditors. As with any

---

<sup>65</sup>Efforts to design software to execute automated audit procedures have been attempted before the use of blockchain technology and smart contracts.

other system, the “garbage in, garbage out” principle applies to blockchain, meaning that an incorrect transaction entered will result in incorrect reporting by that system. Because of this, auditors will need to assess the business process, application, and data management controls related to the transactions taking place on the blockchain. FISCAM generally provides a methodology for auditors to do these assessments, but the unique aspects of blockchains may require further refinement by the auditor. Auditors will also need to determine the sources of information needed to obtain sufficient, appropriate evidence supporting recorded balances and transactions, some of which may be off-blockchain.

### **Data Reliability: Garbage In, Garbage Out? Trust, but Verify**

- 1. Data Quality:** The reliability of data is significantly influenced by its quality. Data should be accurate, valid, complete, timely, consistent, and relevant to ensure its usefulness in financial transactions and decision-making processes.
- 2. Accurate Data Entry:** Initial data entering the blockchain must be accurate to ensure that the information processed and reported is reliable. Even the most robust systems cannot fix incorrect or incomplete initial data.
- 3. Comprehensive Data Verification:** Data must be verified for accuracy and completeness. This could involve automated checks or manual reviews.
- 4. Regular Data Audits and Reconciliations:** Periodic audits and reconciliations of data ensure ongoing reliability by identifying and resolving any discrepancies, errors, or inconsistencies. Sampling techniques can assist in this process.

**Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01**

Additionally, blockchains often work in concert with the other financial management systems of an entity. As previously mentioned, these systems may have invalid, inaccurate, or unauthorized information flowing into the blockchain, which the blockchain cannot always detect. As a result, controls for recording information in these systems can be key to ensuring the reliability of data coming into the blockchain from legacy systems. Therefore,

the controls of the financial management systems interfacing with the blockchain will also have to be assessed by auditors.

Further, the transactions stored on blockchains may still be fraudulent, illegal, or unauthorized. Similarly, a transaction occurring on a blockchain is not proof that a transaction has occurred in the real world. Although a blockchain can prove a digital transaction has occurred, a gap between the digital and physical world still exists. Due to these risks, controls to prevent asset misappropriation and inaccurate information are still necessary in a blockchain environment, as are audits of those controls, as well as gathering sufficient, appropriate audit evidence.

For highlights of the benefits, challenges, and actions auditors can perform regarding executing audit procedures, see Table 4.

**Table 4: Considerations for Executing Audit Procedures**

BENEFITS	CHALLENGE	WHAT AUDITORS CAN DO
<p>Blockchain may increase the efficiency of audits, and allow smart contracts to automate manual and repetitive audit tasks.</p> <p>Blockchain may allow efficiencies to test full populations for certain attributes instead of statistical samples.</p> <p>Blockchain's potential efficiencies could allow auditors to focus resources on high-risk areas.</p>	<p>Blockchain records can still be fraudulent, illegal, or unauthorized.</p>	<p>Determine the utility of full population testing, and weigh it against the costs.</p> <p>Monitor how smart contracts with encoded auditing steps are being executed.</p>

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

### Blockchain’s Effect on Audit Resources

When auditing a federal agency that uses blockchain technology, auditors will need to evaluate the potential benefits that the blockchain provides—through more reliable and easily accessible audit evidence—against the cost of resources needed to test the design, implementation, and operating effectiveness of the blockchain’s controls.

Additionally, auditing blockchains require skillsets that include an understanding of the blockchain itself. To attain this understanding, auditors may need special training in the areas of systems and security, smart contracts, data science, statistics, and cryptography, due to blockchain's technical complexity. Acquiring this technical competence could be challenging for auditors. Further, if contracting out these duties to experts, auditors may still not necessarily have the knowledge to supervise the experts. Due to the high demand for talent and expertise in this space, internal training could be necessary for audit organizations to build these skillsets.

On the other hand, improved audit quality could potentially occur if continuous audit procedures or real-time auditor monitoring are implemented. For example, if previous financial statement audits identified certain line items as consistently being at risk of material misstatement, auditors could monitor the related transactions year-round using a read-only node. However, continuous audit procedures or auditor monitoring of financial transactions in real-time, is a substantial change from the way financial audits are currently performed, and the cost-benefit analysis of this change would have to be considered. Also, it may require additional audit resources to investigate potentially erroneous transactions that may be identified through continuous auditing. It is also unknown whether agencies would approve of giving this continuous access to auditors.

Nevertheless, current financial audit procedures can be labor-intensive and costly. For example, at the beginning of each audit, auditors may receive journal entries, spreadsheet files, and other documents. Before the actual audit process begins, auditors invest significant time in preparing the data and planning the audit, which require identifying transactions and balances.

Blockchains, by their nature, can provide access to financial transaction records almost immediately and can potentially provide substantial efficiencies. However, auditors would still need to utilize their knowledge of accounting to ensure that transactions are adequately supported and recorded in the right lines of accounting according to standards, estimates are fair, and other issues requiring professional expertise are addressed. Providing assurance over balances on financial statements requires other information, such as knowledge of the obligations of the entity, that would likely not be included on the blockchain. Blockchain introduces potential efficiencies, but these efficiencies could be limited in the context of auditing.

Although the effect of blockchain technology on federal audits has yet to be determined, auditors could take these considerations into account when

preparing for a future where blockchains could be widely used to support agency financial management. However, these considerations are only applicable to blockchains generally, and may be substantially impacted by the design and implementation of a specific blockchain.

For highlights of the benefits, challenges, and actions auditors can perform regarding audit resources, see Table 5.

**Table 5: Considerations for Audit Resources**

BENEFIT	CHALLENGE	WHAT AUDITORS CAN DO
Blockchain could potentially enable continuous auditing in the future.	Auditing blockchain requires skillsets that could be difficult to (1) acquire; or (2) adequately supervise if hiring experts.	Provide training to build necessary skillsets.

Source: Joint Financial Management Improvement Program (JFMIP). | JFMIP-24-01

## GAO’s Read-Only Node on the Grants Financial Management Prototype

As described previously, one intent of the JFMIP initiative was to explore considerations related to expanding Fiscal Service’s blockchain. The other intent was to explore oversight considerations related to an auditor having read-only access to transactions occurring on a blockchain. For example, the coordination between financial auditors and information systems auditors will be impacted by blockchain, since additional training may be required for auditors to effectively supervise experts.

Given independence requirements firmly established in the audit profession, a read-only node, as opposed to a read-write node, may be a more plausible way to optimize the potential efficiencies of a blockchain node while not risking auditor participation in the transactions of the audited entity. Further, it may allow auditors to have more control over when and how they access data within a blockchain to better suit the needs of the auditors.

### Considerations for Auditors of Federal Agencies

A read-only node on a blockchain could provide auditors with instant and continuous access to information, potentially affecting both the planning and execution phases of the audit. During planning, the FAM instructs auditors to gather information from a variety of sources to evaluate risk. The auditor’s evaluation of risk affects the nature, extent, and timing of other audit



procedures, such as tests of controls and tests of details. A read-only node could provide information to the auditor for planning purposes and enable the auditor to perform planning procedures such as risk assessments more easily.

Additionally, during execution of audit procedures, the FAM states that using evidence that can be more readily obtained may be more efficient. The higher the quality of a type of evidence, the greater the level of assurance the auditor may derive from that type. These are some of the factors that determine the appropriate mix of tests.

As discussed earlier, blockchain has the potential to streamline the gathering of audit evidence, reflected in the read-only node. The read-only node could be an efficient source of evidence by providing readily available information, affecting the procedures necessary for completing the audit. Moreover, the read-only node could impact the quality of evidence. The FAM establishes that data obtained from an independent source outside the entity are generally more reliable than data obtained from inside the entity. Auditors may have to consider where data from the read-only node falls on this spectrum of externality. For further discussion of how blockchain could streamline the evidence gathering process, see the “Audit Evidence and Resource Factors” section above.





## Appendix I: Methodology

In August 2021, the Joint Financial Management Improvement Program (JFMIP) embarked on its initiative with its principal agencies, the Department of the Treasury, the Government Accountability Office (GAO), the Office of Personnel Management (OPM), and the Office of Management and Budget (OMB), with goals to (1) provide information technology (IT) considerations for a potential multi-agency blockchain, including cybersecurity, authority-to-operate, and operational factors and (2) explore potential federal financial management, human capital, and oversight efficiencies and challenges in using blockchain technology. To address the first goal, we identified IT considerations for federal agencies implementing blockchain by testing the blockchain prototype, interviewing experts and cognizant officials, and analyzing and reviewing documents found during literature reviews. To address the second goal, we explored potential federal financial management, human capital, and oversight efficiencies and challenges by interviewing experts and cognizant officials and analyzing and reviewing documents found during literature reviews. See below for more details on each of these methodologies.

### Goal 1: Information Technology Considerations

***Testing of Blockchain Prototype.*** We conducted hands-on testing and setup of the blockchain prototype. We also used the MongoDB Compass tool for access to the off-chain database, and the Postman Application Programming Interface (API) tool for access to the front end user interface.<sup>66</sup>

The grants financial management blockchain prototype was tested to ensure that all aspects of the system were operational. This included user interface testing, data validation, and transaction processing on the blockchain. Test cases were created to simulate various scenarios, such as normal usage and error handling.

The grants financial management blockchain prototype's testing included not only testing the front end user interface, but also verifying the correlation of grant financial management actions with blockchain transactions. This was accomplished by cross-referencing blockchain transactions with the expected outcomes of grant financial management actions using the transaction hash. This type of testing is critical for ensuring the grants financial management system's integrity and accuracy because it ensures that all transactions are properly recorded and processed on the blockchain.

***Interviews.*** We interviewed representatives from the Department of Homeland Security, the Department of Health and Human Services, the United States Postal Service, and external firms such as KPMG and Ernst & Young. These interviews gave us valuable insights into the strategies used by these agencies to implement blockchain technology, which assisted us in developing our own

<sup>66</sup>Compass is a free interactive tool for querying, optimizing, and analyzing MongoDB data. Postman is an API platform for building and using APIs.

assessment strategies. We were able to gain a better understanding of the challenges and opportunities associated with blockchain implementation in the federal government by participating in these interviews, as well as best practices and lessons learned from agencies that have already begun using this technology. We were able to develop a comprehensive approach to assessing blockchain solutions using this information, considering both the unique needs of our clients and the broader landscape of blockchain adoption across the federal government.

**Document Review.** We conducted a thorough review of several relevant publications as part of our assessment of the blockchain infrastructure. Articles, guidelines, and reports from reputable sources such as the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), the Cybersecurity and Infrastructure Security Agency (CISA), and GAO. We reviewed the following:

- Tan, Boon Seng, and Kin Yew Low. "Blockchain as the Database Engine in the Accounting System." *Australian Accounting Review*, no. 89, vol. 29, issue 2 (2019), pp. 312-318.
- Schmitz, Jana, and Giulia Leoni. "Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda." *Australian Accounting Review*, no. 89, vol. 29, issue 2 (2019), pp. 331-342.
- NIST, *Shared Services for Cybersecurity: A Guide for Federal Agencies*. Unpublished internal document provided by NIST.
- OMB, *Shared Services: A Guide for Federal Agencies*. Unpublished internal document provided by OMB.
- CISA, *Shared Services for Cybersecurity: Leveraging the Power of Community*. Unpublished internal document provided by CISA.
- Choo, Kim-Kwang Raymond, Ali Dehghantanha, and Reza M. Parizi. "Blockchain Cybersecurity, Trust, and Privacy," *Springer*, vol. 79 (2020).
- GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).
- GAO, *Assessing Data Reliability*. GAO-20-283G. (Washington, D.C.: updated Dec. 2019).
- NIST, *Special Publication - Digital Identity Guidelines*, NIST SP 800-63-3 (Mar. 2, 2020).
- NIST, *Special Publication - Digital Identity Guidelines: Enrollment and Identity Proofing*, NIST SP 800-63A (Mar. 2, 2020).

	<ul style="list-style-type: none"> <li>• NIST, <i>Special Publication - Digital Identity Guidelines: Authentication and Lifecycle Management</i>, NIST SP 800-63B (Mar. 2, 2020).</li> <li>• NIST, <i>Special Publication - Digital Identity Guidelines: Federation and Assertions</i>, NIST SP 800-63C (Mar. 2, 2020).</li> <li>• OMB, <i>Managing Information as a Strategic Resource</i>, OMB Circular No. A-130 (revised 2016).</li> </ul>
<p><b>Goal 2: Federal Financial Management Considerations</b></p>	<p><b>Interviews.</b> We interviewed representatives from the National Science Foundation, Department of Health and Human Services, Department of Commerce, NIST, and Federal Demonstration Partnership. These interviews gave us valuable insights into the needs of the grants processes, focusing on the financial management aspects, and provided feedback on the prototype and its potential to help streamline the processes.</p> <p><b>Document Review.</b> We conducted a thorough review of several relevant publications as part of our assessment of the blockchain technology and understanding of the grants processes. The following articles, guidelines, and reports from reputable sources such as NIST, OMB, and GAO were reviewed.</p> <ul style="list-style-type: none"> <li>• Nicolai Anderson, <i>Blockchain Technology: A game-changer in accounting?</i>, (Berlin, Germany: Deloitte Deutschland, 2016).</li> <li>• Olivier Gakwaya, Dr Uta Meier-Hahn, Dr Ralph Oyini Mbouna and Lars Wannemacher, “Blockchain in Africa: Opportunities and Challenges for the next Decade,” (Kigali, Rwanda, 2020).</li> <li>• William Bible, Jon Raphael, Peter Taylor, and Iliana Oris Valiente, “Blockchain Technology and Its Potential on the Audit and Assurance Profession,” (Toronto, Canada: CPA Canada, 2021).</li> <li>• Derrick Bonyuet, “Overview and Impact of Blockchain on Auditing,” <i>The International Journal of Digital Accounting Research</i>, vol. 20, pp. 31-43, (2020).</li> <li>• Jun Dai and Miklos A. Vasarhelyi, “Toward Blockchain-Based Accounting and Assurance,” <i>Journal of Information Systems</i>, vol. 31, no. 3 (2017).</li> <li>• Tatiana Garanina, Mikko Ranta, and John Dumay, “Blockchain in Accounting Research: Current Trends and Emerging Topics,” <i>Accounting, Auditing &amp; Accountability Journal</i>, Vol. 35 No. 7, pp. 1507-1533 (2022).</li> <li>• Sten Hankewitz, “The Bank of Estonia Tests the Technological Possibilities of a Central Bank Digital Currency.” <i>Estonian World</i>, December (December 19, 2021).</li> </ul>

	<ul style="list-style-type: none"> <li>• Petteri Kivimäki, “There Is No Blockchain Technology in X-Road,” Nordic Institute for Interoperability Solutions, Nordic Institute for Interoperability Solutions, (May 5, 2020).</li> <li>• Mary Lacity, and Remko Van Hoek, “Requiem of Reconciliations: DL Freight, a Blockchain-Enabled Solution by Walmart Canada and DLT Labs,” Blockchain Center of Excellence, University of Arkansas (January 2021).</li> <li>• Manas Pattanaik, “Blockchain for Global Payments, Oracle Financial Services Blog (April 14, 2020).</li> <li>• Tom Phillips, “Estonia’s Central Bank Tests Blockchain-Powered Digital Euro Solution,” NFCW, (July 28, 2021).</li> <li>• Pritt Martinson, “Estonia – the Digital Republic Secured by Blockchain,” (Tallinn, Estonia: PricewaterhouseCoopers, 2019).</li> <li>• Juan Ignacio Ibañez, Chris Bayer, Tasca Paolo, and Jiahua Xu, “Triple-entry accounting, Blockchain and next of kin: Towards a standardization of Ledger terminology,” Centre for Blockchain Technologies, University College of London (January 20, 2021).</li> <li>• David Stahler, and Anthony Waelter. “Digital Controllershship™,” Deloitte US, Deloitte United States, Center of Controllershship, 2018).</li> <li>• Jon Raphael, and Amy Steele, “Audit transformation and opportunities in cognitive, blockchain, and talent”, Deloitte United States, (2020).</li> <li>• Lisa Mosley, Jeremy Forsberg, and David Ngo, “Reducing Administrative Burden in Federal Research Grants to Universities,” IBM Center for The Business of Government, (2020).</li> </ul>
<p><b>Goal 2: Human Capital Considerations</b></p>	<p><b>Interviews.</b> We participated in interviews with representatives from the National Science Foundation, the United States Postal Service, and external firms including Deloitte, KPMG, Grant Thornton, and Ernst &amp; Young. These interviews focused mostly on financial management improvement concerns, but were analyzed for human capital considerations.</p> <p><b>Document Review.</b> We performed multiple searches of publications to provide us with background information on the use of blockchain technology and the implications for human capital. The searches were scoped to materials that used variations on terms related to blockchain and auditing in the context of the U.S.</p>

	<p>government sector. Additionally, we reviewed other studies which were surfaced by other agencies participating in this initiative.</p> <ul style="list-style-type: none"> <li>• NIST, <i>Shared Services for Cybersecurity: A Guide for Federal Agencies</i>. Unpublished internal document provided by NIST.</li> <li>• OMB, <i>Shared Services: A Guide for Federal Agencies</i>. Unpublished internal document provided by OMB.</li> <li>• CISA, <i>Shared Services for Cybersecurity: Leveraging the Power of Community</i>. Unpublished internal document provided by CISA.</li> <li>• OMB, <i>Managing Information as a Strategic Resource</i>, OMB Circular No. A-130 (revised 2016).</li> <li>• NIST, <i>Special Publication - Digital Identity Guidelines</i>, NIST SP 800-63-3 (Mar. 2, 2020).</li> <li>• NIST, <i>Special Publication - Digital Identity Guidelines: Enrollment and Identity Proofing</i>, NIST SP 800-63A (Mar. 2, 2020).</li> <li>• NIST, <i>Special Publication - Digital Identity Guidelines: Authentication and Lifecycle Management</i>, NIST SP 800-63B (Mar. 2, 2020).</li> <li>• NIST, <i>Special Publication - Digital Identity Guidelines: Federation and Assertions</i>, NIST SP 800-63C (Mar. 2, 2020).</li> <li>• NIST, <i>Internal Report - Blockchain Technology Overview</i>, NISTIR 8202 (October 2018).</li> <li>• GAO, <i>Technology Assessment - Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges</i>. GAO-22-104625 (Washington, D.C.: Mar. 23, 2022).</li> </ul>
<p><b>Goal 2: Oversight Considerations</b></p>	<p><b>Interviews.</b> We interviewed representatives from the National Science Foundation, the United States Postal Service, and external firms including Deloitte, KPMG, Grant Thornton, and Ernst &amp; Young. These interviews gave us valuable insights from practitioners on blockchain’s impact on financial management processes and implications for auditing.</p> <p><b>Document Review.</b> We performed an initial search of publications published between January 2017 and May 2022 to provide us with background information on the use of blockchain technology and the implications for audits. The results of the search process provided documents that helped us gain some familiarity with blockchain technology and related audit considerations. We limited our search to materials that used variations on terms related to blockchain and auditing in the context of the U.S. government sector.</p> <p>The search was targeted toward the following sources: scholarly (peer reviewed) material, working papers, conference papers,</p>

	<p>government reports, and association/nonprofit/think tank publications. After an initial review for relevance and excluding articles that primarily focused on countries outside of North America or Western Europe, we identified 79 abstracts for further review. After analyzing abstracts for the 79 articles identified from the literature search, we determined that 30 articles were relevant.</p> <p>From our analysis of those articles, we identified additional search terms for a second, more targeted search of studies. The time frame for this search was January 2017 through July 2022. The scope of our second search excluded association/nonprofit/think tank publications and trade and/or industry articles as we deemed these publications and articles not rigorous enough to be used as support.</p> <p>We searched key databases such as Scopus, a large multidisciplinary database of abstracts from peer-reviewed literature, and dozens of databases aggregated in the Dialog, EBSCOhost, and ProQuest research platforms for material generally related to the use of blockchain technology for auditing in the government sector.<sup>67</sup> The second search provided 137 results: 116 scholarly journal articles, 20 conference papers, and one government report. After receiving the results, we decided to focus on the 116 scholarly articles published in peer-reviewed journals. We performed the following steps to arrive at seven articles for which we would do in-depth reviews. Finally, based on citation counts, we then added three articles, as described below.</p> <ul style="list-style-type: none"> <li>• Two reviewers on the JFMIP Blockchain Initiative team read through the abstract of each article to determine its relevance. If the reviewers differed on whether the article was relevant, we discussed it and reached a final determination. We determined 57 of these articles were relevant.</li> <li>• We chose to focus on U.S. based articles since the scope of this work is to provide information and input for U.S. government and regulatory entities. Therefore, we screened out articles published in international journals, journals specific to another country, and journals with editorial boards that primarily consisted of representatives from foreign universities.</li> <li>• We tested, using citation counts from the Scopus database, as to whether our methodology of limiting our articles to those in U.S. -based publications excluded valuable articles. We identified three articles that were published in international journals that were cited more than 20 times in other publications. Based on this analysis, we added three articles to</li> </ul>
--	---

---

<sup>67</sup>In total, we looked at over 100 databases through these platforms, spanning many disciplines and types of literature. Keyword searches were conducted across all of these databases to locate relevant materials in academic journals, working papers, and government reports.



the seven articles in U.S.-based journals for a total of 10 articles.

The 10 articles selected are listed below.

- Dai, Jun, and Miklos A. Vasarhelyi. "Toward Blockchain-Based Accounting and Assurance." *Journal of Information Systems*, vol. 31, no. 3 (2017), pp. 5-21.
- Coyne, Joshua G., and Peter L. McMickle. "Can Blockchains Serve an Accounting Purpose?" *Journal of Emerging Technologies in Accounting*, vol. 14, no. 2 (2017), pp. 101-111.
- Pimentel, Erica, and Emilio Boulianne, Shayan Eskandari, and Jeremy Clark. "Systemizing the Challenges of Auditing Blockchain-Based Assets." *Journal of Information Systems*, vol. 35, no. 2 (2021), pp. 61-75.
- Rozario, Andrea M., and Chanta Thomas. "Reengineering the Audit with Blockchain and Smart Contracts." *Journal of Emerging Technologies in Accounting*, vol. 16, no. 1 (2019), pp. 21-35.
- Rozario, Andrea M., and Miklos A. Vasarhelyi. "Auditing with Smart Contracts." *The International Journal of Digital Accounting Research*, vol. 18, 2018, pp. 1-27.
- Sargent, Carol Springer. "Replacing Financial Audits with Blockchain: The Verification Issue." *Journal of Computer Information Systems* (2021).
- Smith, Sean Stein, and John Castonguay. "Blockchain and Accounting Governance: Emerging Issues and Considerations for Accounting and Assurance Professionals." *Journal of Emerging Technologies in Accounting*, vol. 17, no. 1 (2020), pp. 119-131.
- Vincent, Nishani Edirisinghi, and Reza Barkhi. "Evaluating Blockchain Using COSO." *Current Issues in Auditing*, vol. 15, no. 1 (2021), pp. A57-A71.
- Tan, Boon Seng, and Kin Yew Low. "Blockchain as the Database Engine in the Accounting System." *Australian Accounting Review*, no. 89, vol. 29, issue 2 (2019), pp. 312-318.
- Schmitz, Jana, and Giulia Leoni. "Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda." *Australian Accounting Review*, no. 89, vol.29, issue 2 (2019), pp. 331-342.

In addition to the 10 articles selected for evaluation from the results of our document review, we utilized the following 12 articles as background information to help contextualize the blockchain considerations for oversight that were discovered through interviews

and the document review. Auditor expertise and professional judgment were utilized to identify these articles.

- NIST, *Shared Services for Cybersecurity: A Guide for Federal Agencies*. Unpublished internal document provided by NIST.
- OMB, *Shared Services: A Guide for Federal Agencies*. Unpublished internal document provided by OMB.
- CISA, *Shared Services for Cybersecurity: Leveraging the Power of Community*. Unpublished internal document provided by CISA.
- OMB, *Managing Information as a Strategic Resource*, OMB Circular No. A-130 (revised 2016).
- NIST, *Special Publication - Digital Identity Guidelines*, NIST SP 800-63-3 (Mar. 2, 2020).
- NIST, *Special Publication - Digital Identity Guidelines: Enrollment and Identity Proofing*, NIST SP 800-63A (Mar. 2, 2020).
- NIST, *Special Publication - Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST SP 800-63B (Mar. 2, 2020).
- NIST, *Special Publication - Digital Identity Guidelines: Federation and Assertions*, NIST SP 800-63C (Mar. 2, 2020).
- NIST, *Internal Report - Blockchain Technology Overview*, NISTIR 8202 (October 2018).
- Choo, Kim-Kwang Raymond, Ali Dehghantanha, and Reza M. Parizi. "Blockchain Cybersecurity, Trust and Privacy," *Springer*, vol. 79 (2020).
- GAO, *Standards for Internal Control in the Federal Government*. GAO-14-704G (Washington, D.C.: Sept. 2014).
- GAO. *Assessing Data Reliability*. GAO-20-283G. (Washington, D.C.: updated December 2019).
- The MITRE Corporation, *Report - Assessing the Potential to Improve Grants Management Using Blockchain Technology*, June 2019

## Appendix II: Technical Details of Blockchain Prototype

### Part 1 – Tracing a Grant with the Blockchain Prototype

What follows is an example of tracing a grant created on the Grant Financial Management Blockchain Prototype user interface to the back end blockchain node, which is the blockchain prototype’s connection to the Ethereum platform that is not customer facing. The user interface accepts all user entries, such as new grant creation and drawdown requests, and the back end carries out the transaction on the blockchain, which includes the consensus mechanism process and hashing. The Address and Transaction below represents the hashing that takes place in the back end, which is the process of linking the blocks of transactions together such that they are immutable.

Screen shot of the user interface view of Grant to “Internet of Things for Air Quality (03242023-1)”:

DATE	TOPIC	ORIGIN	STATUS
MAR 24, 2023	Grant Created	NSF	COMPLETE
<b>Timestamp</b> Friday, March 24, 2023 8:56 AM			
<b>Address</b> 0x51E93FF5Ccb86374786826A8Da438a277Fc5Ed15		<b>Transaction Hash</b> 0xcd318dae29c6c193b1bcb1178643b6c2e2c586c86bbf4d227b77bc0b353e938f	
MAR 24, 2023	Funds Transferred	NSF	COMPLETE
<b>Timestamp</b> Friday, March 24, 2023 8:56 AM			
<b>Address</b> 0x51E93FF5Ccb86374786826A8Da438a277Fc5Ed15		<b>Transaction Hash</b> 0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd	

As can be seen on the user interface screen shot above, and the back end node screen shots below, the blockchain transaction address “0x51e93ff5ccb86374786826a8da438a277fc5ed15” and the transaction hash “0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd” are both identical on the user interface and the back end node. A second screen shot of the back end node has been included below, without the blockchain transaction address’s pop-up window obscuring it. As you can see in both back end node screen shots, the transaction hash is also in the first row following the “Transaction –“ title. This information can be used to track any transaction performed on the blockchain.

Screen shot of Blockchain transaction as seen from the back end node:

... / Block Explorer / Transactions / 0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd... Help & Support ORGANIZATION GAD

### Transactions

Transaction - 0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd

Hash	0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd
Block	5846300
From	Addr...   51e93f
To	Cont...   a98d76
Gas	6721975
Status	Success
Timestamp	3/24/2023, 8:56:53 AM (6 months ago)

Input Data

Hex Viewer  
 Hex

```
00000000: b48a b0b5 0000 0000 0000 0000 0000 0000 .....
00000010: 7448 efe1 b36d 3ed9 88e2 fea5 ea9a 304e TH...B>.....9M
00000020: 9a9f 8c5a 0000 0000 0000 0000 0000 0000 .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000040: 0000 0030 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0140 0000 0000 0000 0000 0000 0000 .....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000080: 0000 0200 0000 0000 0000 0000 0000 0000 .....
```

... / Block Explorer / Transactions / 0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd...

### Transactions

Transaction - 0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd

Hash	0x49d31040964d522ef9a5fa394ef0f196d3698fe096741cd15cf5e5e4936027cd
Block	5846300
From	Addr...   51e93f
To	Cont...   a98d76
Gas	6721975
Status	Success
Timestamp	3/24/2023, 8:56:53 AM (4 minutes ago)

## Part 2 – Smart Contracts and Solidity Programming Language

Solidity is a high-level programming language that is used to create smart contracts on the Ethereum blockchain platform. It is classified as a "contract-oriented" language, which means that its syntax and structure are specifically designed for writing smart contracts.

Unlike general-purpose programming languages like Java or Python, which are intended to support a wide range of programming tasks, Solidity is designed specifically for writing code that runs on the blockchain. As such, it includes several blockchain-specific features, such as the ability to manage digital assets and enforce specific rules and conditions for their transfer.

## Part 3 – The Grants Management Blockchain Prototype Token

ERC is an abbreviation for Ethereum Request for Comments, a technical standard for smart contracts on the Ethereum blockchain. There are many ERC tokens in use, but ERC-1155 is used in the blockchain prototype:

This token type is used for both fungible and non-fungible tokens and is intended to be more efficient than other ERC token types.

## Part 4 – Blockchain Prototype Actions

### Grant Actions

- Create Grant
- Update Grant
- Threshold Update Options
- Search for Grant by AwardID, Granting Agency, or Awardee

### Authentication Actions

- Create User
- User Login

### Drawdown Requests Actions

- Create New Request
- Create New Request Batch
- Reject Request
- Approve Request
- Search for Request by AwardID or Awardee
- Redeem or Return Token from Drawdown

### Utilities Actions

- Search for User or Granting Agency
- Search for Pre-Population Data (previously known information about Granting Agencies or Awardees such as demographic information and drawdown history that can be automatically populated by the system)
- Deploy the ERC-1155 Token
- Deploy the Grant Factory application (The Grant Factory is a smart contract that creates and tracks funds in the grant payment process. It ensures that grants are unique and records

events, such as grant creations and fund transfers among participants.)

- Search for Grant or Sub-Grant Balance
- Search by Transaction ID Numbers

#### Sub-Grant Actions

- Create Sub-Grant
- Search for Sub-Grant by AwardID or Prime Grantee



## Appendix III: Additional Information on Related Laws, Regulations, and OMB Guidance

### Federal Financial Management Law

Currently, federal law does not explicitly address the use of blockchain technology in the financial management of federal entities. However, current federal laws, regulations, and guidance that govern federal agency financial management, grants administration, information technology (IT) systems, and personal privacy information may apply to blockchains that federal agencies develop, such as to streamline grants administration.

A federal agency developing blockchains for internal use must ensure that the technology will provide the financial data needed to fulfill a variety of federal financial management requirements. Most fundamentally, any blockchain system that governs the payment of federal funds must support the legal requirements for control of those funds. For example, federal agencies must ensure that funds are not obligated or expended in excess of available budget authority.<sup>68</sup> Obligations of federal funds must be duly recorded and supported by documentary evidence.<sup>69</sup> Executive agencies must also have a system of internal control to reasonably ensure that obligations and costs comply with law, assets are safeguarded, and revenues and expenditures are recorded and accounted for properly.<sup>70</sup> Further, federal officials known as certifying officers face potential personal financial liability for payments made improperly.<sup>71</sup>

There are also many legal requirements for federal agencies to account for and report on their finances. While developing grants administration blockchains, federal agencies must ensure that they can appropriately account for transactions conducted on blockchains so that they can prepare required reports and support inquiries from auditors and other oversight bodies. For example, most executive agencies must prepare annual audited financial statements covering the financial position and results of operations of the entire agency.<sup>72</sup> These statements must be

---

<sup>68</sup>31 U.S.C. §§ 1341, 1517.

<sup>69</sup>31 U.S.C. § 1501.

<sup>70</sup>31 U.S.C. § 3512(c). GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014). This publication provides the overall framework for establishing and maintaining a system of internal control.

<sup>71</sup>31 U.S.C. § 3528.

<sup>72</sup>31 U.S.C. § 3515.

consistent with guidance from the Office of Management and Budget (OMB) and accounting standards applicable to federal entities.<sup>73</sup> A separate statutory requirement calls for executive agencies to assess the risks of, and publish certain information on, improper payments in their programs.<sup>74</sup> Additionally, certain large federal agencies must develop and maintain integrated accounting and financial management systems that comply substantially with federal financial management systems requirements, federal accounting standards, and the U.S. standard general ledger at the transaction level.<sup>75</sup>

An agency implementing a blockchain-based grants administration system may also consider requirements for public data reporting. The Federal Funding Accountability and Transparency Act of 2006, as amended, requires agencies to report data about certain federal contracts, loans, and grant awards on a public website, which is currently USASpending.gov.<sup>76</sup> These data include linkages between spending data and federal program activities. Agencies must certify quarterly that their data submissions are valid and reliable.

## Federal Information Systems Security Requirements

**Legislation.** In addition to passing legislation on federal financial management, Congress, over the years, has addressed serious information security weaknesses related to information systems through legislation. This legislation does not specifically address blockchain; however, the current federal laws, regulations, and guidance that govern IT systems may apply to blockchains. First passed in 2002, FISMA is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.<sup>77</sup> To accomplish this, FISMA requires each

---

<sup>73</sup>OMB's guidance on annual financial reports is contained in Circular No. A-136, *Financial Reporting Requirements*. The Federal Accounting Standards Advisory Board is recognized as the body that establishes generally accepted accounting principles for federal entities. See <https://fasab.gov>.

<sup>74</sup>31 U.S.C. § 3352.

<sup>75</sup>Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, div. A, §101(f), title VIII, 110 Stat. 3009, 3009-389, *reprinted in* 31 U.S.C. § 3512 note. This requirement applies to the 24 federal departments and agencies listed in section 901(b) of title 31, U.S. Code. These entities are commonly referred to as "Chief Financial Officer Act agencies."

<sup>76</sup>Federal Funding Accountability and Transparency Act of 2006, Pub. L. No. 109-282, 120 Stat. 1186, *codified as amended at* 31 U.S.C. § 6101 note.

<sup>77</sup>The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 120 Stat. 3073, largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L.

agency to develop, document, and implement an agency-wide information security program for the information and systems that support the agency's operations and assets, using a risk-based approach. These operations and assets include those provided or managed by another agency or contractor, or other sources. To support this requirement, most information systems and applications used by federal agencies must follow the National Institute of Standards and Technology's (NIST) Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, as the standard for the assessment and authorization process before being put into production, and perform this process every five years after being put into production.<sup>78</sup>

Further, to facilitate the adoption and use of cloud services, OMB established the Federal Risk and Authorization Management Program (FedRAMP) in 2011. The program provides a standardized approach for selecting and authorizing the use of cloud services that meet federal security requirements, which may apply if agencies choose to leverage cloud services for their blockchain. Managed by the General Services Administration, the program aims to ensure that cloud computing services have adequate information security, while also eliminating duplicative efforts and cost inefficiencies. Agencies are required to use FedRAMP to authorize the use of cloud services. FedRAMP's security requirements and guidelines meet the provisions of FISMA and implementing guidance.

**Agency Guidance.** In addition to legislation enacted to respond to information security, agencies have issued guidance and regulations generally applicable to information systems that may include blockchain systems used within the federal government. OMB is required by FISMA to develop and oversee the implementation of policies, principles, standards, and guidelines for information security. In Circular No. A-130, *Managing Information as a Strategic Resource*, OMB directed agencies to follow NIST's information security standards.<sup>79</sup> For example, NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes standards and guidelines, including minimum requirements, for

---

No. 107-347, 116 Stat. 2899, 2946-2961. As used in this report, FISMA refers to both FISMA 2014 and to those provisions of FISMA 2002 that were incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

<sup>78</sup>The standards and guidelines found in NIST SP 800-37 do not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems.

<sup>79</sup>NIST Special Publications are technical standards outlining computer security policies and guidelines for the federal government (i.e., NIST 800 series).

providing adequate information security for agency operations and assets.<sup>80</sup> OMB Circular No. A-130 states that agencies must apply these NIST standards and guidelines. Appendix I of OMB Circular A-130 also outlines the responsibilities for protecting and managing federal information resources. Additionally, GAO is required by the Federal Managers' Financial Integrity Act of 1982 to prescribe standards for executive agency internal controls. These standards establish the overall framework for establishing and maintaining an effective internal control system that provides reasonable assurance that the objectives (operations, reporting, and compliance) of an entity will be achieved.<sup>81</sup>

**Other Guidance.** Other guidance that may affect the implementation of blockchain include Executive Orders and OMB Memorandums. For instance, Executive Order 14028, *Improving the Nation's Cybersecurity*,<sup>82</sup> and OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*,<sup>83</sup> discuss the enhancement of cybersecurity through a variety of initiatives related to the security of federal technology infrastructure, in addition to requirements for agencies to meet specific cybersecurity standards. This guidance, in addition to laws and implementing guidance listed above, provides new and higher standards for security across the government for consistent protections and monitoring.

## OMB Guidance

OMB guidance, published in Circulars and other documents, provides instructions and information for use by executive branch agencies, both implementing legal requirements and conveying executive branch policies. Some of these instructions provide direction for the performance of oversight by managers. Auditors may need to be able to provide assurance over agency management's compliance with these instructions. A read-only node may prove impactful when auditors perform this type of work.

For example, OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," directs agency managers to continuously monitor, assess, and improve the effectiveness of internal control. Further, in the case of the grants financial

---

<sup>80</sup>The standards and guidelines found in NIST SP 800-53 do not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems.

<sup>81</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014), contains the internal control standards that executive agencies are to follow in establishing and maintaining systems of internal control as required by 31 U.S.C. § 3512 (c), (d) (commonly referred to as the Federal Managers' Financial Integrity Act).

<sup>82</sup>Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021.

<sup>83</sup>OMB, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

management process, the Circular discusses the importance of internal control over federal grant dollars. Leveraging a risk-based perspective, the internal controls framework in the circular is meant to ensure the effective and efficient allocation and use of federal grant dollars. A read-only node could provide more insight for auditors into how management is executing these requirements, especially as it relates to grants through its independent vantage point.

Circular No. A-123 also describes agency requirements for enterprise risk management (ERM). The circular states that, from an ERM perspective, an agency's interdependencies with other agencies are referred to as an "extended enterprise," which affects the agency's risk management. As discussed previously, this extended enterprise, such as in the case of an interagency blockchain, would give rise to certain additional risks that agencies would need to consider. This is also true in the case of grant payments, for which Circular No. A-123 prescribes ERM and the use of data analytics. This applies to (1) pre-grant award decision support, (2) pre- and post-grant award monitoring plans and activities, (3) award grantee risk mitigation, and (4) grant policy monitoring standards. A read-only node could give auditors insight into how all of this is being performed by agency management on a blockchain. Finally, as explained in Circular No. A-123's Appendix A, agencies are required to consider controls over reporting in their annual assurance statements. In addition, if agencies are required to submit spending data to USA Spending.gov, they must establish a Data Quality Plan that considers the incremental risks to data quality. Read-only nodes could allow auditors to verify agency management's Circular No. A-123 risk management and monitoring processes, as well as how agency management ensures data quality on a blockchain.

In addition, other OMB guidance may create considerations for auditors in using read-only nodes to assess management compliance. For example, OMB Circular No. A-50, Audit Follow-up, states that audit follow-up is an integral part of management and is a shared responsibility of agency management and auditors. In the case of audits resulting in findings and recommendations for an agency related to a blockchain or financial management processes executed on a blockchain, a read-only node could allow auditors, such as from inspector general offices, to more efficiently verify or assess agency management's corrective actions taken in response to those findings and recommendations, if needed. These auditors may have unique efficiencies when following-up on findings and recommendations as compared to other auditors following-up on similar findings for other, non-blockchain information systems.

As another example, in OMB Circular No. A-130, Managing Information as a Strategic Resource, OMB requires agencies to collect or create

information in a way that supports downstream interoperability among information systems and streamlines dissemination to the public. Circular No. A-130 also requires that agencies ensure the ability to access, retrieve, and manage records throughout their life cycle regardless of the form or medium. As blockchain use increases across federal agencies, auditors could use read-only nodes to ensure agency management is complying with these and other Circular No. A-130 requirements for data. For example, auditors may need to ensure that configuration management is operating effectively across blockchain components. In the case of grant payments on a blockchain, OMB's implementing guidance for the Single Audit Act provides requirements for auditing recipients of federal grant dollars, which may be relevant to read-only nodes. In total, OMB circulars provide requirements of agency management and auditors. Auditors having access to read-only nodes could affect how auditors verify the fulfillment of these requirements.



---

## Appendix IV: Abbreviations

API	Application Programming Interface
ATO	Authority-to-operate
CPAG	Cybersecurity Program Audit Guide
ERM	Enterprise Risk Management
FAM	GAO/Council of the Inspectors General on Integrity and Efficiency Financial Audit Manual
FedRAMP	Federal Risk and Authorization Management Program
FFMIA	Federal Financial Management Improvement Act of 1996
Fiscal Service	Department of the Treasury's Bureau of the Fiscal Service
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FTT	Fiscal Service's Office of Financial Innovation and Transformation
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GDP	Gross Domestic Product
IT	Information Technology
JFMIP	Joint Financial Management Improvement Program
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
UI	User Interface

---

## Appendix V: Glossary

Authority-to-Operate	The formal authorization for an information technology system within federal agencies, granted by the designated authorizing official, such as the Chief Information Security Officer. This involves assessing security controls, evaluating risks, and ensuring secure and approved operations.
Back end of the System	The back end typically includes scripts to support the front end appearance and back end functionality; databases to store data; and web services to present the application to users and connect the user's front end experience with the back end tasks.
Block	A collection of data in a blockchain that includes transactions and a unique identifier called a hash. It serves as a building block for the blockchain, adding new data as each block is created and linked to the previous ones.
Blockchain	A blockchain is a decentralized digital ledger that uses cryptography— such as encrypting the data—to enhance the security and permanence of transactions.
Blockchain Logic	The "logic" of a blockchain refers to the rules and algorithms that govern how the blockchain operates and processes transactions.
Chain	Chains are used to connect blocks of data, providing a secure and tamper-resistant record of transactions, similar to a pearl necklace that cannot be altered without breaking the string.
Consensus Mechanism	Consensus mechanism is a way for a blockchain to verify that a transaction is valid by having many computers on the network to agree that is genuine and reliable before it is considered valid.
Consortium	A committed group or consortium on a permissioned blockchain refers to the approved users who establish the rules and manage participation in the privately operated network.
Cryptography	Cryptography is the practice of using codes and special methods to secure and protect information so only the intended people can understand it.
Cryptographic Signature	A cryptographic signature refers to a method of using mathematical algorithms
Drawdown	The amount drawn down from a funding source.
Front End	The front end has the user interface (UI). It is the location of user interaction, business logic, and UI design.
Hash Digest	A hash digest is like a digital fingerprint that uniquely identifies a block of data on a blockchain. It makes it hard for someone to tamper with the data because any change would alter the fingerprint and be easy to spot.
Immutable	Immutable is the property of not being subject to change. In the context of data, it refers to data that can only be written, not modified or deleted.

Key Rotation	Preemptively changing or replacing a key with a new key, and making corresponding updates to the places in which the key is used.
Layer	In the context of blockchain architecture, a layer refers to a building block or level that plays a specific role in making the blockchain work smoothly. Each layer has its own function and works together with other layers to ensure the blockchain functions properly.
Minimally Viable Product	The simplest version of a product that can be released and generate positive financial returns.
Node	Blockchain nodes consist of individuals systems—computers or servers—in the peer-to-peer blockchain network that are operated by a single person, group, business, or organization.
Non-fungible token	A non-fungible token is a digital identifier, similar to a certificate of ownership, that represents a digital or physical asset. In general, a non-fungible asset is unique and not interchangeable with others.
Non-repudiation	Non-repudiation in blockchain refers to the ability to prove the authenticity and integrity of transactions. It ensures that once a transaction is recorded on the blockchain, it cannot be denied or disputed by the sender, providing strong evidence of its origin and accuracy
Off-chain Database	An off-chain database is a separate storage system used in blockchain applications. It securely stores sensitive information such as access credentials, roles and responsibilities, and grant details. The lead agency maintains and manages this database to ensure data integrity and confidentiality.
Peer-to-peer Transfer	A peer-to-peer transfer is a direct transfer of assets, such as money or digital assets, between two persons or companies that does not require the use of middlemen such as banks or financial organizations
Permissioned Blockchain	A type of blockchain where the nodes on the network are authorized by, and known to, the network.
Permissionless Blockchain	A form of blockchain where any node is allowed to participate in verifying and validating transactions.
Proof of Authority	A consensus algorithm where a limited group of trusted nodes validate transactions on a blockchain network.
Proof of Stake	A consensus algorithm for ensuring new transactions on a blockchain are verified by only allowing nodes to add new transactions in proportion to how much they have previously invested or “staked” into the blockchain.
Proof of Work	A consensus algorithm for ensuring new transactions on a blockchain are verified by requiring large amounts of computing power and energy to generate a new transaction on the blockchain.
Read-only Node	A read-only node can observe and independently verify transactions on the blockchain but does not contribute to consensus.

Sandbox	A sandbox is a controlled testing environment that enables safe experimentation, validation, and development of the blockchain system. It allows for testing alternative scenarios, interoperability with other systems, and ongoing evaluations without impacting the live environment.
Scalability	The ability to expand the network or add more users to the blockchain.
Secure Key Storage	Various methods of protecting cryptographic keys and preventing unauthorized parties from gaining access to the keys and resulting information. Storage protects the key while keeping it readily available for use.
Smart Contracts	Software code stored on a blockchain that contains a set of conditions, so that transactions automatically trigger when the conditions are met.
Smart Contract Logic	The business logic that distributes the parameters of the smart contract.
Solidity	Solidity is a special programming language used for creating smart contracts on the blockchain. It is unique because it enables developers to write rules and conditions directly into the contracts, ensuring that transactions are secure, reliable, and trustworthy. It has mechanisms to catch errors early in the development process to ensure greater program reliability.
Standardized Method	A standardized method consists of a predefined set of rules and procedures that have been agreed upon by network participants. These rules ensure that transactions are processed consistently and predictably, with all network entities adhering to the same guidelines.
Tamper-resistant Ledger	A tamper-resistant ledger ensures that once data is recorded on the blockchain, it cannot be altered or manipulated without detection, providing a secure and trustworthy record of transactions and information.
Token	Tokens are digital assets on the blockchain. The process of adding new digital assets to a blockchain is called tokenization.
Traditional database	A centralized system that stores financial data in a structured format. Access to this data is controlled by a central authority and updates are processed by the same authority.
Vendor-lock-in	Vendor-lock-in refers to being dependent on a specific company's products or services, making it difficult to switch to alternatives.
Wallet	A contactless payment application that can store forms of payment, identification cards, non-fungible tokens, and more.

---

## Appendix VI: Contacts and Acknowledgments

<b>Contacts</b>	<p>Amanda Kupfner, Chief Strategy Integration Officer, Fiscal Service, (304) 480-6571 or <a href="mailto:Amanda.Kupfner@fiscal.treasury.gov">Amanda.Kupfner@fiscal.treasury.gov</a></p> <p>Taka Ariga, Chief Data Scientist, GAO, (202) 512-6888 or <a href="mailto:ArigaT@gao.gov">ArigaT@gao.gov</a></p> <p>Dawn Simpson, Director, GAO, (202) 512-3406 or <a href="mailto:SimpsonDB@gao.gov">SimpsonDB@gao.gov</a></p> <p>Katie Malague, Chief Management Officer, OPM, <a href="mailto:Katie.Malague@opm.gov">Katie.Malague@opm.gov</a></p> <p>Federal Financial Assistance Mailbox, OMB, <a href="mailto:MBX.OMB.Grants@omb.eop.gov">MBX.OMB.Grants@omb.eop.gov</a></p>
<b>Acknowledgments</b>	<p>In addition to the contacts named above, the following individuals made key contributions to this publication.</p> <p><b>Department of the Treasury:</b> Adam Goldberg, Cindy Good, Bernadette Goodwin, Tammie Johnson, and Mike Moore</p> <p><b>Government Accountability Office:</b> Mark Canter, Robert Dacey, Jennifer Franks, Ram Gollakota, Joanne Howard, Jason Kirwan, Olivia Kleiner, Robert Mabasa, Matthew Minter, Amy Pereira, Joseph Rando, Aaron Ruiz, Sandy Silzer, and Martin Skorczynski</p> <p><b>Office of Personnel Management:</b> David Edward Jones</p> <p><b>Office of Management and Budget:</b> Stephanie Teller-Parikh</p> <p>-----</p> <p>Also contributing to this publication were Andrew Kurtzman (GAO), Dara Higgs (GAO), Gerald Morris (Treasury), Ralph Jones (Treasury), and Lisa Taylor (GAO).</p>
<b>Special Thank You</b>	<p>The JFMIP would also like to extend a special thank you to the following organizations, whose time and expertise provided the JFMIP with key information during this initiative: United States Postal Service-Office of Inspector General, National Science Foundation, Department of Homeland Security, Department of Health and Human Services, Executive Office of the President-Office of Science and Technology Policy, Deloitte, Ernst &amp; Young, Grant Thornton, KPMG, and The MITRE Corporation.</p>