ASSESSMENT AND AUTHORIZATION OF BLOCKCHAIN SYSTEMS

Government Blockchain Association
Cyber Security Working Group

Executive Summary

Blockchain technology continues to gain attention and generate excitement throughout industry and Government. This emerging technology has the potential to disrupt current business practices, by streamlining many government business processes and instituting trust within the process itself, but with this change comes risk. Security is a major concern for both Government and Government partners. The goal of this paper is to provide insight and considerations to promote and inspire discussion regarding the process of assessment and authorization of blockchain systems for use in Government, how it aligns with the current FISMA requirements and NIST frameworks and how it can address blockchain systems and applications.

CONTENTS

Executive Summary....1
Introduction....4
Blockchain Programs in the Federal Government....4
The Assessment and Authorization Challenge....4
Types of Blockchains....5
Background....6
Risk Management Framework (RMF) Overview....7
Risk-Based Approach....7
Blockchain – Considerations for Assessment and Authorization....8
RMF Control Families....8
Access Control (AC)....8
Awareness and Training (AT)....9
Audit and Accountability (AU)....9
Security Assessment and Authorization (CA)....10
Configuration Management (CM)....10
Contingency Planning (CP)....11
Identification and Authentication (IA)....12
Incident Response (IR)....12
Maintenance (MA)....13
Media Protection (MP)....13
Physical and Environmental Protection (PE)....13
Planning (PL)....14
Personnel Security (PS)....14
Risk Assessment (RA)....14
System and Services Acquisition (SA)....15
System and Communications Protection (SC)....16
System and Information Integrity (SI)....16

Conclusion and Future Considerations 17
A&A Application of the Blockchain 17
Contributors 18

Introduction

Blockchain technology is gaining attention in government because of the potential to streamline business process and improve their efficiency and efficacy. Federal programs such as General Services Administration (GSA) FASt Lane, the Office of Personnel Management (OPM) Employee Data Record (EDR), and agencies such as Centers for Disease Control and Prevention (CDC), Food and Drug Administration (FDA), and United States Agency for International Development (USAID) have started exploring the technology and have implemented pilot programs.

Blockchain Programs in the Federal Government

The General Services Administration, Emerging Citizen Technology Office maintains a quick reference list of current programs, initiatives, pilots, events, RFIs, and other blockchain efforts in progress on GitHub at https://emerging.digital.gov/blockchain-programs/. The list continues to grow as new programs kick off.

GSA's Emerging Citizen Technology program launched the government-wide Blockchain initiative, including both an internal federal community of more than 200 managers and a public-facing listserv of more than 100 U.S. businesses, researchers, subject matter experts and more. For ideas and concepts on using blockchain in Government, see the U.S. Federal Blockchain Forum, the "Emerging Tech and Open Data for a More Open Government," a workshop to draft the first potential national goals for Blockchain through Open Government, and the U.S. Emerging Citizen Technology Atlas.

The Assessment and Authorization Challenge

While blockchain technology provides an opportunity for innovative solutions throughout government, for a blockchain solution to be used in a production environment and handle real data and customers, it must meet stringent federal security requirements under the Federal Information Security Management Act (FISMA). Federal information systems must go through a complete Security Authorization (SA) process before being granted an Authorization to Operate (ATO), and blockchain systems are no exception.

The security authorization process uses the guidelines for Risk Management Framework (RMF) defined in NIST Special Publication (SP) 800-37. The RMF includes security categorization, security control selection and implementation, security control assessment[i], information system authorization, and security control monitoring.

Blockchain systems present unique challenges to the security authorization process due to their distributed, peer to peer (P2P), and sometimes permissionless design. The type of blockchain - Permissioned vs Permissionless and Public vs Private - are major considerations in the design, implementation, and assessment of a blockchain system (see the table below). Assessment concepts surrounding each type of blockchain will be discussed in the following sections.

Types of Blockchains

	Permisionless (no restrictions on processors)	**Permissioned** (defined rules for access)
Public (no restrictions on reading blockchain data)	Every user can read transaction data. Every user can validate transactions in blocks *e.g., Bitcoin & Ethereum*	Every user can read transaction data. Only predefined users can validate transactions. *e.g., Hyperledger Fabric*
Private (direct access to data is limited to defined users)	Only predefined users can see the data. Every predefined user can validate transactions. *e.g., Private deployment of Ethereum*	Only predefined users can see the data. Only a smaller subset of these users can validate transactions. *e.g., Hyperledger Fabric*

Despite these unique considerations, blockchain technology is capable of fitting within the RMF assessment process and successfully being granted an ATO.

At present, there is little guidance on how to apply RMF security principles to blockchain systems. Based on RMF control families, this document presents a high-level overview of considerations when deciding whether to use blockchain technology in an information system that will process, store and/or transmit federal data, or when taking a blockchain solution through the RMF process.

Blockchain technology and the RMF are both complex topics, and there are many ways to implement each – there's no way an introductory document can address all aspects of blockchain assessment and authorization (A&A). This document provides a starting point to stimulate consideration and discussion about blockchain and A&A.

Background

United States Government (USG) Federal Information Systems require A&A before becoming operational. The USG has converged on the Risk Management Framework guidelines outlined in NIST 800-37 as the common underlying A&A approach for USG systems; many commercial entities are also using the RMF as a template for their own certification activities.

Blockchain technology provides a new tool to address challenges in many application domains. Blockchain technology is not security "magic" – blockchains are built on software, which will always have implementation flaws, and run on operating systems with flaws, some of which may be exploitable.

The notion of a "trustless" blockchain depends on the architecture and implementation details. For many practical applications, there will be a trust agent; in a permissioned blockchain, somebody is responsible for managing the users who are granted access and roles. In all blockchain applications, there is underlying trust that the identity of an agent is not compromised – if an adversary gets your credentials, their illegitimate activity is not easily distinguishable from your actions.

Blockchain solutions are by nature distributed, and can be decentralized, which presents interesting A&A challenges, such as:

- *Who "owns" the blockchain?*
- *Who is responsible for the overall security of the blockchain system or application?*
- *Who is responsible for determining whether a node is permitted to join the blockchain?*
- *Who is responsible for monitoring activity to ensure ongoing compliance?*
- *Who has the authority to authorize a blockchain solution?*
- *How do you assess "smart contracts" before they're put on the blockchain?*
- *Who is responsible for managing consensus mechanisms?*

This paper will address some of these challenges and presents a high-level approach to A&A of blockchain solutions.

Effective A&A requires understanding the risks associated with a solution and weighing this risk against the operational benefit of deploying the system or application. The A&A process includes documenting the operating configuration of the system and any risk mitigations that are in place and monitoring the system to ensure it is compliant with the A&A configuration. No system is perfect, but the more insight responsible parties have into the system and the associated risks and mitigations, the more informed the decision they can make about authorizing the solution for operational use.

Risk Management Framework (RMF) Overview[ii]

The selection and specification of security controls for a system is accomplished as part of an organization-wide information security program that involves the management of organizational risk - that is, the risk to the organization or to individuals associated with the operation of a system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for a system - the security controls necessary to protect individuals and the operations and assets of the organization.

Risk-Based Approach

The Risk Management Framework provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. The following activities related to managing organizational risk are paramount to an effective information security program and can be applied to both new and legacy systems within the context of the system development life cycle and the Federal Enterprise Architecture:

Blockchain – Considerations for Assessment and Authorization

When considering A&A of a blockchain solution, it is helpful to consider the elements that make up the system. Blockchain technology is just software running on computers – the innovation is in how distributed ledger technologies (DLT) and cryptography can be utilized to provide data integrity, availability, and resiliency. The following sections list the RMF control families and highlight topics that may present unique challenges when assessing blockchain systems.

Before starting A&A on a blockchain system it is very important to clearly analyze and define its boundary. This can be challenging due to the possibility of a node existing on a variety of different platforms and infrastructure within an organization. Considerations for this topic will be covered in the Risk Assessment Family below.

RMF Control Families

The following sections address the RMF control families documented in NIST SP 800-53 revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST 800-53). While there are many controls within each family, this paper provides some points worth considering for each family specific to a blockchain system. For the blockchain system to be approved for operation, the System Security Plan (SSP) must describe how the system implementation addresses each applicable control.

Access Control (AC)

The Access Control family addresses who, when, and what can access a system; how they can access it; and what they are permitted to do on the system. In a blockchain system, this will include logical access to the nodes that are part of a blockchain infrastructure, and to endpoints used to interact with the blockchain. The specifics vary depending on the technology used to implement the system.

- Is the implementation permissioned or permissionless?
- How do you determine who can deploy a node and attach it to the network?
- How is a blockchain network or application accessed? Is it through a web application? Is access limited from an application?
- Once you are an authorized user within an organization and granted access to network resources is there a need for an additional layer of permission on the blockchain?

- Where is it appropriate to implement User Access Control vs Network Access Control?
- What policies exist for adding, removing, and monitoring participants? Devices and Network Components?
- What mechanisms are in place to implement least privilege through granular User/Data Access Control?
- Will data be stored directly on the blockchain? Consider data sensitivity and access by users and nodes.
- How are external data sources ("blockchain oracles") and access to them from the blockchain protected?
- How are the access logs generated? Do system administrators have access to those, particularly for permissionless systems?

Awareness and Training (AT)

Security training is critical for any user. While there are some security capabilities inherent in blockchain technologies, it is important to have a training plan to ensure users understand what they are permitted to do with the system. A training plan likely exists for most operational information processing environments; while users may not know that they are using a system that runs on the blockchain, the security training plan may need to be updated to include unique aspects of the blockchain implementation.

- Is there any training in place to educate system owners and users on blockchain?
- Does existing training need to be updated to emphasize potential risks introduced by a blockchain implementation (e.g., consequences of compromised credentials)?

Audit and Accountability (AU)

Blockchain is unique in that its purpose is to audit activity and record it in a manner that cannot be modified and is made available in a highly resilient environment to those authorized to see it. However, blockchain code is often distributed amongst many machines, each of which will have auditing requirements that must be met. The environment must support audit aggregation as per the requirements of the Authorizing Official (AO). Since blockchain solutions may include multiple organizations, it may not be possible to merge auditing from all entities comprising the blockchain.

- How will transactions be audited on the blockchain? A dedicated block explorer? Who will have access?
- Will the use of Blockchain applications be audited? If so, what operations? Only when data is written to the blockchain? When data is read?
- Will a blockchain be used to store audit records? Login/Logoff? Other organizational data?

- How do data retention/archiving policies apply? Will blockchain records be archived?
- Do you need off-chain centralized auditing of more specific data?
- How do you determine the severity of events?
- Who owns the auditing responsibility? Is it shared among the participants?
- How are the access logs generated? Do system administrators have access to those, particularly for permissionless systems?

Security Assessment and Authorization (CA)

If the blockchain solution is being deployed in a system that already has an ATO, the SSP will have to be updated to reflect the additional devices, services, and capabilities the blockchain introduces.

If an organization is standing up their own blockchain instance, they will need to satisfy their organizational A&A requirements. If blockchain is provided as a service, the service provider must specify requirements for entities that wish to use the service.

Blockchain implementations may cross A&A boundaries; in such cases, coordination between AOs will be critical to getting ATO for the complete system.

- Will the blockchain system connect to other applications? Will there be off-chain storage?
- How is the system boundary defined? Does the notion of the system boundary itself need to be updated to account for the distributed nature of the system?
- What external systems are permitted to connect to the system? What are the security requirements for those systems?
- How will the system be continuously monitored for security vulnerabilities after authorization?
- How will security assessments of the blockchain solution be performed?
- Is there a single owner of the A&A?
- Who will be the AO for the system?
- Are the system risks shared among the participants of the network?

Configuration Management (CM)

Configuration management is critical for all systems, but for a system that requires an ATO, changes to the system configuration must be considered within the context of the approval. The approved configuration must be documented, and any security-relevant changes to the implementation must be approved by the AO. Due to the immutable nature of the

blockchain, it can be complicated to correct errors, so changes must be thoroughly scrutinized before being deployed.

- How will you manage changes to the system?
- If you must make critical changes, what are the circumstances that must be met to approve a fork in the code?
- Who has authority to make changes?
- How will you coordinate blockchain application changes with infrastructure requirements?
- If you use smart contracts, what is the procedure to change a contract?
- How will you migrate data from an old smart contract to a new smart contract?
- How do you assess risks when changing or upgrading smart contracts?
- How will you implement an effective test network?
- How do you create Dev/Test/Production blockchain environments with strict procedures in place for transition?
- What are the policies around 'roles' of participating nodes? What is the consensus mechanism? How many validating nodes are there? Which nodes allow data to be written into the blockchain?
- Are there on-ramp and off-ramping procedures for nodes on the network?

Contingency Planning (CP)

The distributed nature of the blockchain can enhance solution resiliency, but it is still important to architect the solution to mitigate risk associated with loss of power, communications, facilities, personnel, etc. The specific blockchain implementation determines the approach to contingency planning. Contingency planning for a solution that replicates the entire blockchain on every node will be different from one that has specific nodes authorized for consensus approval.

- How many nodes will be running?
- What is the minimum number of nodes that need to be operational to maintain the consensus mechanism and system integrity?
- Are the nodes geographically distributed?
- Can all the nodes be turned off? Which events will require nodes to be turned off?
- Is there any backup off-chain storage in case of a full system failure?
- Which data is deemed necessary to maintain integrity and consistency of data on the blockchain and does it need to be recoverable?
- How is the IT Service Management (ITSM) of the system managed? Is it a shared responsibility?

Identification and Authentication (IA)

For the blockchain to serve as a trustworthy system of record, there needs to be a way to ensure that transactions recorded to the blockchain are performed by an authorized user or node. Effective access control depends on reliable identification and authentication of a user or node.

For permissionless blockchains, IA is managed by the individual users; the user may be pseudonymous to the blockchain. If a user loses control of their authentication credentials, a bad actor who has those credentials can execute transactions on the user's behalf, and it is difficult to prove that the transaction is not legitimate, since there may be no direct association between the credentials and the actual user.

For permissioned blockchains, the solution should include robust identification and authentication, both to limit the activity of the user to authorized actions, and to provide some attestation that the identified user performed an action.

- How are keys generated and managed for each user? Centrally? By each user?
- Are user keys tied to a person's identity? Is there some type of Know Your Customer (KYC) for the blockchain solution? Is it necessary?
- Are there requirements to be compliant with NIST SP 800-63 Digital Identity Guidelines?
- Will you require multi-factor authentication for logins?
- How do you ensure unique identification of users/nodes/devices/groups/etc.?

Incident Response (IR)

Incident response requires defining what constitutes an incident, and the potential consequences of that incident. To respond to an incident, you must first detect it. In addition to the incident detection capabilities deployed on individual platforms, there may be a way to identify incidents on the blockchain itself. A blockchain incident could include a malicious actor gaining control of the network or someone attempting to tamper with a block.

The distributed nature of a blockchain can improve resilience, so incident recovery may mean blocking access to a specific node or standing up new instances of a replacement node. As with any incident response plan, details about any incident will inform corrective action to mitigate the risk of a repeated incident.

- What is the incident response process if the blockchain and/or smart contract is compromised?
- Is there a group of people that decide on changes to the system? Hard-fork? Soft-fork?

- Who has the capability to revert transactions?
- How are incidents detected? Who has the authority to declare an incident?
- What process will be involved in resolving the incident? Does resolution require standing up new instances or blocking a node?
- What escalation procedures are in place among network participants?

Maintenance (MA)

The blockchain is implemented on information processing systems, each of which will require maintenance.

- Will the blockchain itself require any special considerations for maintenance?

Media Protection (MP)

While there will likely be no special considerations for media protection with respect to the blockchain, media protection requirements will apply to the machines comprising the blockchain implementation.

- What are the risks presented to the blockchain by media used in participating machines?

Physical and Environmental Protection (PE)

Information Systems implementing the blockchain will need to be protected as per the requirements of the most sensitive information deployed on the blockchain. It is up to the AO to determine the relevance of physical and environmental protection of any node that wishes to access the blockchain. The redundant and distributed nature of many blockchain architectures will improve the resiliency of the overall solution, but each information system connected to the blockchain must be considered as to its importance in keeping the blockchain functioning properly and protecting loss of information if a node is compromised.

- Are there any changes in physical and environmental protection required for a node to be permitted to join the blockchain? Has the risk posture changed?
- What PE controls are relevant for organizational nodes versus external nodes?
- Are there minimum PE controls for spinning up a node?

Planning (PL)

The security concept of operations (SCoO) and SSP must take the blockchain architecture and use into consideration. If systems from multiple security enclaves connect to the blockchain, each of those enclaves must update their SSP for any node in their enclave.

In addition to the individual SSPs and SCoOs, it may be necessary to have an overarching SCoO for the blockchain system implementation addressing proper use and defining requirements for accessing and limits on what can be placed on the blockchain. For example, if a blockchain is to have no data above Secret stored on it, users must know to not put Top Secret information on the blockchain, and there should be no access to the blockchain from any system that shouldn't have access to Secret information.

Need-to-know is another consideration for blockchain. One of the benefits of the blockchain is having data widely available; in many applications, that data should be widely available, but only to authorized users. Classification guidance must apply to the entire blockchain, which implies centralized authority, even if the implementation supports a distributed technical solution.

- What changes need to be made to the SSP and SCoO to support the blockchain implementation?
- Is there a requirement for an overarching SSP or SCoO?
- Is there classification guidance required to manage access to information?

Personnel Security (PS)

Typical personnel security requirements apply to blockchain administrators and users. It will be necessary to consider personnel authorizations before granting access to the blockchain, just as for any other system. That access will need to be coordinated across all users of the blockchain.

- Is there a clearance level associated with access to information on the blockchain?
- What authorizations must a user have to be permitted to access the blockchain?

Risk Assessment (RA)

The security categorization and risk assessment are dependent on what the information systems connect to, what data they are handling, and who has access to them. As with any solution, the blockchain architecture and implementation approach must consider these aspects across the entire solution. Security considerations may limit the viability of a

blockchain for a solution – this needs to be considered before committing to a blockchain implementation.

- What kind of data will be stored on the blockchain? Is it sensitive?
- Will off-chain storage be implemented for sensitive data?
- How will various parts of the system be assessed? Blockchain infrastructure, Blockchain applications/smart contracts, web applications?
- How will vulnerability scanning of the node hosts be conducted?
- Will there be an approved operating system build of a node?
- Are there any privileged keys? What happens when they are lost, stolen, or compromised?
- How do you discern risks to the network versus the blockchain itself?
- How do you ensure the scope and system boundary of the blockchain system is well defined?
- Does any of the solution reside on an already FedRAMP-approved environment?
    - If so, how does it affect the system boundary of the blockchain system and what are the corresponding risks?
- Are there different risks and questions about ownership for every participating node of the network?
- Do you need to differentiate between the node and the underlying infrastructure and their risks?
- If your system is categorized Low, do you need the availability and integrity of a blockchain system?

System and Services Acquisition (SA)

System and services acquisition for a blockchain solution is much like for other systems. Some of the technology introduced by blockchain will be new to acquisition personnel, so education of security implications will be an important part of any blockchain initiative. As emphasized throughout this paper, good security practices will need to be applied to all components of the blockchain solution, from architecture and design through individual component selection and implementation. Secure development practices for foundational technology and targeted technology (such as smart contracts) are an important consideration for understanding the risk associated with the composed solution.

- What processes are in place to ensure the security of a blockchain system before acquisition?
- What information do you need to provide in a blockchain solution acquisition package to limit confusion? What new controls specifically for blockchain systems may be needed?
- What blockchain education may be required for acquisition staff, if any?

System and Communications Protection (SC)

Blockchain is a distributed system; apart from best practices to protect the systems and communications links, the sensitivity of data stored on the blockchain may drive encryption and access requirements.

- Will blockchain nodes reside on encrypted storage? Is this necessary?
- Will users need to tunnel P2P blockchain traffic through a VPN?
- Should everyone be allowed to see all the data on the blockchain?
- Will there be a separate blockchain node enclave? A firewalled environment?

System and Information Integrity (SI)

Blockchain technology inherently provides data integrity through its consensus mechanisms and cryptography. However, end-users could still commit invalid information to the system, either through lost/stolen keys or user error. That information could then be committed to the chain and mistaken as valid. Therefore, one should consider how to mitigate such cases to ensure the integrity of the data being put into the system.

- How do you detect data corruption on the blockchain?
- How do you correct data corruption on the blockchain?
- How do you ensure the consensus mechanism is working properly?

Conclusion and Future Considerations

In this paper we posit that a blockchain system can be evaluated through a standard A&A process, though there are concepts that are unique to blockchain that should be considered throughout the RMF process. There are many details to be explored for a blockchain A&A process that can be explored in future papers; here are some potential topics:

- Develop an initial set of baseline security controls for a blockchain system based on the security categorization and tailoring and supplementing the security control baseline as needed.
- Develop guidance on how to implement the security controls and describe how the controls are employed within the blockchain system and its environment of operation.
- Develop assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Define procedures to authorize a blockchain system operation based on a determination of the risk to the data.
- Describe tools, techniques and procedures to monitor the security controls in the information system on an ongoing basis.

A&A Application of the Blockchain

Turning around the basic concept of this paper, blockchain technology could be used to facilitate the A&A process. Blockchain technology provides auditability and immutability, which are key facets of the RMF process. Therefore, it is possible that a blockchain-based system can be the parent system of these features within an organization. This is a topic that can be explored in future papers.

Contributors

Special thanks to those that have contributed to this white paper:

Ajay Chandhok
GBA Cyber Security Working Group Lead
CEO Stratus Cyber

Art Wilson
GBA Member
Tresys Technology

Venkat Kodumudi
GBA Member

Sandy Barsky
GBA Member

Christina McGhee
GBA Member

Jitendra W. Chandhna
GBA Member

GBA Product Owner:
Robert Perry
GBA Director, PMO

If you are interested in working on creating this security authorization process for blockchain systems, please contact Ajay Chandhok or join our Cyber Security Working Group listed on the GBA Working Group site at: https://gbaglobal.org/working-groups.

[i] **Security Control Assessment** - Assess the security controls following the SAP and using the NIST 800-53 Rev 4 Test Cases to determine if the controls implemented in RMF are operating as intended and producing the desired outcome with respect to meeting the security requirements for the information system.

[ii] This RMF Overview is taken from the NIST RMF page: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview