Implications of the Use of Blockchain in SOC for Service Organization Examinations
Contents

2 Introduction

5 Objectives and Organization of this Document

6 Overview of Blockchain
   6 Classification of Different Types of Blockchains
   7 Unique Features of Blockchain
      7 Access Control Mechanisms
      7 Consensus Mechanisms
   8 Data Integrity
   8 Smart Contracts
   8 Internet of Things (IoT)
   8 Oracles
   10 Risks Associated with a Service Organization’s Use of Blockchain

14 Implications of a Service Organization’s Use of Blockchain in SOC for Service Organization Examinations
   14 Overview of Professional Standards and Criteria Governing SOC for Service Organization Examinations
   15 Determining Whether the Engagement Team Possesses the Appropriate Competence and Capabilities
   16 Obtaining an Understanding of the System
   19 Additional Considerations When Smart Contracts are Used in the Blockchain
   19 Forming an Opinion on the Description of the System, the Suitability of the Design of the Controls, and in a Type 2 Examination, the Operating Effectiveness of the Controls

20 Summary

21 Appendix A
   21 Examples of Service Organizations’ Use of Blockchain
      21 Example #1: Payroll Processing
      21 Example #2: Employee Benefit Plan Recordkeeping
      22 Example #3: Broker-dealer Blockchain Consortium
      22 Example #4: Commercial Real Estate Management Services

23 Appendix B
   23 Additional AICPA Resources
Introduction

The term blockchain\(^1\) refers to a growing list of digital records of transactions organized into blocks that are linked together by cryptography. Each block contains a cryptographic\(^2\) hash of the previous block and other information that permits users of the blockchain to easily detect tampering with any previous block. A blockchain distributed ledger shares transactions across a peer-to-peer network, thereby enabling participants (entities, companies, organizations, or individuals), to read or write records, and to confirm transactions without the need for a central clearing authority.

Blockchain networks have many unique features that make them different from other technologies that a service organization may use in its systems. Although individual features vary depending on the type of blockchain network, they generally

- enable data, information, or content to be structured so that it is secure, verifiable, current, reliable, and accurate;
- reduce the risk of unauthorized changes or destruction through the use of applied cryptographic functions;
- enable records of transactions to be accessible to participants and available on demand;
- allow participants to update and record transaction data in a linear and chronological order to provide a record of transactions and an audit trail; and
- eliminate the need for a third party to maintain the data.

Because of these and other features discussed in the Unique Features of Blockchain section of this document, the use of blockchain may provide opportunities for service organizations to provide new services (for example, developing new systems to support supply chain efficiency) and to reduce the costs of providing existing services to user entities (for example, by eliminating the time spent on reconciliations; researching and resolving differences between separate ledgers maintained by parties to transactions; reducing the risk of unauthorized changes to business records; and reducing the risk that business records are not available when needed).

---

1 The term blockchain is often used synonymously with the term distributed ledger; however, not every distributed ledger is a blockchain. This document focuses only on a blockchain distributed ledger, not on distributed ledgers in general.
2 In this document, terms are italicized on first use and defined in the Blockchain Universal Glossary developed as a reference for all Association content related to blockchain and digital assets.
The opportunities provided by use of blockchain technologies, however, come with increased risks for service organizations and their user entities. Service organization management is responsible for identifying, assessing, documenting, and responding to those risks through the design and implementation of controls that mitigate those risks to acceptable levels.

Understanding those risks and the controls implemented by service organization management to mitigate those risks is also critical for the service auditor who performs a SOC 1® — SOC for Service Organizations: (ICFR) examination or a SOC 2® — SOC for Service Organizations: Trust Services Criteria examination (collectively referred to as SOC for service organization examinations in this document). Although this paper specifically addresses SOC 1 and 2 examinations, it may also be helpful to a practitioner who performs a SOC for Supply Chain examination. Practitioners can find guidance on performing such an examination in the AICPA Guide SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System.

Because blockchain is a relatively new technology, service auditors may have limited experience with how blockchain works. In addition, the complexity of the technology increases the competency needed to perform a SOC for service organization examination when the service organization uses blockchain. Before accepting such an engagement, the service auditor should be satisfied that the engagement team has the appropriate competence and capabilities, including a sufficient knowledge of blockchain, to perform the engagement in accordance with professional standards. If not, the service auditor may determine it is necessary to use a specialist who possesses the relevant knowledge and skills to assist in performing the engagement. The section of this document titled Determining Whether the Engagement Team Possesses the Appropriate Competence and Capabilities discusses this further.
The term blockchain refers to a growing list of digital records of transactions organized into blocks that are linked together by cryptography. Each block contains a cryptographic hash of the previous block and other information that permits users of the blockchain to easily detect tampering with any previous block.
Objectives and Organization of this Document

When blockchain is an integral part of a service organization's system or when that system interfaces with blockchain, the service auditor's understanding of the unique features of blockchain and the risks it presents to the service organization and user entities enables the service auditor to (a) identify and assess those risks and (b) design and perform procedures to obtain sufficient appropriate evidence to support the service auditor's opinion.

The objectives of this document are twofold: to educate the service auditor about some of the unique aspects of blockchain and to discuss the implications of the use of blockchain in a system used to provide services to user entities of a SOC for service organization report.

To achieve these objectives, this document is organized into two parts:

Part 1 of the document

- presents an overview of blockchain, including a discussion of the different types of blockchain networks and some of its unique features, and
- identifies specific risks of using blockchain; this document does not, however, identify specific controls a service organization may implement to address those risks, nor does it describe the procedures a service auditor might perform to obtain evidence about the suitability of design or operating effectiveness of those controls.

Part 2 of the document

- presents an overview of relevant professional standards and criteria governing SOC for service organization examinations;
- discusses the need for the engagement team to possess knowledge about blockchain and the specialized skills and competencies to perform the engagement, including the use of specialists when appropriate;
- describes the unique elements of the service auditor's understanding of a service organization's system when blockchain is integral to and interfaces with that system; and
- discusses unique considerations when forming an opinion on the description of a service organization's system that includes blockchain; the suitability of the design of the controls; and in a type 2 examination, the operating effectiveness of controls.

This document also includes the following appendices:

- Appendix A includes examples of how service organizations might use blockchain in a system used to provide services to user entities.
- Appendix B lists additional AICPA resources for service auditors who want to learn more about blockchain.

This document does not address an examination of a blockchain in accordance with the attestation standards; however, if a practitioner were engaged to provide such an examination, some of the information in this document may be helpful to the practitioner when determining how to perform the engagement in accordance with AT-C section 205, Examination Engagements.
Overview of Blockchain

A blockchain network is a digital, decentralized, and distributed ledger that can be used to record transactions across multiple devices (for example, computers, laptops, or servers), which are often referred to as nodes. If there is an attempt to retroactively alter transactions, participants are alerted and may respond accordingly (for example, by obtaining an understanding of the reasons for the proposed alterations to determine if they agree with them). Blockchain enables participants to write or read transactions to or from the ledger, and to independently validate the transactions without the need to know or trust one another. By distributing information previously held in a centralized ledger across a network of computers, blockchain may reduce the need for third-party intermediaries (for example, banks for financial transactions, clerks of courts for recording land deeds and vehicle titles, or clearing firms to settle security trades.)

Classification of Different Types of Blockchains

There are several different types of blockchain networks, including the following:

- **Permissionless public blockchain.** Enables any participant who has internet access to join the blockchain and to read, write, and send transactions. There are no permissions required for any actions that participants may take. A permissionless public blockchain distributes transactions to all full nodes.³ Permissionless public blockchains are the most prevalent type of blockchain used for buying, selling, and trading digital assets. Bitcoin, the most popular and widely held digital asset, is an example of a permissionless public blockchain. Because of some of the risks associated with permissionless public blockchains, however, they are less likely to be used for many commercial business-to-business (B2B) transactions than other types of blockchains.

- **Permissioned private blockchain.** Exist in a secured and segregated environment for a group of participants who know and trust one another. Participants’ access rights are assigned according to an agreement among the participants. Because participants are permissioned, they see only what they are permissioned to see per that agreement.

For certain permissioned private blockchains, the controller of the blockchain may designate a central authority that has the power to change the protocols.⁴ Because some of the key features of permissioned private blockchains mitigate the risks inherent in permissionless public blockchains, commercial businesses are more likely to use permissioned private blockchains for recording and processing B2B transaction.

- **Hybrid blockchain.** Uses the features of both permissionless public blockchains and permissioned private blockchains. In a hybrid blockchain, access to information recorded in the blockchain and other functionality may be restricted to specified participants, while access to other information is available to all. For example, a logistics hybrid blockchain could include both a private component (that is, information and functions that are available to only a few large suppliers who are permissioned to read, write, transact, and vote on changes to the blockchain protocols) and a public component (that is, information and functions such as transaction status queries and report generation that are available to a large number of subcontractors, customers, and smaller suppliers).

---

³ Only full nodes have a complete copy of all of the blockchain transactions; other nodes, known as lightweight nodes, download the block headers only to validate the authenticity of the transactions.

⁴ Protocols are the common communication rules that govern how a blockchain operates, including how to reverse transactions and make other decisions that may affect all participants.
Unique Features of Blockchain

Although the characteristics of a specific blockchain network may vary based on the type of blockchain, this section describes some of the unique features of blockchain technology. Blockchain is a distributed ledger, but it is distinct from other types of distributed ledgers because transactions on a blockchain are grouped together and organized chronologically in blocks of transactions. The blocks are linked to one another and secured using cryptography. A blockchain is essentially a continuous ledger of transactions. It is an append-only structure that allows data to be added to it, while significantly limiting the ability to alter or delete previously recorded transactions. Participants agree to the transactions to be added to the blockchain through the use of a consensus mechanism.

Validators collect transactions and perform cryptographic functions to verify them. Once consensus has been reached and transactions verified, the new block of transactions is added to the ledger and distributed automatically to each full node.

Access Control Mechanisms

Access control mechanisms are a means of safeguarding the security of a blockchain network and the records in it by permitting access to only authorized users (for example, persons, organizations, participants, members, devices, users, or nodes) and by preventing and detecting unauthorized access. Access control mechanisms in a blockchain include cryptographic keys, and may also include hardware or software features, operating procedures, management procedures, and various combinations of these. How access is controlled is one of the key differences between permissionless public blockchains and permissioned private blockchains.

- **Permissionless public blockchain access control mechanisms.** Anyone can join and access a permissionless public blockchain, without approval by a central authority or security administrator. The access control mechanism in a permissionless public blockchain is a wallet, which allows the participant to write new records and read all existing records created by all other participants. There are no restrictions on who can obtain a wallet.

- **Permissioned private blockchain access control mechanisms.** Access to permissioned private blockchains is configured at the network level by user access policies and access control lists and at the application level by specific permissions granted to users and resources by the blockchain’s security administrator.

Consensus Mechanisms

The integrity of records in a blockchain depends on the consensus mechanism used to validate blocks and add them to the blockchain. A consensus mechanism refers to the method used to authenticate and validate transactions; the consensus mechanism uses a consensus algorithm and protocols to define how consensus is achieved.

---

5 Algorithms are used as specifications for performing calculations to enable validators to agree on the same version of the blockchain without having to trust each other.
Consensus Mechanisms (continued)

There are various types of consensus mechanisms, all of which present different risks to the service organization and those with whom it does business. The service auditor needs to understand the type of consensus mechanism used by the service organization’s system, how it works, the related risks, and the controls the service organization has implemented to mitigate those risks.

Data Integrity

A blockchain’s consensus mechanism helps preserve the integrity of transactions recorded on the blockchain by detecting changes made to previously recorded transactions and preventing distribution of such changes to other copies of the blockchain on the network. (Usually, a previously recorded transaction cannot be changed, but in some cases, a consensus mechanism and protocols may permit a change to a previously recorded transaction when parties to a transaction or full nodes agree to the change—for example, when there is a hard fork or when the protocol permits adjusting entries)

Smart Contracts

A smart contract is a computer program that uses data in a blockchain and implements a set of rules agreed to by the parties to the smart contract. The smart contract rules—including rules for transaction processing—are intended to facilitate, verify, and enforce the performance of an agreement or transaction. Once executed, the results of the transaction are recorded in the blockchain. Although a smart contract may function without human intervention, it may also include rules for the parties to a transaction to approve the transaction before it can be executed (for example, approval of a purchase requisition before it becomes a purchase order or approval of a receiving report before an invoice is paid).

Smart contracts often form the first block of a B2B blockchain. Like other blockchain transactions, transactions executed by a smart contract are usually irreversible. (Some smart contracts may contain functionality that allows reversal of transactions made in error or when certain conditions are met.)

Internet of Things (IoT)

Various business blockchain applications that use the Internet of Things (IoT) to collect data may include smart contracts. For example, a smart contract may be used to verify that perishable food is prepared, transported, stored, and sold in environments maintained at specific temperature and humidity levels to ensure that it is safe for human consumption. IoT sensors may be placed in various locations to capture these metrics, as well as the specific location, vendor, supplier, handler, batch number, and other relevant information. The results can be reported to a smart contract, which can automatically flag as unsafe any food that was not maintained in accordance with established parameters. When this data is written in a blockchain, authorized participants in the blockchain can see information about the condition of the food and other related information. This transparency in near real-time enables all parties involved in the supply chain to confirm the condition of the food and verify the accuracy and completeness of the data. As discussed in the Risks Associated with a Service Organization’s Use of Blockchain section, however, smart contracts using data communicated from oracles (see subsequent section) that obtain their data from IoT devices may be susceptible to centralized points of risk and compromise.

Oracles

A blockchain and a smart contract have no internal mechanisms for obtaining external information necessary to execute the computer code that is at the heart of a smart contract. For that reason, blockchain oracles use information obtained from sources outside the blockchain as input to smart contracts. Oracles establish the connections that carry information from external sources, such as the IoT devices that record external information, and communicate it to a smart contract. Without oracles, the usefulness of smart contracts is limited, because a smart contract alone is only able to obtain information from data in the blockchain. Some oracles are able to allow data to be transmitted to destinations outside the blockchain. The following conceptualized example shows the use of such oracles by a service organization’s blockchain.
The growers receive data about the quantity and quality of fruit delivered to each plant, along with the prices paid to each grower. The plants receive data that they use to record inventory, accounts payables, and payments made to growers. Information provided to growers is recorded in the growers’ accounts receivable, revenue, and bank accounts. Because all of these transactions are recorded on the blockchain, the information is visible to all participants; therefore, they all have the opportunity to verify the accuracy and completeness of the data.

The first block in the OJBC is a smart contract, which includes rules to pay growers at the time their fruit is delivered to the plant based on the market price reported in a database maintained by an association of growers, fruit dealers, and processors (Association), and the quality and quantity of fruit delivered. Four (4) oracles are involved in this scenario:

PROBLEM:
Citrus processing plants needed to reduce costs, and the growers that supplied them wanted to reduce the time between delivery of fruit and payment.

BLOCKCHAIN SOLUTION:
To achieve these objectives, the plants and growers formed the OJ Blockchain Consortium (OJBC), a service organization that provides financial and supply chain data on fruit delivered to the plants and facilitates the timely payment for fruit to growers.

When the fruit is delivered to the plants, the four oracles transmit the information to the smart contract in near real-time.

The smart contract calculates the amount due to the grower and initiates an ACH credit from the plant’s bank account to be paid into the grower’s bank account. Without a blockchain, smart contracts, and oracles, the parties to the transaction would have to reconcile the related information and research and resolve discrepancies. Prior to the creation of the OJBC, this process often took a month or more, thereby delaying payment to the growers.
There are several different types of oracles (software-based, hardware-based, and human) that may be used to communicate with smart contracts. Often, the type of oracle used depends on whether the communication is (a) initiated by code or by a physical device; (b) outflow, inflow, or both; (c) controlled by a single authority or many; or (d) a combination of these. The risk for each of the different types of oracles is described in the following section of this document.

Risks Associated with a Service Organization’s Use of Blockchain

This section includes some of the risks related to the use of blockchain when a service organization uses blockchain in a system to provide services to user entities. As previously stated, understanding those risks is critical to the service auditor’s identification and assessment of risks that could affect a service organization’s achievement of its control objectives in a SOC 1 examination or its service commitments and system requirements in a SOC 2 examination. The risks in this section are not intended to be all inclusive; there may be additional risks that may be relevant to the specific facts and circumstances related to a particular SOC examination.

In a SOC for service organization examination, the service auditor obtains an understanding of the system, including the controls that service organization management has designed and implemented, to (a) identify and assess the risk that the subject matter (the description of the system, the suitability of the design of the controls, and, in a type 2 examination, the operating effectiveness of the controls) is materially misstated and (b) design procedures that are responsive to those risks. When a service organization uses blockchain, the risks related to its use are relevant to the service auditor’s understanding of the system and the assessment of the risk of material misstatement.

In most cases, the risks identified throughout this document, if not properly mitigated by a service organization, could

- in a SOC 1 engagement, lead to a service organization’s failure to meet one or more of its control objectives, resulting in a potential misstatement of the user entity’s financial statements, and
- in a SOC 2 engagement, lead to a service organization’s failure to achieve one or more of its principal service commitments and system requirements.

Although this document is written for service auditors, user auditors may also find it helpful when trying to understand the risks of material misstatement to user entities’ financial statements in a SOC 1 examination. The following list, although not a comprehensive, includes risks related to the more significant features of blockchain discussed in the Unique Features of Blockchain section of this document.

- **Access control mechanism**
  - The failure of an access control mechanism may result in unauthorized transactions or disclosures of confidential business or personal information. Unauthorized or unauthenticated participants may have inappropriate read or write access to transactions recorded in the blockchain.
  - **Cryptographic key management**
    - The failure to properly manage cryptographic keys may result in unauthorized or unauthenticated participants having inappropriate read or write access to transactions recorded in the blockchain.
    - If sharding used for cryptographic keys is done incorrectly, there is a significant risk of lost or corrupted data.
    - If multi-signature cryptographic keys\(^6\) are stored on the same server, there is a risk that an attack that compromises one key may also compromise the others; in that case, there are increased risks of recording unauthorized transactions in the blockchain and of unauthorized disclosures being made.

---

\(^6\) Multisignature cryptographic keys allow a group of users to sign a single document.
• The use of a single signature cryptographic key increases the risk of loss of access to the records on a blockchain, unauthorized transactions, and unauthorized disclosures.

• Storage of cryptographic keys in insecure locations or weak controls over key access may result in unauthorized individuals having inappropriate read or write access to transactions recorded in the blockchain.

• The loss of cryptographic keys may result in the service organization's or user entities' inability to access digital assets and records.

• If a complete and accurate inventory of cryptographic keys is not maintained, or the inventory is not periodically reviewed by service organization management, unauthorized parties may have inappropriate access. Such access may enable unauthorized transactions to be entered in the blockchain or allow unauthorized disclosure of information.

• If audit logs of access to cryptographic keys are not properly enabled, service organization management may not have sufficient information to detect and research unauthorized access attempts to the keys.

• If audit logs that track access to cryptographic keys are not appropriately restricted, unauthorized attempts to alter such logs may not be detected in a timely fashion; this may permit unauthorized users to enter unauthorized transactions in the blockchain or to make unauthorized disclosures of information.

• If log analysis software designed to alert security officers, internal audit, and appropriate senior level management of suspicious or unusual access to the keys is not enabled or is improperly enabled, successful and unsuccessful attempts to obtain the keys by unauthorized parties may not be detected in a timely fashion. This may result in an unauthorized user entering unauthorized transactions in the blockchain or unauthorized disclosure of information recorded in the blockchain that is not detected in a timely fashion.

• If the individuals who receive and review log analysis software alerts are not competent or do not have sufficient authority to act when unusual or suspicious activity is reported, unauthorized activity may not be detected and responded to in a timely fashion.

• If recertification of users with access to the cryptographic keys is not periodically performed, the risk of unauthorized transactions in the blockchain or unauthorized disclosure of information recorded in the blockchain may not be detected and prevented in a timely fashion.

• **Compliance with laws, rules, and regulations**
  – In certain SOC 2 examinations, a service organization that uses a permissionless public blockchain to provide services to user entities may not be able to achieve its principal service commitments and system requirements related to compliance with laws, rules, and regulations. Examples of situations in which the service organization may be unable to achieve such commitments and requirements include the following:
    • All users on a permissionless public blockchain have unrestricted read access to all records, which may present challenges for compliance with privacy laws, rules, and regulations and for achieving the service organization's service commitments and system requirements.
    • One of the key features and benefits of a permissionless public blockchain is that it allows users to hide their true identities and remain anonymous. Such features may make it difficult for user entities in the financial services industry to comply with the Know Your Customer rules and similar laws and regulations that require them to know and keep detailed records for each customer, as well as for each person who has authority to act on the customer's behalf.

---

7 Financial Industry Regulatory Authority (FINRA) Rule 2090 requires broker-dealers to “use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer.”
• **Consensus mechanisms and protocols**
  
  - A key risk of some consensus mechanisms is the “51% attack,” which refers to an attack on a blockchain by a group of miners who control more than 50% of the network’s computing power. The fewer the number of full nodes, the easier it is for a 51% attack to succeed. Because fewer nodes control the majority of the computer power, attackers may be able to manipulate additions to the blockchain, invalidate previously recorded transactions, and potentially replace older blocks of data — all of which may compromise the integrity of the blockchain.

  - Blockchains used to trade digital assets may use consensus mechanisms based on the validator’s stake (that is, the amount of assets a validator puts up as collateral in order to have the chance to be selected as the validator of a block). The greater a validator’s stake, the less likely the validator will be to falsely validate a block for personal gain; however, the validator’s incentive to be honest is directly related to the stake’s percentage of the validator’s net worth. For example, suppose two validators each stake digital assets worth $50,000 for a chance to validate blocks of transactions. If $50,000 represents only 1% of one validator’s net worth, but 50% of the other validator’s net worth, the former may have less incentive to remain honest than the latter.

  - When a consensus mechanism allows a hard fork in the blockchain, the risk of validation of previously invalid blocks and invalidating valid transactions increases.

  - Compromise of the consensus mechanisms or protocols may lead to freezing of digital assets held by user entities.

  - Consensus mechanism failure, algorithm weakness, obsolescence, or corruption may lead to user entities’ loss of assets or the recoding of inaccurate, incomplete, or duplicate transactions.

  - Weak hashing methods used by a consensus mechanism may result in unauthorized changes, destruction, or disclosure of information.

  - Consensus mechanisms may fail to prevent malformed data (that is, data that cannot be read or correctly processed), or allow invalid transactions, unauthorized transactions, transaction reversals; or enable the inappropriate transfer of digital assets between participants.

• **Double-spend**

  - Permissionless public blockchains used to trade digital assets that use certain consensus mechanisms may permit the same digital asset to be sold or spent more than once — often referred to as a double spend. The perpetrator of a double spend generates multiple transactions that are sent to validators to reverse the original sale of the asset or spend, making it appear as if the original transaction did not occur.

• **Immutability**

  - The protocols of some consensus mechanisms may allow previously recorded transactions to be changed. For example, a hard fork in the blockchain — which may be made for legitimate reasons or facilitated by a 51% attack — may cause previously recorded transactions to be reversed or altered. Other consensus mechanisms, protocols, and smart contracts used by permissioned private blockchains may allow for the reversal of previously recorded transactions when their protocols allow for reversal of ledger entries.
• **Integration and interoperability**
  - The failure to properly integrate the service organization's and user entities' existing technology and systems and make them interoperable (that is, able to work together seamlessly now and in the future with other products, systems, or applications) with the blockchain may degrade processing integrity and availability.

• **Legal ownership**
  - When joining a permissioned private blockchain, the failure to define the legal ownership of transaction records in the blockchain may result in the participant's (owner's) denial of access to records of transactions.

• **Oracles**
  - Oracles are not protected by a blockchain's security controls, which may result in incorrect data being sent to the smart contract (either intentionally or unintentionally) and the execution of transactions that are contrary to the intentions of the parties to the transactions.

  - **Software oracle**
    • Coding errors may cause erroneous information to be communicated to the smart contract, which may result in the incorrect execution of transaction rules or the rejection of otherwise valid transactions.
    • Latency in the communication channel between oracles and smart contracts affects all types of oracles and could result in transactions not being executed or information not being communicated in a timely fashion (for example, the failure to automatically execute security trades based on market information received from the oracle or the failure to notify a buyer of food of spoilage conditions.)

  - **Hardware oracle.** Component malfunctions or failures may result in the reporting of erroneous information to users or the failure to report critical information to users. For example, the malfunction of oracles embedded in medical devices increases the risk of misdiagnosis in electronic health care records entered in blockchains. In another example, the failure of oracles embedded in machines used in food processing plants could delay quality certifications or fail to detect environmental conditions that result in food spoilage.

  - **Human oracles.** Oracles are tasked with reporting certain events that could not be reported by automated means, the inability to confirm their identity may enable unqualified people to introduce data into the blockchain to bias the results.

• **Smart Contracts**
  - Smart contracts that rely on oracles may make erroneous decisions if the oracle is compromised, which could result in financial losses to user entities or inaccurate reporting.
  - When a transaction initiated by a smart contract is recorded in the blockchain, there is a risk that the governing law and jurisdiction specified in the contract may fail to recognize and enforce the rights and obligations of all parties to the transaction. That may affect the parties' legal rights to assets or liabilities incurred as intended by the smart contract. The service organization would ordinarily expect a user entity to address this risk by establishing a complementary user entity control (CUEC), which is discussed in the Additional Considerations for the Service Auditor section of this paper.
  - Smart contracts may not always function as intended. Even the smallest coding errors may have significant consequences, including material financial losses, with little recourse for the injured party. Coding errors and inadequate testing of smart contracts may result in transactions being processed out of the intended sequence (for example, paying for goods before they are received and prior to payment authorization).
  - Inadequate or ineffective change management controls may permit unauthorized changes to smart contracts, which in turn may affect the processing of transactions. The revised terms may result in financial losses to one or more of the parties to the transaction or in a misstatement of the user entity's financial statements in a SOC 1 examination.
Implications of a Service Organization’s Use of Blockchain in SOC for Service Organization Examinations

Overview of Professional Standards and Criteria Governing SOC for Service Organization Examinations

The professional standards and interpretive guidance under which service auditors perform SOC 1 and SOC 2 examinations are presented in the following table:

<table>
<thead>
<tr>
<th>Subject Matter and the Service Auditor’s Opinion</th>
<th>SOC 2 Report: Trust Services Criteria (TSC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In all material respects, based on the criteria described in the service organization's assertion,</td>
<td>In all material respects,</td>
</tr>
<tr>
<td>a. the description of the service organization’s system fairly presents the system that was designed and implemented throughout the period [date] to [date].</td>
<td>a. the description presents the service organization’s system that was designed and implemented throughout the period [date] to [date], in accordance with the description criteria;</td>
</tr>
<tr>
<td>b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period [date] to [date]; and</td>
<td>b. the controls stated in the description, were suitably designed throughout the period [date] to [date] to provide reasonable assurance that the service organization’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period; and</td>
</tr>
<tr>
<td>c. in a type 2 examination, the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period [date] to [date].</td>
<td>c. in a type 2 examination, the controls stated in the description operated effectively throughout the period [date] to [date] to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria.</td>
</tr>
</tbody>
</table>

Professional Standards and Guidance Under Which the Engagement is Performed

<table>
<thead>
<tr>
<th>AT-C section 105, Concepts Common to All Attestation Engagements</th>
<th>AT-C section 105, Concepts Common to All Attestation Engagements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT-C section 205, Examination Engagements</td>
<td>AT-C section 205, Examination Engagements</td>
</tr>
<tr>
<td>AT-C section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting</td>
<td>AT-C section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting (SOC 1®) (SOC 1 guide)</td>
</tr>
<tr>
<td>AICPA Guide Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting (SOC 1®) (SOC 1 guide)</td>
<td>AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)</td>
</tr>
</tbody>
</table>

Criteria

Control criteria: Paragraph 16 of AT-C section 320 presents the minimum criteria for evaluating whether the controls were suitably designed. Paragraph .17 of AT-C section 320 presents the minimum criteria to evaluate whether controls operated effectively for a SOC 1 engagement.

Description criteria: Paragraph 15 of AT-C section 320 presents the attributes of the minimum criteria for the description in a SOC 1 engagement.

Control criteria: TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Description criteria: DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report.
Determining Whether the Engagement Team Possesses the Appropriate Competence and Capabilities

Paragraph .27b of AT-C section 105 indicates that, among other preconditions, a practitioner should accept an attestation engagement only when the practitioner is satisfied that the engagement team possesses the appropriate competence and capabilities to perform the engagement. As previously discussed, however, blockchain is a relatively new and very complex technology. For that reason, service auditors may lack the requisite knowledge of blockchain that is necessary to identify and assess the related risks and to evaluate the controls that the service organization has implemented to mitigate those risks.

The service auditor may obtain knowledge about blockchain through formal or continuing education, practical experience, or consultation with others; however, continuing education alone may not be sufficient to gain the requisite skills and competencies, because blockchain technology is extremely complex and evolving. Although formal or continuing education may include a high-level overview of the key features and risks of using blockchain, it may not enable a service auditor to obtain the in-depth knowledge, skills, and competencies that may be necessary to perform a SOC for service organization examination.

If a service auditor lacks the requisite knowledge and skills, the service auditor may consider using an internal or external specialist who possesses such expertise. According to paragraph .A35 of AT-C section 205, the greater the significance of the work of the specialist in the context of the engagement, the more likely it is that the specialist will work as part of a multidisciplinary team comprising subject-matter specialists and other attestation personnel. Using the work of a specialist in SOC 1 or SOC 2 examinations is discussed in paragraphs .32a–.b and .A61 of AT-C section 105; and paragraphs .36–.38, .A13, .A35–.A43 of AT-C section 205. Using the work of a specialist in a SOC 2 examination is also discussed in paragraphs of 2.160-.166 of the AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.
Obtaining an Understanding of the System

According to paragraph .14–.15 of AT-C section 205, the service auditor should obtain an understanding of the subject matter, as well as an understanding of internal control over its preparation. The service auditor’s understanding of the subject matter needs to be sufficient to enable the service auditor to

a. identify and assess the risks of material misstatement in the subject matter, and

b. provide a basis for designing and performing procedures to respond to the assessed risks and to obtain reasonable assurance to support the service auditor’s opinion.

The evidence the service auditor obtains from those procedures should be sufficient and appropriate to support the service auditor’s opinion in the examination.

When blockchain is an integral part of the system used to provide services to user entities, understanding blockchain is critical. In a SOC 1 examination, an understanding of blockchain allows the service auditor to consider whether it is relevant to a user entity’s ICFR and, if so, how the blockchain interfaces with a user entity’s systems. In that examination, an understanding of blockchain also enables the service auditor to consider whether controls identified in the description, including controls over the blockchain, were suitably designed and implemented and, in a type 2 examination, whether such controls were operating effectively to meet the control objectives.

In a SOC 2 examination, understanding blockchain is critical to forming an opinion about whether the description of the system, including the controls over the blockchain, is presented in accordance with the description criteria relevant to the examination. It also enables the service auditor to evaluate the suitability of design and, in a type 2 examination, the operating effectiveness of controls over the blockchain that are necessary to achieve the principal service commitments and system requirements.

When a service organization’s system uses blockchain, the service auditor’s understanding of blockchain generally includes the following:

• **Architecture and design of the blockchain**
  - If a cloud provider is used to provide services that are part of the blockchain architecture, the nature of the services — for example, infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS), or blockchain as a service (BaaS) — and whether the cloud provider is considered a vendor or a subservice organization. For a SOC 1 examination, the determination of whether a cloud service provider is a vendor or a subservice organization is discussed in paragraphs 3.17–3.18 and in table 3-1 of the SOC 1 guide. For a SOC 2 examination, it is discussed in paragraphs 2.06–2.11 of the SOC 2 guide.
  - The type of blockchain used by the system (that is, whether it is a permissioned private blockchain, a permissionless public blockchain, or a hybrid blockchain) and other relevant information depending on the type of blockchain (such as who can join; the different classes of members and their rights; and how members can interact with others on the blockchain).

• **Access control mechanism**
  - The party, if any, that controls the access control mechanism
  - When the scope of a SOC 2 examination includes the confidentiality or privacy trust services categories,
    - how confidential or personal data stored in the blockchain are protected from unauthorized disclosure;
    - the encryption method used, if any, for confidential or personal information stored in the blockchain;
    - the vulnerability of the encryption method to compromise; and
    - the likelihood that the encryption will be broken during the period covered by the service auditor’s examination.
• **Consensus mechanisms**
  - The design of the consensus mechanism
    - The party, if any, that controls the consensus mechanism
    - The hashing and encryption methods used and the strength of those methods
  - In a permissioned private blockchain
    - If the service organization or user entities control or are permitted to control full nodes that can serve as validators according to the rules of the blockchain

• **Cryptographic key management**
  - Cryptographic key life cycle controls, including controls over
    - design and development,
    - implementation,
    - key generation,
    - storage,
    - access management, and
    - retirement of the keys.
  - The titles of employees, contractors, or consultants that
    - designed and developed the cryptographic key architecture,
    - implemented the cryptographic keys architecture, and
    - generated the keys.
  - How the cryptographic key architecture was tested and the test results
  - The date the cryptographic key architecture was implemented and the keys generated
  - Where and how the keys are stored and whether access to the keys is restricted to only authorized individuals and systems that need such access to perform their job duties and functions
  - The inventory of cryptographic keys maintained by the service organization, including the names and titles of individuals with access to the keys and controls over the inventory’s completeness and accuracy
  - Audit logging and review of access to cryptographic keys and whether the logs are stored in a manner that restricts access to users who do not have access to the keys
  - Log analysis software that alerts appropriate members of management (such as security officers, internal auditors, or other senior personnel) of suspicious or unusual access to the keys, attempts of and successful alteration of the logs, and the names and titles of individuals who receive and review the alerts
  - Frequency of recertification of users with access to the keys and the name and title of the officer that performs the recertification
  - Whether the cryptographic keys have been split into multiple parts (shards), where a subset of those parts is used to recover the original cryptographic key and, if so, the names and titles of the individuals to which the shards have been distributed
  - If multisignature cryptographic keys are used, the titles of the parties who must agree before a transaction can occur

• **Interaction and integration**, if any, between legacy systems at the service organization and the blockchain, including the flow of information and transactions between those systems and the blockchain, as well as controls related to the completeness and accuracy of data exchanged.
  - Whether the blockchain is designed to interact with other blockchains and the effect that may have on the service organization’s ability to meet its control objectives (in a SOC 1 examination) or achieve its principal service commitments and system requirements (in a SOC 2 examination)
  - Reconciliation of legacy system records at the service organization and the records in the blockchain
  - The degree of integration with other technologies such as IoT

• **Monitoring**. How the blockchain is monitored for evidence that recorded transactions actually occurred.
• **Participants.**

  - Whether participants are individuals with a single identity or multiple identities, or individual entities, such as companies, organizations, or government agencies.
  - Whether there may be conflicting interests among the participants, members, and users of the blockchain.

• **Privacy.** When the scope of a SOC 2 includes the privacy trust services category, how the service organization addresses inherent conflicts created by some of blockchain’s key features, including:
  - the purported immutability of records with privacy laws, rules, and regulations, such as the right to be forgotten;
  - procedures to correct, amend, or redact personal information previously added to the blockchain, when the consensus mechanism does not allow changes to records;
  - in a permissionless public blockchain, the pseudo-anonymity of users, because that may undermine privacy laws and requirements to track certain information about such users;
  - the choices offered to data subjects and the consent they have provided; and
  - the disclosure of the use of a decentralized network (that is, that personal information is stored on devices controlled by participants that are not party to the transactions for which the personal information was provided).

• **Smart contracts**

  - The design and nature of transactions that are initiated by smart contracts without human intervention.
  - Oracles and the types of data communicated to and from smart contracts, including the controls over the accuracy and completeness of information communicated.
  - Whether the smart contract was audited by an independent third party to determine that the contract functions as intended.
  - Controls over smart contract rules that result in the complete and accurate initiation, recording, processing, or reporting of transactions and events.
  - Whether the rules for use of the blockchain require the parties to a smart contract transaction to execute a legally binding printed or electronic agreement and whether the agreement requires electronic or physical signatures.
  - Whether transactions executed by smart contract are reversible and, if so, the procedures to reverse them.
  - Whether the smart contract is used to facilitate the integration of the blockchain with other systems and technologies.
  - If smart contracts communicate information about transactions or conditions to user entities, the controls over the completeness and accuracy of the information.
Additional Considerations When Smart Contracts are Used in the Blockchain

When a service organization’s system uses a blockchain that initiates and executes transactions with smart contracts, the service auditor may wish to consider the following additional matters:

- As discussed in the Risks Associated with a Service Organization’s Use of Blockchain section, a smart contract may not always function as intended; therefore, a service organization may have a control that requires the functionality of the smart contract to be audited by an independent third party prior to being placed into production. In this case, the service auditor would expect to see disclosure of the audit of the smart contract in the description.

- A smart contract may not have all of the requirements to be legally enforceable based on governing law or jurisdiction. Therefore, when the service organization’s system includes a smart contract, service organization management may expect a user entity to implement a CUEC requiring a review of the smart contract by the user entity’s general counsel to determine whether it is legally enforceable based on governing law or jurisdiction.

Forming an Opinion on the Description of the System, the Suitability of the Design of the Controls, and in a Type 2 Examination, the Operating Effectiveness of the Controls

As illustrated in the table in the Overview of Professional Standards and Criteria Governing SOC for Service Organization Examinations section, the service auditor opines on (a) the description of the system, (b) the suitability of the design of the controls; and (c) in a type 2 engagement, the operating effectiveness of the controls.

The purpose of the description of the system is to provide user entities with information they can use to assess the risks of doing business with the service organization. Because of the risks associated with the use of blockchain, the description would also be expected to disclose the relevant aspects of the blockchain to meet the description criteria. The description of the system would ordinarily disclose the relevant matters listed in the Obtaining a Understanding of the System section of this document along with the other system elements, including the controls that have been designed, implemented, and operated to mitigate the risks associated with the use of blockchain. The service auditor’s procedures would be designed to obtain sufficient appropriate evidence that disclosures required by the criteria, including relevant aspects of the use of blockchain, are included in the description of the system.

To form an opinion on the suitability of design and, in a type 2 examination, the operating effectiveness of controls, the service auditor focuses on the controls included in the description of the system, including those related to the relevant aspects of the blockchain. To form an opinion on the suitability of design, the service auditor would design procedures to obtain sufficient appropriate evidence to support the opinion on design suitability. Likewise, in a type 2 examination, the service auditor’s procedures would be designed to obtain sufficient appropriate evidence to support the opinion on operating effectiveness. The tests performed and results thereof would be included in section 4 of the SOC report.
Summary

This document discussed how a service organization’s use of blockchain can introduce unique risks into a SOC for service organization examination. The service auditor is required to obtain an understanding of the service organization’s system that will enable the service auditor to identify and assess those risks and provide a basis for designing and performing procedures in response to the assessed risks. When a service organization’s system uses blockchain, the service auditor’s understanding includes how blockchain integrates with the system and the controls over it. An understanding of the issues described in this document will assist the service auditor in performing SOC for service organization examinations in accordance with the attestation standards.
Appendix A

Examples of Service Organizations’ Use of Blockchain

As discussed throughout this document, the integration of blockchain into a system used by a service organization to provide services to user entities raises new challenges and presents unique and significant risks. For illustrative purposes only, this appendix presents four hypothetical examples of how service organizations might use blockchain in systems that provide services to user entities.

Example #1: Payroll Processing

The Payroll BC Consortium, of payroll service organizations uses BaaS to build and implement a permissioned private blockchain to process payroll transactions for its members’ user entities. The identity and access rights of the blockchain’s users are authenticated and established with consensus mechanisms that are used to validate transactions and to achieve consensus.

The first block of the Payroll BC Consortium’s blockchain is a smart contract that initiates, records, processes, and reports user entity transactions. Oracles embedded in tax authorities’ systems communicate changes in the tax code to the smart contract, which calculates employer and employee tax liabilities. All transactions related to the processing of payroll by members of the consortium for user entities are recorded in the blockchain.

Example #2: Employee Benefit Plan Recordkeeping

A large publicly held bank (service organization), provides a full range of retirement plan services to customers. To provide greater value to retirement plans and their participants, and to make the process more efficient, the bank developed and implemented a blockchain solution. The bank utilizes a hybrid blockchain owned and controlled by the members of its permissioned private blockchain component (private component.) The private component runs on a private blockchain platform. Nodes are stored on members’ servers.

The first block of the private component is a smart contract, which contains the logic for processing transactions and identifies the actions to take if certain conditions occur. The smart contract automatically rebalances portfolios, updates reports, and if necessary, alerts user entities’ plan participants of changes (for example, changes in their retirement portfolio) based on data received from oracles. Plan participants have the option to join the bank’s public component, which runs on the platform. Participants can enter and update their retirement plan elections on the blockchain — which allows for automatic changes to their portfolio when certain conditions are met — and download reports and tax forms from a secure website.

---

8 A consortium is composed of a group of companies or organizations formed to undertake an enterprise beyond the resources of any one member.
Example #3: Broker-dealer Blockchain Consortium

A service organization and its peers provide financial services to small- and medium-sized brokers dealers. Such services include recordkeeping, maintenance of trade blotters, stock record books, trading, valuation, and reporting services. To remain competitive, the service organization, its peers, and their clients banded together to create a blockchain consortium (the BD BC Consortium) with the objective of reducing transactions costs and settlement times.

The BD BC Consortium's blockchain is a permissioned private blockchain, which is owned and controlled by its members. Members vote on the governing rules and consensus mechanism protocols used, and ownership and voting rights are proportional to the value of transactions processed by a member.

The BD BC Consortium's blockchain uses a consensus mechanism that uses three key factors to determine members' voting rights and to elect validators: (a) the member's market value, (b) whether the member's stock is publicly traded, and (c) brand recognition. For factor (a), members that are not publicly traded may use discounted future positive cash flows as a proxy for market value. For factor (b), registration with the SEC and membership in the Financial Industry Regulatory Authority (FINRA) satisfies this requirement. For factor (c), brand recognition is measured by data analytics that report the number of favorable or unfavorable mentions of a member's name in the financial press and social media. All potential validators must be approved in advance by the BD BC Consortium's Consensus Mechanism Validation Committee (the Validation Committee).

Example #4: Commercial Real Estate Management Services

A real estate management service organization (service organization) provides virtual services to real estate investment companies (landlords) for the commercial real estate market. The service organization's blockchain system is built on a permissioned private blockchain and uses a consensus mechanism that requires validators to provide a valid government-issued ID. Participants in the blockchain include the service organization, landlords, tenants, and banks, although only the service organization, landlords, and banks can be full nodes and serve as validators of new blocks.

The first block in the blockchain is a smart contract. The service organization informs participants that the smart contract has no legal standing and does not bind the service organization, landlords, and tenants to any rights or obligations; however, the smart contract includes an option to reverse transactions if one of the parties to the transaction makes an error, or if the logic in the smart contract is faulty and causes a transaction to be recorded that is contrary to the intentions of the parties. In addition to agreeing to the terms of the smart contract, the participants must also sign a traditional lease agreement; the terms and conditions of the agreement are agreed to by the landlord and tenant prior to execution.

The cryptographic keys that allow access to the blockchain for service organization employees are stored on a secure server. Landlords and tenants are responsible for the security of their own cryptographic keys.
Appendix B

Additional AICPA Resources

The AICPA has developed several resources to help increase knowledge about blockchain and digital assets, including the following:

White papers
• Blockchain and Internal Control: The COSO Perspective
• Blockchain and Its Potential Impact on the Audit and Assurance Profession
• CPAs Leveraging Blockchain
• 2019 Blockchain Symposium: Experts’ Insights Indicate Growing Use Cases and Value for the Technology

CPE
• Blockchain for Financial Advisors
• Blockchain for Financial Services
• Blockchain for Healthcare
• Blockchain for Insurance
• Blockchain Implications for Audit and Assurance Services
• Blockchain for Not-for-Profits
• Blockchain for Supply Chain
• Digital Mindset Pack (2019-20)

Certificate program
• Blockchain Fundamentals for Accounting and Finance Professionals Certificate Program

Additional resources
• Blockchain Legislation Emerging in State Legislatures
• Emerging Technology Report: Blockchain
• How will blockchain change accounting?

Blog posts
Recognition

The AICPA gratefully acknowledges the following members of the AICPA Implications of Blockchain on SOC 1 and SOC 2 Working Group and others who reviewed or otherwise contributed to the development of this publication.

Implications of Blockchain on SOC 1 and SOC 2 Working Group

Dave Palmer, Chair
Danielle Austin
Brandon Brown
Noah Buxton
Sai Gadia
David Gola
Anthony Graziano
Chris Halterman
Vikram Panjwani
Soma Sinha

AICPA Staff

Amy Pawlicki
Vice President
Assurance and Advisory Innovation

Mimi Blanco-Best
Associate Director
Attestation Methodology and Guidance

Judith Sherinsky
Senior Manager
Audit and Attest Standards

The working group would also like to thank Bruce Nearon for his help developing this paper.